Yevseyeva I, Basto-Fernandes V, Emmerich M, van Moorsel A. Selecting Optimal Subset of Security Controls. *Procedia Computer Science* 2015, 64, 1035-1042.

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 64 (2015) 1035 – 1042

Procedia Computer Science

Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2015 October 7-9, 2015

Selecting optimal subset of security controls

Iryna Yevseyeva[a]*, Vitor Basto-Fernandes[b], Michael Emmerich[c], Aad van Moorsel[a]

[a] *Centre for Cybercrime and Computer Security, School of Computing Science, Newcastle University, Newcastle-upon-Tyne, NE1 7RU, United Kingdom*

[b] *School of Technology and Management, Computer Science and Communications Research Centre, Polytechnic Institute of Leiria, 2411-901 Leiria, Portugal*

[c] *Leiden Institute of Advanced Computing Science, Leiden University, Niels Bohrweg 1, 2333-CA Leiden, The Netherlands*

Abstract

Choosing an optimal investment in information security is an issue most companies face these days. Which security controls to buy to protect the IT system of a company in the best way? Selecting a subset of security controls among many available ones can be seen as a resource allocation problem that should take into account conflicting objectives and constraints of the problem. In particular, the security of the system should be improved without hindering productivity, under a limited budget for buying controls. In this work, we provide several possible formulations of security controls subset selection problem as a portfolio optimization, which is well known in financial management. We propose approaches to solve them using existing single and multiobjective optimization algorithms.

Peer-review under responsibility of SciKA - Association for Promotion and Dissemination of Scientific Knowledge

Keywords: multicriteria optimisation; security; subset selection; portfolio optimization

1. Introduction

The ubiquitous nature of the Internet as well as accessibility and availability of mobile devices (e.g. laptops, phones, tablets) provides great opportunities not only for individuals in their personal life, but also for companies to support work in distributed mobile environments. However, these trends expose both the devices and data stored on

* Corresponding author. Tel.: +44-191-208-7873; fax: +44-191-208-8232.
E-mail address: iryna.yevseyeva@newcastle.ac.uk

Peer-review under responsibility of SciKA - Association for Promotion and Dissemination of Scientific Knowledge
doi:10.1016/j.procs.2015.08.625

them to security risks. For example, devices may be lost or stolen together with sensitive private data owned by individuals or companies, or private data may be observed or intercepted in transition by malicious attackers.

The work on the risk mitigation strategies to prevent potential risks and provide directions for developing security policy for companies has started with initiatives from different institutions: government, companies and researchers, see [1], [2], and [3], correspondingly. However, developing security policies for companies preventing potentially risky situations and protecting from malicious attacks is difficult. It is not only due to the complexity of the risk assessment of all possible risky scenarios, but also due to the multidimensional nature of such scenarios dependent on the potentially uncertain environment, only partially observable by the decision maker, and permanent presence of uncertainty with respect to known and yet unknown attacks.

For large companies, including universities, risk assessment and security policy development are done by the Chief Information Security Officer (CISO), who usually follows governmental or international security initiatives/standards, such as [1, 2]. The CISOs makes sure that important IT assets, both devices and data, of the company are protected from potential security breaches by analyzing security threats and vulnerabilities of the company. For instance, threats may be related to the prevention of denial of service attacks, intellectual property loss and loss of personally identifiable information.

In addition to selecting security controls that will be used in the company, a CISO has to identify potentially risky behaviors of employees that might lead to security breaches and develop a security policy which employees have to follow at work or outside when using their device or dealing with company's sensitive data. A recent trend of consumerization of IT, which considers users of IT devices and services as consumers and pushes companies to adapt to their employees' wishes and needs, created additional security problems. For instance, allowing employees to bring and work with their own devices, a strategy known as Bring Your Own Device (BYOD), or taking mobile working devices and work on them from other than working environment, e.g. in public transport or from home, increases security risks. These trends may introduce opportunities for companies but also introduce new security vulnerabilities and threats that have to be taken into account when developing security policies. In particular a security policy of a company should identify a set of rules and recommendations for employees of the company to follow in order to prevent possible security breaches.

