Cyber Security Problem based on Multi-Objective Distributed Constraint Optimization Technique

Tenda Okimoto, Naoto Ikegai
Transdisciplinary Research Integration Center
Tokyo, Japan
tenda@nii.ac.jp, naoto@ikegai.jp

Tony Ribeiro
The Graduate University for Advanced Studies
Tokyo, Japan
tony ribeiro@nii.ac.jp

Katsumi Inoue, Hitoshi Okada
National Institute of Informatics
Tokyo, Japan
{inoue,okada}@nii.ac.jp

Hiroshi Maruyama
Institute of Mathematical Statistics
Tokyo, Japan
hm2@ism.ac.jp

***Abstract*—A cyber security problem is an important application domain for systems resilience. The increase of malware, computer viruses, and intensive cyber attacks are serious problems for our information society. In this paper, we introduce a new presentation of a cyber security problem. Our model is based on a Multi-Objective Distributed Constraint Optimization Problem (MO-DCOP) which is a fundamental problem that can formalize various applications related to multi-agent cooperation. MO-DCOP is suitable for modeling a cyber security problem, since cyber security problems involve multiple criteria, e.g., risk (security), surveillance (privacy) and cost. Furthermore, MO-DCOP is a decentralized model. In this model, variables and constraints are distributed among agents. Since there exists no single agent which maintains all informations, it is resilient against intensive cyber attacks. Furthermore, we develop a novel algorithm for solving a cyber security problem which utilizes well-known and widely used branch and bound technique and depth-first search strategy and finds all trade-off solutions. We also propose the extension of this algorithm which utilizes a preprocessing technique called soft Arc Consistency. The softAC is a well-known preprocessing technique which transforms a constraint optimization problem into a simplified problem that can be solved efficiently. In the experiments, we examine the run time of our proposed algorithms in cyber security problems and show that our algorithms can solve cyber security problems quickly.**

***Keywords*-Cyber Security Problem, Multi-Objective Distributed Constraint Optimization**

I. Introduction

Security and privacy problems are major issues for the Internet users. The conveniences of Internet are counterbalanced by the lack of resilience in security systems and the risk of misuse of private data. High levels of security for Internet communications usually require analysis of such data by accredited individuals or organisations. Paradoxically, these security measures themselves invade personal privacy and organisational needs for confidentiality. An example of such measure is the Data Retention Directive (2006/24/EC) adopted in 2006 by the European Union because of the terrorist attacks in London (2005) and Madrid (2004). This directive requires EU member country to make new law that includes the obligations for telecommunication companies to retain all communications data for six to 24 months. Communications data include such as IP address and time of use of every email, phone call and text message sent or received. Such information can be used for crime investigation such as terrorist communication, cyber attack, and other serious cyber crimes.

More recently, in 2011, U.S. representatives proposed the Cyber Intelligence Sharing and Protection Act (CISPA). At the time of writing, this is just a proposal under the congress debate process. This act allows U.S. based ISPs to share cyber threat information including customer's communications data with intelligence community and cyber security entities in case cyber attack occurs, regardless of any privacy and data protection law. Most of ISPs welcomes this act because of recent growing cyber attack risks. Especially in these years, reality of international cyberwar grows increasingly, so cyber security problem has also been treated as an important factor even in the national defense policy context. But these measures have been broadly criticized by civil groups around the world regarding the violation of individual liberties and privacy [1], [9]. The adequate balance between security and privacy is the central issue for institutional design of the modern information society.

In this paper, we introduce a novel presentation for cyber security problems using the formalization of a *Multi-Objective Distributed Constraint Optimization Problem* (MO-DCOP) [7]. An MO-DCOP is the extension of mono-objective *Distributed Constraint Optimization Problem* (DCOP) [13] which is a fundamental problem that can formalize various applications related to multi-agent cooperation. An MO-DCOP is a DCOP which involves multiple criteria. MO-DCOP is suitable for modeling a cyber security problem, since cyber security problems involve mul-

tiple criteria, e.g., risk (security), surveillance (privacy) and cost. Furthermore, MO-DCOP is a decentralized model. In this model, variables and constraints are distributed among agents. Since there exists no single agent which maintains all informations, it is resilient against intensive cyber attacks.

