SCIENCE CHINA
Information Sciences

• INSIGHT •

October 2016, Vol. 59 108102:1–108102:3
doi: 10.1007/s11432-015-0856-7

Multi-objective evaluation and optimization on trustworthy computing

Chuang LIN [*] & Chao XUE

Department of Computer Science & Technology, Tsinghua University, Beijing 100084, *China*

Received March 1, 2016; accepted April 19, 2016; published online September 13, 2016

Citation Lin C, Xue C. Multi-objective evaluation and optimization on trustworthy computing. Sci China Inf Sci, 2016, 59(10): 108102, doi: 10.1007/s11432-015-0856-7

TC (trustworthy computing) is important. Since the appearance of TCB in TCSEC in the 1980s and the following TDI and TNI, to the establishment of TCPA and the reorganization of TCG in April 2003, discussion and research on TC have lasted more than 30 years both in academia and industry. There are plenty of achievements and understanding in the exploration of software and networking trustworthiness, and they have been continuously developing and evolving with the appearance of new technology and environment.

Different from traditional system and data security, more attributes are imported to form the trustworthy characteristics, including reliability, survivability, correctness and so on as illustrated in [1]. Ref. [2] gives a hierarchical model for trustworthy metrics of software which distinguishes the trustworthy attributes into critical and non-critical ones. Ref. [3] applies these attributes into sub-attributes further in their spacecraft software environment recently.

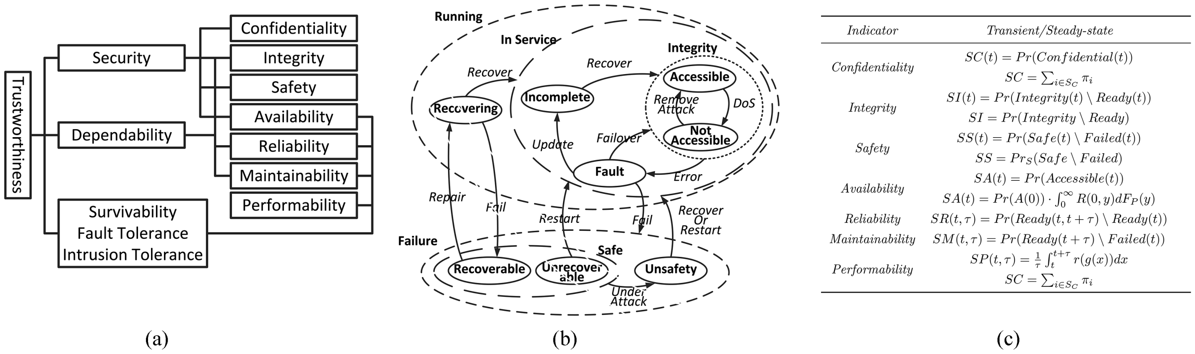
Previous work on TC evaluation is mainly in two ways, combination model and state model. The former focuses on combinational logic relationship and probability analysis between components in references such as Fault Tree [4], Decision Diagram [5] and Reliability Block Diagram [6]. State based model focuses on description of the system's continuous transmutation process based on state transition rate, for example, Markov Reward Model and Stochastic Petri Nets [7]. The former is simple with less calculation, and the latter is complex with a stronger descriptive power. Trust chain [8] based logical derivation and Model Checking [9] are also used to consider the trustworthy attributes.

However, there is a lack of quantitative indicator definitions. Indicators involved are often different without an uniform standard. We believe that a quantitative indicator system which contains the main indicators of the past researchs is necessary and feasible. It is the premise of comprehensive system design and optimization. And it should be based on the basic attributes and self-consistent.

According to existing research, we propose a quantified multi-objective indicator system for TC as in Figure 1(a). We put the trustworthy attributes of a system hierarchically into different levels which is similar to [3]. The high-level attributes, such as security and dependability, also have their intersection of low-level attributes. We give the quantified expression for each attribute in Figure 1(c) based on this framework. The expressions include transient form and steady-state form depending on the evaluation model.

With this indicator system, we can construct the trustworthy analysis model and service state transition model. In trust analysis model, Statis-

[*] Corresponding author (email: chlin@tsinghua.edu.cn)
The authors declare that they have no conflict of interest.



Indicator	*Transient/Steady-state*
Confidentiality	$SC(t) = Pr(Confidential(t))$ $SC = \sum_{i \in S_C} \pi_i$
Integrity	$SI(t) = Pr(Integrity(t) \setminus Ready(t))$ $SI = Pr(Integrity \setminus Ready)$
Safety	$SS(t) = Pr(Safe(t) \setminus Failed(t))$ $SS = Pr_S(Safe \setminus Failed)$
Availability	$SA(t) = Pr(Accessible(t))$ $SA(t) = Pr(A(0)) \cdot \int_0^\infty R(0,y) dF_P(y)$
Reliability	$SR(t,\tau) = Pr(Ready(t,t+\tau) \setminus Ready(t))$
Maintainability	$SM(t,\tau) = Pr(Ready(t+\tau) \setminus Failed(t))$
Performability	$SP(t,\tau) = \frac{1}{\tau} \int_t^{t+\tau} r(g(x)) dx$ $SC = \sum_{i \in S_C} \pi_i$

Figure 1 Quantified multi-objective indicator system for trustworthy computing. (a) Indicator system; (b) state relationship; (c) indicator expression.

tical Decision Theory can be used to analyze trust behavior, and Game Theory can be used to construct the cost model of network intrusion. In service state transition model, we can set up a state transition model based on end-to-end service state and compute the instantaneous state probability or stationary probability distribution. Formalized relevance between each trustworthy attribute is shown in Figure 1(b).