In spite of the standards and guidelines created to help with risk assessment for companies, such as [1, 2], still one of the main difficulties for the company is to make sure employees follow the specified security policy rules and help them making security decisions. At the same time, selection of security controls for the company to invest in is another challenging problem, which should be done based on assessment of security vulnerabilities and identification of potential security threats for the company. On the one hand, introducing many various security measures should increase security; on the other hand, applying them simultaneously may reduce productivity, as it might be time consuming to process many security checks simultaneously. Moreover, the company might have a limited budget for buying controls and has to be selective. Ideally, such selection should try to optimize several conflicting objectives, e.g. productivity and security, simultaneously, and take into account constraints, e.g. limited budget to be spent or limited number of security controls to be bought.

In this work, we propose the formulation of the security controls subset selection as a portfolio optimization problem, which is well known in financial management, and which suites well the need for the selected controls to complement each other. Selection of a subset of security controls should make sure that at least one of the selected controls provides protection against one of critical threats identified by CISO, so that all threats are covered. However, a control might provide protection against several threats simultaneously, and selecting such controls will minimize the size of the portfolio, which is often desired. At the same time the price of the controls can vary and minimizing budget may be considered either as an objective or as a constraint (assuming limited budget can be spent).

The existence of several conflicting objectives, constraints and large number of possible controls need to be considered. However, investigating their properties on the subject of complementarity makes the selection of the optimal subset of security controls complex. In this work, we discuss possible formulations of this problem as a single objective and multiobjective portfolio optimization problems.

In section 2, we discuss existing approaches to the security controls selection. In section 3 we introduce possible formulations of security subset selection as a portfolio optimization problem, compare them, and propose approaches

to solve them using existing optimization algorithms. Finally, in section 4 we conclude our work with implications of the provided approach and indicate directions for future work.

2. Existing approaches to security controls subset selection

Security risk assessment of an organization becomes increasingly sophisticated, information-intensive, and complex, due to constant race against newly appearing security attacks. National and international information security standards, such as ISO/IEC 27001/2 [4], provide general requirements and guidance for information security management and security of information assets in particular. 39 high-level control objectives and 133 security controls are specified for organizations to address risks with respect to information confidentiality, integrity and availability. However, these objectives and controls are suggested as a starting point to define high-level principles for an organization's information security policy, and in reality CISOs have to deal with hundreds of controls to compose their organizations' protection.

Due to such high dimensionality of the information security risk management problem the problem decision aiding tools may be helpful for CISO to compare and choose security controls to be implemented in the company. Searching large combinatorial spaces is challenging, and, in spite of the fast progress of computers hardware, exhaustive search is practically infeasible. Heuristic algorithms, such as evolutionary algorithms, and other metaheuristics made it possible to search large combinatorial spaces automatically and to find solutions near or even optimal [5-8].

Current guidelines for security managers for evaluating security policies are oriented towards monetary-based techniques, mainly cost-benefit analysis [9] or financial and cost-effectiveness analyses. Other approaches from financial analysis were applied to security controls selection, such as value-at-risk and conditional value-at-risk for analysis of the worst-case scenarios, see e.g. [10] and [11]. However, in practice, not only costs and benefits of security controls need to be considered, but also non-monetary, technical and non-technical aspects that may be quantified but not valued, or social aspects that are evaluated only in qualitative terms [12]. Examples include productivity, which might be restricted when introducing security controls; fitness of a control to the culture of organization; other human factors; complexity; maintenance; etc. Such objectives are usually in conflict with each other, e.g. increasing security can be done only at the expense of decreasing productivity and/or increasing cost.

Optimizing several objectives simultaneously is addressed with operational research techniques called multiobjective/multicriteria optimization, see e.g. [5] and [7]. It leads to obtaining not a single solution but a set called Pareto optimal set, represented by all possible trade-offs, e.g. between security and productivity. The size of Pareto optimal set grows exponentially with the number of objectives to be considered. Among other techniques for multiobjective optimization, evolutionary algorithms are considered very efficient due to their capability of directing the search towards and along Pareto optimal front, and thereby representing it well.

The suggestion to use multicriteria decision-making for information security decision-making has been made earlier, e.g. in [13] and [14]. UK government has published a manual on multicriteria decision analysis [9] written by the London School of Economics, providing guidelines for using multicriteria decision analysis techniques with examples of successful application in transport and environment. Recently, a USA-based company, MSB Cybersecurity, delivered to the market Security i-Cue, an enterprise monitoring and analysis tool [15]; it was developed using multicriteria decision analysis techniques [16] and provides analysis of security trade-offs. However, the techniques used are proprietary and it is not clear how advanced or robust they are. Attempts to introduce multicriteria analysis into the field of cyber security were made by Linkov et al. [17, 18] also for managing portfolio of risks [19].