Furthermore, we develop a novel algorithm called Branch and Bound search algorithm (BnB) for solving a cyber security problem. This algorithm utilizes well-known and widely used branch and bound technique and depth-first search strategy and finds all trade-off solutions. The BnB is resilient algorithm. Since agents know all trade-off solutions of a cyber security problem, they can easily switch/change their decisions in an emergency, e.g., serious cyber attacks. We also propose the extension of BnB which utilizes a preprocessing technique called soft Arc Consistency (softAC). The softAC is a well-known preprocessing technique which transforms a constraint optimization problem into a simplified problem that can be solved efficiently. This extended algorithm can find all trade-off solutions like BnB. In the experiments, we examine the run time of our proposed algorithms in cyber security problems and show that our algorithms can solve cyber security problems quickly.

The contribution of this work is two-fold:

1) For social scientist, this work introduces a novel presentation of a cyber security problem and provides a faster complete algorithm which can solve all trade-off solutions.
2) For AI researcher, this work introduces a challenging application domain. We believe that this paper provides a new exciting research domain, that is build on the success of cyber security and MO-DCOP researches.

The rest of this paper is organized as follows. Section II describes cyber security and introduces the situation in Japan in Section III. Section IV formalizes a cyber security problem using the formalization of an MO-DCOP and provides novel algorithms for solving this problem. Section V evaluates our algorithms in cyber security problems. Section V introduces the related work. We conclude this paper in Section VII and provide some perspectives for future work.

II. Cyber Security

In recent years, a cyber security problem arouses considerable interest around the world. Increasing malware, computer viruses, and intensive cyber attacks are serious risk for our information society. In specific, recent expansion of networked critical infrastructures such as e-government and smart grid increases vulnerability of our society in a sense [4]. If such infrastructure is under massive cyber attack and suspended, our daily life and economic activity suffer a serious damage. Cyber attack on Estonia and following government system down in 2007 is an iconic event of these massive cyber risks [10]. Our society and information systems must be more resilient for a broad array of modern cyber risks. Additionally, Internet can be used as useful communication tool even for the serious crime such like terrorist attack and drug offense. Police office and relevant government authorities must be able to collect communication logs for the purpose of prevention and detect these crimes. This is another considerable aspect of making information society more secure and resilient.

To detect such variety of unlawful activities, communication intercept can be imperative tool for ISPs and relevant authorizes. Especially, recent development of DPI (Deep Packet Inspection) technology expands effectiveness of the interception [8]. As already mentioned, to detect the criminal activity, retention of communication logs by ISPs is important factor. Using and analyzing those data lawfully, privacy and data protection laws must be modified to fit these cyber security activities. Above-mentioned legislations, such as EU's Data retention directive, U.S's CISPA are required for these reasons.

But, what is most important, interception and communication data retention measures, even if the purpose is social security, are under difficult trade-off between SECURITY and PRIVACY. New cyber security legislations have triggered a storm of criticism from civil society and human rights groups on a broad scale [14]. Privacy and confidentiality of communications are guaranteed in the constitutional law in most of developed countries. In some EU countries, implication of the Data retention directive judged as unconstitutional by domestic court [5]. The another element is COST. Activities such like holding large scale communications data, or operating DPI technologies burden heavy cost for ISPs and related companies [3]. In summary, cyber security issue is under the three-dimensions trade off between security, privacy and cost. Our society must solve this trade-off, but the societal consensus of the solution can be changed depending on the technical environment, social/economic situation, and seriousness of the cyber risk. We propose a systematic approach to deal with the complex trade-off.

III. Situation in Japan

In Japan, the problem is more complex. Under the Japanese Constitutional Law which became effective in 1947 and the other related privacy protection laws, the meaning of *secrecy of communication* is very broad. The latter clause of article 21 of the Japanese Constitutional Law says *No censorship shall be maintained, nor shall the secrecy of any means of communication be violated*. The meaning of the word *communication* is interpreted as containing not only communication content itself, but also communication data by court and government, e.g., government's official commentary of Telecommunication Law of 1984 article 4. Even if the purpose is cyber security, government/ISP cannot scan or brock them without strongly clear and comprehensive consent of customers. How to amend or change the

interpretation of secrecy of communication is very important topic in Japanese legal scholars in these years.