In large-scale network system, share and competition of different nodes can make trustworthy behavior complex and nonlinear. Simple models cannot give a clear description of system's trustworthy behavior while complex models will make the evaluation difficult with state space explosion. Model simplification should be emphasized here for fully leveraging the descriptive power of our comprehensive indicator system. With BDD/MDD partially solved, macro state, state truncation, hierarchical model and state merging technique can be used to avoid the appearance of large model and state space explosion.

The goal of indicator system and formal expressions is optimization. Our multi-objective indicator system of TC includes the indicator from different dimensions such as performance, dependability and security. Therefore, design and optimization of a trustworthy system are both essentially MOP (multi-objective optimization problem). Different from SOP (single-objective optimization problem), there is not always a single optimal solution but a Pareto optimal solution set under the scope of Pareto domination instead. We can transform MOP to SOP by some specific methods such as linear weighting and then solve the new SOP as usual. Or, we can solve MOP directly by multi-objective genetic algorithm. In our previous work [10], we have transformed the MOP into SOP to achieve the structure and scalability evaluation on the control plane of SDN. In [11], we propose a partial selection algorithm to improve the MOP algorithm and maintain the Pareto optimal character at the same time. There are some differences between the typical MOP and MOP in trustworthy computing. And we also give the proof on the equivalence of linear weight and ϵ-constraint method under given condition in [12].

The objectives are hierarchical in our indicator system. Low-level indicators covered by high-level attributes may have intersections. Objectives in intersections may cause different results to their upper objectives, thus influence the overall MOP in a complex way. For example, the optimization of dependability and reliability has the hierarchical relationship as illustrated in Figure 1(a). This structure belongs to Multilevel Programming Problem and it is NP-hard. Branch-and-bound [13], penalty function [14] and genetic algorithm have been used to solve such kind of MOP.

In a trustworthy system, indicators may change over time with environment's variation. We should treat trustworthy environment as a time-varying system and define the optimization problem as DMOP (dynamic-MOP) corresponding to SMOP (static-MOP). Objective functions are related to decision variable and time in DMOP. It will make the traditional algorithm in SMOP wrong or inefficient. Methods with more powerful population prediction [15], search strategy [16] and immune mechanism [17] are proposed for DMOP. Simultaneously, improving methods from DSOP or SMOP have also been attempted.

There is a huge research space in multi-objective analysis, evaluation and optimization on TC. Many challenges remain and future work can be conducted within the scope of our indicator system. For example, how to propose more descriptive models that adapt to new environment such as cloud, how to find more efficient model solving method, how to understand the essential relationship between different indicators of TC and how to develop TC specific solutions of Multilevel Programming Problem and DMOP. Theories that can describe complex dynamic processes are also necessary for modeling and evaluation on trustworthy environments at the same time.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61472199), Tsinghua University Initiative Scientific Research Program (Grant No. 20121087999).

References

1 Liu K, Shan Z G, Wang J, et al. Overview on major research plan of trustworthy software. Bulletin National Natural Sci Found China, 2008, 22: 145–151

2 Tao H, Chen Y. A new metric model for trustworthiness of softwares. Telecommun Syst, 2012, 51: 95–105

3 Wang J, Chen Y X, Gu B, et al. An approach to measure and grading software trust for spacecraft software (in Chinese). Sci Sin Tech, 2015, 45: 221–228

4 Nguyen T P K, Beugin J, Marais J. Method for evaluating an extended fault tree to analyse the dependability of complex systems: application to a satellite-based railway system. Reliab Eng Syst Safe, 2015, 133: 300–313

5 Mo Y C. A multiple-valued decision-diagram-based approach to solve dynamic fault trees. IEEE Trans Reliab, 2014, 63: 81–93

6 Catelani M, Ciani L, Venzi M. Sensitivity analysis with MC simulation for the failure rate evaluation and reliability assessment. Measurement, 2015, 74: 150–158

7 Xu M, Zhang L, Jansen D N, et al. Multiphase until formulas over Markov reward models: an algebraic approach. Theor Comput Sci, 2016, 611: 116–135

8 Zhu J X. A trustworthy software designing approach and credibility evaluation. Appl Mecha Mater, 2014, 513: 602–605

9 Alexander P, Pike L, Loscocco P, et al. Model checking distributed mandatory access control policies. ACM Trans Inf Syst Secur (TISSEC), 2015, 18: 6

10 Hu J, Lin C, Li X, et al. Scalability of control planes for software defined networks: modeling and evaluation. In: Proceedings of IEEE 22nd International Symposium of Quality of Service (IWQoS), Hong Kong, 2014. 147–152

11 Chen Y, Huang J, Lin C. Partial selection: an efficient approach for QoS-aware web service composition. In: Proceedings of IEEE International Conference on Web Services (ICWS), Anchorage, 2014. 1–8

12 Lin C, Chen Y, Huang J, et al. A survey on models and solutions of multi-objective optimization for QoS in services computing. Chinese J Comput, 2015, 38: 1907–1923

13 Bard J F. Practical Bilevel Optimization: Algorithms and Applications. Berlin: Springer Science Business Media, 2013

14 Jiang M, Meng Z, Shen R, et al. A quadratic objective penalty function for bilevel programming. J Syst Sci Complex, 2014, 27: 327–337

15 Zhou A, Jin Y, Zhang Q. A population prediction strategy for evolutionary dynamic multiobjective optimization. IEEE Trans Cybernet, 2014, 44: 40–53

16 Wu Y, Jin Y, Liu X. A directed search strategy for evolutionary dynamic multiobjective optimization. Soft Comput, 2015, 19: 3221–3235

17 Lin Q, Chen J. A novel micro-population immune multiobjective optimization algorithm. Comput Oper Res, 2013, 40: 1590–1601