In this work, the complexity of the problem of selecting security controls to be applied within a company will be formulated as both single and multiobjective optimization problems.

3. Portfolio of security controls selection

The motivation for this approach can be illustrated by analogy with financial portfolio selection. When constructing a financial portfolio [20] it is well known that, if returns are generally uncertain, it is not wise to invest everything in an asset with the best optimal expected return. The financial analysts look for diverse assets to

combine within a portfolio in order to minimize risk of failure, if for some reason one type of assets becomes non-profitable. A similar situation appears when selecting security controls to be implemented within a company. In the situation of uncertainty, it is best to be prepared for a variety of possible security threats and attacks (even unknown) and to minimize different types of security risks by implementing security controls of different types.

The approach proposed in this work provides a decision aid for a CISO in the final choice of a set of security controls optimal with respect to objectives, e.g. security and/or productivity, and taking into account constraints, e.g. budget. The selected security policy should be composed by the set of security controls that are mutually complementary with respect to objectives, but taken in isolation might not satisfy either of or all those objectives.

3.1. Formulations of portfolio selection problem

In strategic decision-making and financial management, the portfolio selection problem is well known (see, e.g., [21]). It addresses a way of selecting a combination of several assets in a way that the properties of portfolio assets taken separately may not have the best values, but taken together compose an optimal portfolio. Moreover, they may be very different from each other. However, the combination of such diversified assets, aims at the best possibly achieved quality. Recently, the financial portfolio idea has been successfully applied in various domains, such as strategic decision making for team management [22], IT project portfolio management [23], for environmental selection in evolutionary algorithms for fitness assignment [24].

Portfolio selection problem [22] appears in investment management when it is necessary to combine several assets (companies or industrial sectors) to form an investment portfolio. A financial portfolio should simultaneously satisfy two conflicting goals: minimizing risk and maximizing expected return of the portfolio (see formula (1), a multiobjective formulation):

$$\begin{aligned} &\min \sum_{i=1}^{n} \sum_{j=1}^{n} g_{ij} x_i x_j = x^T Q x; \\ &\max \sum_{i=1}^{n} r_i x_i = r^T x; \\ &s.t. \sum_{i=1}^{n} x_i = 1; \\ &x_i \in [0,1]; i = 1,...,n, \end{aligned} \tag{1}$$

where n is the number of assets; x_i is the proportion of money invested in the asset i; r_i is the expected return (per period) of the asset i; and g_{ij} is the real-valued covariance of expected returns of the assets i and j.

Nobel Prize winner Markowitz developed the most widely used ‘mean-value’ portfolio selection model early in the 50s [20], which assumes that the investor rather minimizes risk at a given minimal level of returns than maximizes expected returns of investments, see formula (2) for one of possible (single-objective) formulation of this portfolio model [22]:

$$\begin{aligned} &\min x^T Q x, \\ &s.t. r^T x \geq R, \\ &Ax = b, \\ &Cx \geq d, \end{aligned} \tag{2}$$

where admissible portfolios in addition to minimizing risk must satisfy some problem specific constraints $X=\{x: Ax=b, Cx\geq d\}$ (i.e., budget constraints) and provide return no less than the expected value R.

The investment management also suggests a large number of measures to evaluate risk to return ratios of portfolios, relatively to a time period (standard deviation), to market behaviour (beta ratio) and to benchmark asset (tracking error, excess return, Sharpe ratio), which would reduce a multiobjective formulation of portfolio selection problem to a single objective one.

3.2. Formulations of security portfolio selection problem

When applying portfolio selection model to security controls selection, some adaptations should be considered. For instance, there is no real return from investing into security; it is rather minimization of expected losses from security breaches (that could be really big), e.g. from possible security attacks or lost data. The expected return of a security control may be interpreted as its capability to protect from potential security threat. Then, the security portfolio expected return might be interpreted as the capability of such portfolio of controls to protect company as a whole from security threats and to minimize losses from potential security breaches.