The retention of communication data is also highly discussed. There is not similar law or provision corresponding to the EU's Data Retention Directive in Japan. But in 2011 amendment of the Criminal Procedure Law that has made for the purpose of ratifying the Convention on Cybercrime, limited preservation of communication data by request from relevant authority has been newly added. The provision accredits the government authority to request ISPs to keep their customer's communications data in at most 30 days in case of specific criminal activities is detected without the court's warrant. Many Japanese legal scholars criticize it from the viewpoint of privacy and secrecy of communication. On the other hand, the need for new data retention law is discussed mainly by police office recently. As internationally known, after the 311 earthquake in Fukushima, the national sensitiveness of large scale risks is rapidly changing. To build the societal consensus to solve such types of trade-offs is crucial problem for the resilience of Japan.

IV. Model and Algorithm

In this section, we model a cyber security problem by using the formalization of a Multi-Objective Distributed Constraint Optimization. Furthermore, we introduce a novel complete algorithm called Branch and Bound search algorithm (BnB) which utilizes well-known and widely used branch and bound technique and depth-first search strategy to find all trade-off solutions. We also provide the extension of this algorithm called Branch and Bound search algorithm with soft Arc Consistency (BnB+softAC) which combines a preproseccing technique (soft Arc Consistency) with BnB.

A. Cyber Security Problem

We introduce a novel presentation for cyber security problems by using the formalization of a Multi-Objective Distributed Constraint Optimization (MO-DCOP) [7]. A cyber security problem is defined by a tuple $< S, X, D, C, O >$ where $S = \{1, ..., n\}$ is a set of agents, $X = \{x_1, ..., x_n\}$ is a set of variables, $D = \{D_1, ..., D_n\}$ is a set of domains, $C = \{C^1, C^2, C^3\}$ is a set of constraints, and $O = \{O^1, O^2, O^3\}$ is a set of objective functions. Each C^l and O^l $(1 \leq l \leq 3)$ represent a set of constraints and objective functions for risk, surveillance and cost, respectively. An agent i (human, intelligent program, company, country etc.) has its own variable x_i. A variable x_i decides its value from a discrete domain $D_i = \{scan, \ no \ scan\}$. A constraint relation (i, j) means there exists a constraint relation between x_i and x_j. For an objective l and x_i, x_j, which have a constraint relation, the cost for an assignment/decision $\{(x_i, d_i), (x_j, d_j)\}$ is defined by a cost function $f^l_{i,j}(d_i, d_j) : D_i \times D_j \rightarrow \mathbb{R}$. For an objective l and an assignment/decision to all variables A, let us denote

$$R^l(A) = \sum_{(i,j) \in C^l, \{(x_i,d_i),(x_j,d_j)\} \subseteq A} f^l_{i,j}(d_i, d_j).$$

Then, the solution of a cyber security problem is defined by a cost vector, denoted $R(A) = (R^1(A), R^2(A), R^3(A))$. For a cyber security problem, finding an assignment/decision that minimizes all objective functions, i.e, risk, surveillance and cost, simultaneously is ideal. However, in general, since trade-offs exist among objectives, there does not exist such an ideal decision. Thus, we characterize the optimal solution of this problem using the concept of *Pareto optimality*.

Definition 1 (Dominance): For a cyber security problem and two cost vectors $R(A)$ and $R(A')$, we say that $R(A)$ *dominates* $R(A')$, denoted by $R(A) \prec R(A')$, iff (i) it holds $R^l(A) \leq R^l(A')$ for all objectives l, and (ii) there exists at least one objective l', such that $R^{l'}(A) < R^{l'}(A')$.

Definition 2 (Pareto optimal decision): For a cyber security problem and a decision of all agents A, we say that A is the *Pareto optimal decision*, iff there does not exist another decision A', such that it holds $R(A') \prec R(A)$.

Definition 3 (Trade-off solution): For a cyber security problem, we call a cost vector obtained by a Pareto optimal decision as the *trade-off solution*. Solving a cyber security problem is to find a set of trade-off solutions.

A cyber security problem can be represented as a graph (constraint graph) in which nodes correspond to variables and each edge represents a constraint. The number of the trade-off solutions is exponential in the worst case, i.e., in case every assignment/decision is Pareto optimal decision.

Example 1 (Cyber security problem): Figure 1 shows an example for a cyber security problem with three agents $\{A_1, A_2, A_3\}$. All agents cooperate with each other, maintain the web site, and decide to scan the web site or not. Table I represents three cost tables among three agents. For example, for a constraint between A_1 and A_2, when they don't scan the web site, the risk value becomes high (12), while the surveillance value is low (0). On the other hand, in case A_1 and A_2 decide to scan the web site, the risk value decreases but the surveillance value increases. The Pareto optimal decisions of this problem are $\{\{(A_1, scan), (A_2, scan), (A_3, scan)\}, \{(A_1, scan), (A_2, no \ scan), (A_3, no \ scan)\}\}$ and the obtained trade-off solutions are $(6, 3)$ and $(10, 1)$.