For selecting a subset of security controls in a portfolio to be implemented in the company, the CISO should be able to evaluate the 'goodness' of security controls, which corresponds to their performance with respect to the objectives considered. For instance, the security of a control can be computed based on its protection capability against each of possible known threat, and can be presented within a following 2-dimensional matrix:

Table 1. Survival proportions of threats after applying security controls.

		Controls (i) r_{iz}		
		1	2	3
Threats (z)	1	0.01	0.5	1
	2	1	1	0.3

Similarly to [11], we can define the probability of an attack scenario k based on the probability of the threats appearing in the attack $z \in Z_k$ and probability of those not related to the attack $z \notin Z_k$, taking place:

$$P_k = \prod_{z \in Z_k} p_z \prod_{z \notin Z_k} (1 - p_z). \tag{3}$$

Then, the overall proportion of successful attacks of threats $z \in Z_k$ that survive all selected controls I_s is computed as the multiplication of individual proportions $\prod_{i \in I_s} r_{iz}$, where $r_{iz} \in [0,1]$ is the proportion of threat z that survives application of the control i, with $r_{iz}=0$ indicating complete prevention of the threat z by the control i and $r_{iz}=1$ indicating the incapability of the control i preventing the threat z. It happens rarely that a subset of selected controls I_s is capable of preventing all possible threats. Then the expected proportion of successful threats z when applying a subset of selected controls I_s is $p_z \prod_{i \in I_s} r_{iz}$. The proportion of successful threats z that survive all applied controls is multiplication of individual proportions and can be computed as $\prod_{i \in I} r_{iz} x_i$.

When compared to the investment in the financial asset by choosing a proportion of the money to be spend on assets of the same type, investment in the security control is done by either selecting it or not (there can be same controls selected twice but it is an integer or binary value). Hence, here we have to deal with integer formulation of the problem and to denote by $x_i \in \{0,1\}$, $i=, \ldots, n$ selection of the control, such that it takes value *1* when a security control is selected or *0* otherwise. Then the security portfolio selection will be formulated as integer programming problem, when compared to continuous formulation of the financial portfolio selection problem presented in formula (1).

Then, the expected loss from all successful attacks can be defined as follows:

$$L = \sum_{k \in K} \sum_{z \in Z_k} P_k a_z \left(\prod_{i \in I} r_{iz} x_i \right), \tag{4}$$

where a_z is the cost of a successful attack from the threat z. Hence, the security objective can be interpreted as minimization of the expected loss presented by (4).

In addition to security, other objectives can be taken into account, such as productivity, which can present all efforts to be spent on taking security measures and applying security controls. It can be presented as minimization of the expected resources to be spent and computed as a weighted sum of all resources used for the implementation of security controls, e.g. man per hour time spent for installation of security controls and applying security measures, e.g. entering password, CPU time needed to run each security control and/or any other resources.

$$S = \sum_{t \in T} w_t \left(\sum_{i \in I} s_{it} x_i \right), \tag{5}$$

where $t \in T$ indicate various resources and w_t their weights. Similarly to the expected losses, expected resources should be minimized.

The cost expressed by the prices of controls can be taken as one of the objectives and minimized. It is also common that security budget is limited and fixed, then it can be taken as a constraint (which is the case here):

$$\sum_{i \in I} c_i x_i \le B, \tag{6}$$

where c_i is the price of the control i.

Some other constraints, such as maximum investment in each type of security control, maximal number of controls to be considered within a portfolio, etc., could also be taken into account. Then, the security portfolio selection problem consists of distributing the budget by investing in different (types of) security controls.

It should be possible to evaluate the capability of security controls to cope with known security threats. However, when it comes to unknown security threats it is really difficult to predict whether controls will be able to protect from security breaches caused by yet unknown threats, as some of new attacks are detected only after damage from them is identified.

In this work we approach uncertainty in protecting against unknown threats by selecting controls that are diverse and differ from each other in their ways of protecting security vulnerabilities. Most of investment professionals agree on diversification as a way to reduce risk by allocating assets of portfolios in different areas or types of financial instruments. By analogy with a financial portfolio selecting controls in a security portfolio could follow the same principle: By associating risk with selecting very similar security controls in portfolio, selection of security controls that differ from each other is encouraged. Then, for minimizing risk in the form of $x^T Q x$, covariance matrix Q should be defined. For instance, it can be presented with 3-dimensional matrix, where a third dimension 'Controls' is added to the matrix presented in Table 2. It should contain pairwise comparison of controls against each other, indicating correlation between performance of controls against each of threats, with positive values g_{ij} indicating similar performance of controls against same threat and negative values g_{ij} indicating uncorrelated performance. The selection of controls with negative covariance in the portfolio is encouraged, as it will improve the risk term. Thus, the presence of 'not-so-good' security controls with respect to some of objective values in the security portfolio can be explained: they are complementary and probably protect against different threats when compared to 'good' security controls. Next, the general portfolio selection problem model will be considered and then adapted to security the portfolio selection problem.