Let us describe why we model a cyber security problem by an MO-DCOP. First, we can handle multiple criteria in MO-DCOPs. Since cyber security problems involve multiple criteria, e.g., risk, surveillance and cost, MO-DCOP is suitable for cyber security problems. Next, MO-DCOP is a

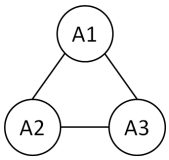


Figure 1: Example of cyber security problem.

Table I: Cost table among A_1, A_2 and A_3.

A_1	A_2	(risk, surveillance)
no scan	no scan	(12,0)
no scan	scan	(10,3)
scan	no scan	(7,1)
scan	scan	(5,2)
A_2	A_3	(risk, surveillance)
scan	scan	(0,1)
scan	no scan	(2,1)
no scan	scan	(0,2)
no scan	no scan	(2,0)
A_1	A_3	(risk, surveillance)
no scan	scan	(0,1)
no scan	no scan	(3,2)
scan	scan	(1,0)
scan	no scan	(1,0)

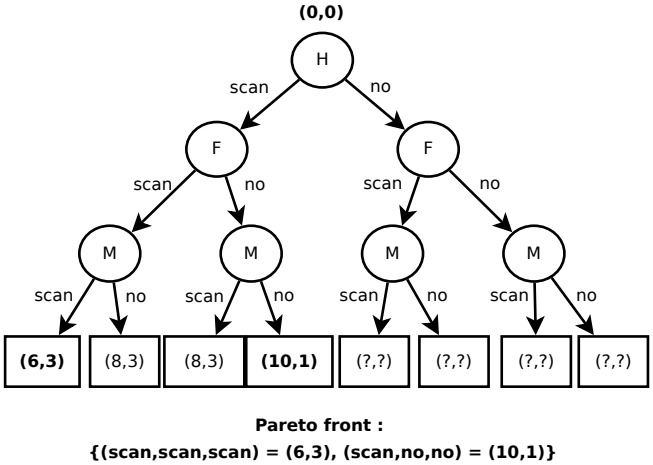
decentralized model. In this model, variables and constraints are distributed among agents. Since there exists no single agent which maintains all informations, it is resilient against intensive cyber attacks. Furthermore, since each agent shares the information locally, it can protect its own privacy.

B. Algorithm

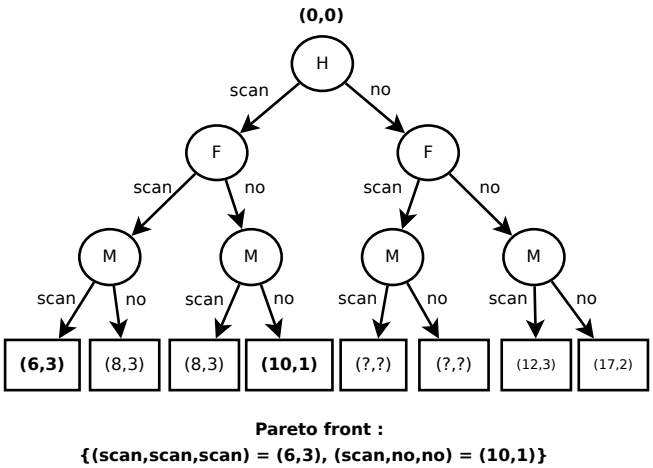
We introduce a novel algorithm called Branch and Bound search algorithm (BnB) for solving a cyber security problem. This algorithm utilizes a branch and bound technique and a depth-first search strategy, which are well-known and widely used for solving an optimization problem. The BnB can find all trade-off solutions. The advantage of this algorithm is that agents can easily switch/change their decisions in an emergency, since they know all trade-off solutions. Thus, we consider that providing all trade-off solutions is more resilient than solving one trade-off solution. But, it takes a lot of time when we solve large scale problem instances.

Figure 2 shows the search tree of Figure 1. Each node (H, F, M) represents a variable of agents A_1, A_2 and A_3, and each edge corresponds to the decision of each agent, e.g., when A_1 decides to scan, we go leftdown and rightdown otherwise. We call a decision of all agents as a path and each leaf node shows a cost vector obtained by each path, e.g., when all agents decide to scan, the path is $\{(H, scan)$, $(F, scan)$, $(M, scan)\}$ and the obtained cost vector is $(6, 3)$.

We describe the procedure of BnB using the Figure 2. The process of BnB in the left subtree (Step 1) is as follows. Let



(a) Step 1

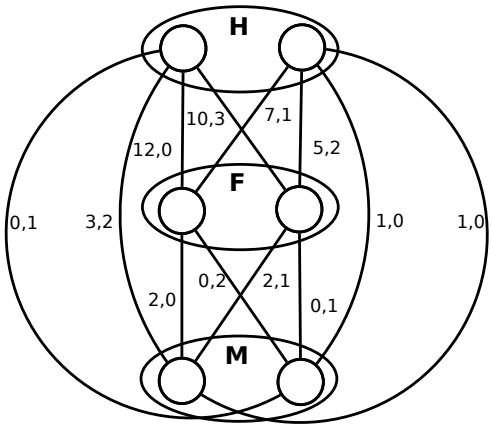


(b) Step 2

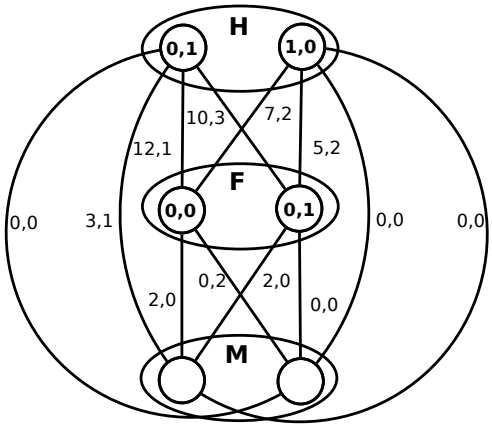
Figure 2: Example of BnB. Step 1 shows the search process of BnB in the left subtree and Step 2 is for the right subtree.

P be set of trade-of solutions. (i) It searches $\{(H, scan)$, $(F, scan)$, $(M, scan)\}$ and we add the obtained cost vector $(6, 3)$ in P. (ii) It searches $\{(H, scan)$, $(F, scan)$, $(M, no)\}$. Since the obtained cost vector $(8, 3)$ is dominated by $(6, 3)$, we don't add it in P. (iii) It searches $\{(H, scan)$, (F, no), $(M, scan)\}$. The obtained cost vector is $(8, 3)$. We don't add it in P. (iv) It searches $\{(H, scan)$, (F, no), $(M, no)\}$. Since the obtained cost vector $(10, 1)$ is not dominated by $(6, 3)$, and also does not dominate $(6, 3)$, we add it in P.

The process of BnB in the right subtree (Step 2) is as follows. (i) It searches $\{(H, no)$, $(F, scan)\}$. The obtained cost vector by this decision is $(10, 3)$ which is already dominated by $(6, 3)$. Then, BnB stops to search, i.e., it does not search $\{(H, no)$, $(F, scan)$, $(M, scan)\}$ and $\{(H, no)$, $(F, scan)$, $(M, no)\}$. (ii) It searches $\{(H, no)$, $(F, no)\}$. Since the obtained cost vector $(12, 0)$ is not dominated by $(6, 3)$ and $(10, 1)$, it continues to search $\{(H, no)$, (F, no),

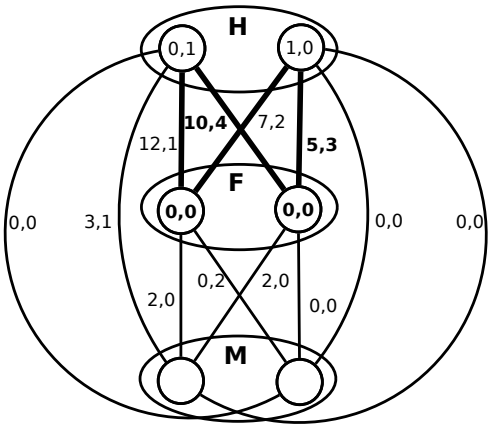


(a) Step 1

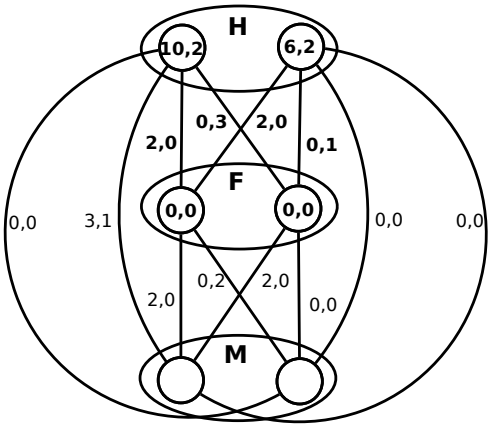


(b) Step 2

Figure 3: Example of Soft Arc Consistency.