The multiobjective *Formulation I* of the security subset selection problem can be presented as follows:

$$\begin{aligned} &\min x^T Q x; \\ &\min l^T x; \\ &\min s^T x; \\ &s.t. c^T x \le B; \\ &x_i \in \{0,1\}; i = 1,...,n, \end{aligned} \tag{7}$$

where $c^T x \le B$ refers to the budget constraint and $x_i \in \{0,1\}$ to the integrality condition. This formulation can be interpreted as follows: where n is the number of security controls to be included in the security portfolio (it is constant); x_i is the decision variable, which indicates where the control i is selected ($x_i=1$) or not ($x_i=0$); l^T and s^T are expected losses and expected resources to be spent, respectively; and Q is a covariance for security controls.

Selecting negatively correlated controls in the security portfolio to be implemented is encouraged: it corresponds to the diverse portfolios, which minimize risk.

It should be noted that solving problems (1) or (7) results in Pareto set of security portfolios. All portfolios in Pareto set are efficient, because they present trade-offs between maximal return and minimal risk. However, from Pareto set a single solution should be selected for implementation. Different ways of choosing such a solution exist, and one of them is moving the expected return from objectives to constraints by setting some minimal return to be achieved as was shown in Markowitz model (2) and obtaining a single optimal security portfolio. Then single objective *Formulation II* of the security subset selection problem can be presented as follows:

$$\begin{aligned} &\min x^T Q x; \\ &s.t. l^T x \le L; \\ &s^T x \le S; \\ &c^T x \le B; \\ &x_i = \{0,1\}, i = 1,...,n, \end{aligned} \tag{8}$$

where the main objective is minimizing the risk, the other objectives: expected losses, expected resources to be spent and budget are presented by constraints with expected maximum values of L, S and B for monetary losses, resources units and budget, respectively.

3.3. Approaches to solve proposed formulations

In this work three alternative formulations of security portfolio selection model are presented: *Formulation I* (multiobjective formulation) presented by formula (7) is selecting a portfolio of diverse security controls that are optimizing return (with respect to minimizing expected losses) and risk (with respect to diversity of controls assuming they can prevent from various known and unknown security threats) and satisfying limited budget constraints simultaneously. Formulation (8) is a single objective formulation reduced from (7). *Formulation II* presented by formula (8) minimizes risk assuming return and budget are constrained.

Both formulations require solving quadratic integer programming problems and are computationally difficult (NP hard), which means they can be solved to the optimality only for small to medium size of the initial data sets of available security controls and subset of controls to be chosen. For solving problems with small to medium data sizes (up to 100 items to be selected out of 750 items) solvers based on branch and bound type of algorithms could be considered. For instance, recently developed Gurobi solver [25] show promising preliminary results. For solving problems with large data sets approximation algorithms such as evolutionary algorithms can be used, e.g. presented in jMetal framework [26].

4. Conclusions and future work

In the situation of uncertainty with respect to known and unknown attacks in security decision-making, selecting a subset of security controls to be implemented within a company is crucial. With the aim of helping a CISO to choose such a subset we proposed several formulations of the portfolio of security controls selection problem. The idea to reduce risk by diversifying such portfolios to order face a-priori unknown attacks. The proposed models are based on well-known financial portfolio selection problems adapted to security portfolio selection. This provides an elegant formulation for these models. One multiobjective and two single objective formulations are presented and exact and approximate approaches to solve them are discussed. In future the models should be tested for the real case scenarios, which are omitted here due to pages limit.

Acknowledgements

Iryna Yevseyeva acknowledges Engineering and Physical Sciences Research Council (EPSRC), UK, and Government Communications Headquarters (GCHQ), UK, for funding Choice Architecture for Information Security (ChAISe) project EP/K006568/1 as a part of Cyber Research Institute.

References

1. 10 Steps to cyber security: executive companion. BIS/12/1120. Published on 5 September 2012. https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility
2. Mobile Devices. Guide for Implementers. Published in February 2013. MWR InfoSecurity. https://www.cpni.gov.uk/Documents/Publications/Non-CPNI_pubs/2013-02-22-mobile_devices_guide_for_implementers.pdf
3. Consumerization of IT: Risk Mitigation Strategies. Responding to the Emerging Threat Environment. ENISA Deliverable. Published on 19 December 2012. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COIT_Mitigation_Strategies_Final_Report
4. ISO/IEC 27002, Information Technology – Security Techniques – Code of practice for information security management, 2005. http://www.iso.org/iso/catalogue_detail?csnumber=50297
5. Miettinen K.: Nonlinear Multiobjective Optimization. Kluwer, 1999.
6. Bäck Th., Fogel D.B. and Michalewicz Z.(Editors): Handbook of Evolutionary Computation, Taylor and Francis, 1997.
7. Deb K.: Multi-Objective Optimization Using Evolutionary Algorithms, Wiley, Chichester, UK, 2001.
8. Eiben A.E. and Smith J.E.: Introduction to Evolutionary Computing, Springer, Natural Computing Series, Corr. 2nd printing, 2007
9. Gordon L.A. and Loeb M.P. Managing Cybersecurity Resources: A cost-benefit analysis. McGraw-Hill Inc. 2006.
10. Rakes T.R., Deane J.K., Rees L.P. IT security planning under uncertainty for high-impact events, Omega: International Journal of Management Science 40 (1) (2012) 79–8.
11. Sawik T., Selection of optimal countermeasure portfolio in IT security planning. Decision Support Systems 55 (2013) 156-164.
12. Dodgson J.S. , Spackman M., Pearman A. and Phillips L.D. Multi-criteria analysis: A manual. Department for Communities and Local Government: London. 2009. ISBN 9781409810230, http://eprints.lse.ac.uk/12761/
13. Butler. S. A. Improving Security Technology Selections with Decision Theory. Third Workshop on Economics - Driven Software Engineering Research, 2001.
14. Viduto V., Maple C., Huang W., Lopez-Perez D. A novel risk assessment and optimization model for a multi-objective network security countermeasure selection problem, Decision Support Systems 53 (2012) 599–610.
15. True North Consulting LLC website: http://www.tru-nor.com/network-monitoring--analysis.html
16. MSB Cybersecurity website: http://www.msbai.com/security-insight-overview.php
17. Linkov I., Satterstrom F.K., Kiker G., Batchelor C., Bridges T., Ferguson E. From comparative risk assessment to multi-criteria decision analysis and adaptive management: Recent developments and applications. Environment International 32 (2006)1072–1093.
18. Lambert J.H., Keisler J.M., Wheeler W.E, Collier Z.A. and Linkov I. Multiscale approach to the security of hardware supply chains for energy systems, Environ Syst Decis, Springer, 2013.
19. Keisler J.M., Linkov I. and Loney D.: Managing a portfolio of risks. University of Massachusetts Boston, US, January 2011.
20. Markowitz, H. Portfolio Selection. The Journal of Finance 7 (1952), pp. 77-91.
21. Kirkwood C. W.: Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets. Belmont, California, USA: Wadsworth Publishing Company, 1997.
22. Cornuejols G. and Tutuncu R.: Optimization Methods in Finance. Cambridge University Press, 2007.
23. Bonham S.: IT Project Portfolio Management. Norwood, Artech House, Incorporated, 2004.
24. Yevseyeva I, Guerreiro A.P., Emmerich M.T.M., Fonseca C.M.: A portfolio optimization Approach to Selection in Multiobjective Evolutionary Algorithms, In T. Bartz-Beielstein, J. Branke, B. Filipič, J. Smith (Editors) "Parallel Problem Solving from Nature – PPSN XIII", Ser. LNCS (vol. 8672), Springer, (2014) 672-351.
25. Gurobi Optimizer 6.0. Gurobi Optimization 2015. http://www.gurobi.com/
26. Durillo J.J., Nebro A.J. jMetal: a Java Framework for Multi-Objective Optimization. Advances in Engineering Software 42 (2011) 760-771.