(a) Step 3



(b) Step 4

Figure 4: Example of Soft Arc Consistency.

$(M, scan)\}$. The obtained cost vector is $(12, 3)$ which is dominated by $(6, 3)$ and $(10, 1)$. We don't add it in P. (iii) It searches $\{(H, no)$, (F, no), $(M, no)\}$. The obtained cost vector $(17, 2)$ is dominated by $(10, 1)$. We don't add it in P. Finally, BnB finds the Pareto optimal decisions $\{\{(H, scan)$, $(F, scan)$, $(M, scan)\}$, $\{(H, scan)$, (F, no), $(M, no)\}\}$ and the obtained trade-off solutions are $(6, 3)$ and $(10, 1)$.

Furthermore, we propose the extension of BnB which utilizes a preprocessing technique called soft Arc Consistency (softAC). The softAC is a well-known preprocessing technique which transforms a constraint optimization problem into a simplified problem that can be solved efficiently. This extended algorithm can find all trade-off solutions like BnB.

We show the process of soft arc consistency using the running example in Figure3 and 4. H, F and M represent variables of A_1, A_2 and A_3, and the left/right node represents $no\ scan$ / $scan$, respectively. The label of each edge shows the cost vector obtained by the decision of each agent, e.g., the edge between H and F (left nodes) is labeled by cost vector $(12, 0)$ which is obtained by $\{(H, no\ scan)$, $(F, no\ scan)\}$ (see in Table I). Step 1 is an initial state.

The softAC processes bottom-up, which starts from the leaves and propagates upwards through edges, Specifically, it propagates minimal value for each objective from M to H. In Step 2, when F decides $no\ scan$ (left node), the minimal cost for objective 1, i.e., risk value, is zero whatever M decides. The minimal cost for objective 2, i.e., surveillance value, is also zero. In case F decides $scan$ (right node), the minimal cost for objective 1 is zero whatever M decides. The minimal cost for objective 2 is one. Then, M sends F minimal cost vectors $(0, 0)$ and $(0, 1)$. F knows that he/she needs at least $(0, 0)$ when he/she decides $no\ scan$ and $(0, 1)$ otherwise. Similarly, M sends H minimal cost vectors $(0, 1)$ and $(1, 0)$. Then, we remove minimal cost vectors from the corresponding edges, e.g., the remaining cost vector for the edge between left nodes of H and M is $(3, 2)$-$(0, 1)$=$(3, 1)$.

In Step 3, the softAC propagates minimal value for each objective from F to H. Finally, in Step 4, when H decides $no\ scan$, the minimal cost vector is $(10, 2)$ and $(6, 2)$ otherwise, that is, in case H decides $no\ scan$, the risk and surveillance values are at least ten and two, whatever the

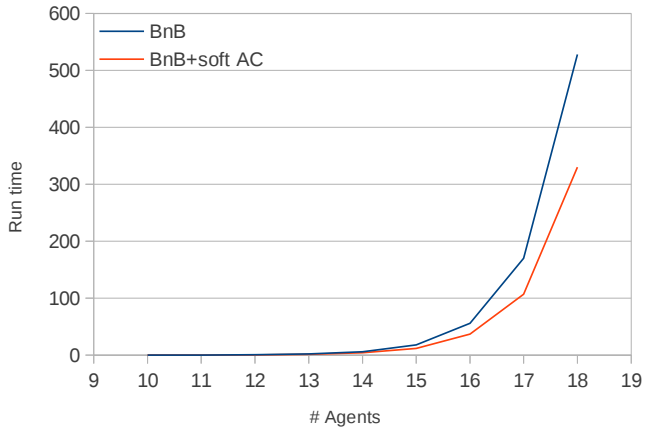


Figure 5: Run time of BnB and BnB+softAC for complete graphs, varying the number of agents.

Table II: Results of BnB and BnB+softAC.

# Agents	# solutions	# Messages	Run Time
10	55	44 000 30 000	0,08 0,06
11	63	120 000 73 000	0,23 0,17
12	85	340 000 200 000	0,68 0,50
13	101	900 000 520 000	1,98 1,41
14	120	2 500 000 1 400 000	6,05 4,19
15	143	7 100 000 3 900 000	18 12
16	172	19 900 000 10 800 000	56 37
17	196	55 400 000 28 600 400	170 107
18	238	155 000 000 80 000 000	528 330

other agents decide. When H decides $scan$, the risk and surveillance values are at least six and two.

The BnB+softAC searches trade-off solutions efficiently by using the cost vector obtained by siftAC as lower bound. In Figure 2 for Step 2, when H decides $no\ scan$, he/she knows the lower bound $(10, 2)$ which is obtained by softAC in preprocessing. This cost vector is already dominated by $(10, 1)$ that is computed in Step 1. Thus, BnB+softAC can prune the search space. We can expect that BnB+softAC solves cyber security problems faster than BnB.

V. Experimental evaluation

In this section, we examine the run time of our algorithms in cyber security problems with following problem instances [1]. We assume that each agent is a company. The number of objectives is three, i.e., risk, surveillance and cost. The domain size of each variable is three, i.e., $all\ scan$, $partial\ scan$, $no\ scan$. For each objective, we choose the value uniformly at random from the range [0,100]. Each data point in a graph represents an average of 100 problem instances. We evaluate our algorithms in most complex graphs. For each objective, we generate the same complete graph, i.e., each agent has constraints with all other agents.

Figure 5 represents the run time in BnB and BnB+softAC for complete graphs varying the number of agents/nodes. The x axis represents the number of agents and y axis shows run time. Table II shows the detailed results where $\#\ solutions$ is the number of trade-off solutions and $\#\ Messages$ is the number of messages sent among agents. The first line represents the results for BnB and the second line is for BnB+softAC. When the number of agents is ten, both algorithms can solve cyber security problems in less than 0.1s. However, in case the number of agents is 18, the run time is 528s in BnB and 330s in BnB+softAC. We can see that the run time of BnB and BnB+softAC increases, when the number of agents increases. This is because the number of trade-off solutions is exponential in the number of agents in the worst case. In Table II, when the number of agents is 18, the number of trade-off solutions is approximately four times larger than that for 10 agents. Furthermore, BnB+softAC outperforms the BnB. When the number of agents is 18, the run time of BnB+softAC is approximately 37% faster compared to that of BnB. Also, the number of sent messages reduces approximately 48%.

In summary, these experimental results reveal that our algorithms can solve cyber security problems quickly, e.g., BnB+softAC can provide all trade-off solutions in less than 330 seconds. However, these complete algorithms are not scalable. It is important to consider fast but incomplete algorithms for large-scale applications, since the number of trade-off solutions is exponential in the number of agents.

It is important to develop an algorithm that can find trade-off solutions quickly. For example, if we have a cyber attack, we need to switch our decision from a normal mode to urgent mode. Since BnB+softAC solves all trade-off solutions, we can change the current solution quickly. Thus, we consider that our proposed algorithms are resilient.

VI. Related Work

A *Multi-Objective Distributed Constraint Optimization Problem* (MO-DCOP) [7] is the extension of mono-objective *Distributed Constraint Optimization Problem* (DCOP) [13] which can formalize various applications related to multi-agent cooperation. A DCOP consists of a set of agents, each of which needs to decide the assignment of its variables

[1]We implemented BnB and BnB+softAC in C++ and carried out all experiments on 8 core running at 2.3GHz with 4GB of RAM.

so that the sum of the resulting costs is minimized. An MO-DCOP is a DCOP which involves multiple criteria. The representative application problem for MO-DCOPs is a wireless network of unmanned aerial vehicles (UAVs) [15].

The Bounded Multi-Objective Max-Sum algorithm (B-MOMS) [7] is the first (approximate) algorithm for MO-DCOPs. Compared to B-MOMS, our algorithms (BnB and BnB+softAC) are complete algorithms which can guarantee to find all trade-off solutions. The Pseudo-tree based solver [12] is a complete algorithm for MO-DCOPs. The BnB is quite similar to this algorithm. The main difference between the pseudo-tree based solver and BnB+softAC is that our algorithm utilizes a preprocessing technique. The BnB is similar to Multi-objective AND/OR Branch-and-Bound search algorithm (MO-AOBB) [11] which is a complete algorithm for solving a Multi-Objective Constraint Optimization Problem (MO-COP). Compared to MO-AOBB, BnB is an MO-DCOP algorithm. Furthermore, compared to evolutionary algorithms [2], [6], the advantage of our algorithms is that we can guarantee to find trade-off solutions.

VII. Conclusion

In this paper, we introduced a new presentation of cyber security problems and developed a novel algorithm for solving a cyber security problem. In the experiments, we evaluate our algorithms and showed that BnB+AC can solve cyber security problem quickly. There are several important future works. The first is to apply our algorithm on real cyber security problems. In this paper, we used the assumptive variables for calculating trade-offs. But we can collect and analyze the real consumer acceptance data by the means of social investigation and online questionnaires. Especially, the algorithm to obtain the social consensus related to a complex trade-off must be a powerful way in case of emergency, which changes consumer acceptance for trade-offs between privacy, security and cost dramatically. Designing the questionnaires to be able to capture such type of changing and introducing the result data into our algorithm has the highest priority. The second is to develop a novel algorithm which can find diverse solutions. Since the number of trade-off solutions is exponential in the worst case, it is intractable to solve all trade-off solutions in large scale problem instances. We consider to develop an algorithm which can switch to solve the trade-off solutions according to the user's requirement. Such algorithm is necessary, when we solve a large scale problem in an emergency.

Acknowledgment

This research is supported by grant for the Systems Resilience project from the Transdisciplinary Research Integration Center in Japan.

References

[1] F. Bignami. Privacy and law enforcement in the european union: the data retention directive. *Chicago Journal of International Law*, 8:233–255, 2007.

[2] K. Bringmann, T. Friedrich, F. Neumann, and M. Wagner. Approximation-guided evolutionary multi-objective optimization. In *Proceedings of the 22nd International Joint Conference on Artificial Intelligence*, pages 1198–1203, 2011.

[3] E. Commission. Evaluation report on the data retention directive. *COM(2011) 225 final*, 2011.

[4] S. M. Condron. Getting it right: Protecting american critical infrastructure in cyberspace. *Harvard Journal of Law Technology*, 20(2):403–422, 2007.

[5] K. de Vries. Proportionality overrides unlimited surveillance the german constitutional court judgment on data retention. *CEPS Papers in Liberty and Security in Europe*, 2010.

[6] K. Deb, S. Agrawal, A. Pratap, and T. Meyarivan. A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE Trans. Evolutionary Computation*, 6(2):182–197, 2002.

[7] F. M. D. Fave, R. Stranders, A. Rogers, and N. R. Jennings. Bounded decentralised coordination over multiple objectives. In *Proceedings of the 10th International Conference on Autonomous Agents and Multiagent Systems*, pages 371–378, 2011.

[8] C. Fuchs. Implications of deep packet inspection (dpi) internet surveillance for society. *The Privacy Security Research Paper Series*, (1), 2012.

[9] C. Hayes and J. Kesan. At war over cispa: Towards a reasonable balance between privacy and security. *llinois Program in Law, Behavior and Social Science Paper No. LBSS13-04*, 13:85–133, 2012.

[10] S. Herzog. Revisiting the estonian cyberattacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2):49–60, 2011.

[11] R. Marinescu. Exploiting problem decomposition in multi-objective constraint optimization. In *Proceedings of the 15th International Conference on Principles and Practice of Constraint Programming*, pages 592–607, 2009.

[12] T. Matsui, M. Silaghi, K. Hirayama, M. Yokoo, and H. Matsuo. Distributed search method with bounded cost vectors on multiple objective dcops. In *Proceedings of the 15th International Conference on Principles and Practice of Multi-Agent Systems*, pages 137–152, 2012.

[13] P. Modi, W.-M. Shen, M. Tambe, and M. Yokoo. ADOPT: asynchronous distributed constraint optimization with quality guarantees. *Artificial Intelligence*, 161(1-2):149–180, 2005.

[14] G. T. Nojeim. Cybersecurity and freedom on the internet. *Journal of National Security Law Policy*, 4(1):119–137, 2010.

[15] A. Sivakumar and C. K.-Y. Tan. UAV swarm coordination using cooperative control for establishing a wireless communications backbone. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems*, pages 1157–1164, 2010.