Multi-objective Optimization for Computer Security and Privacy

Seyed Mahmood Hashemi, Jingsha He and Alireza Ebrahimi Basabi
(Corresponding author: Seyed Mahmood Hashemi)
School of Software Engineering, Beijing University of Technology (BJUT)
Beijing Engineering Research Center for IoT Software and Systems
100 Ping Le Yuan, Chaoyang District, Beijing 100124, China
(Email: Hashei2138@yahoo.com)
(Received Feb. 20, 2016; revised and accepted Apr. 12 & May 7, 2016)

Abstract

There is need for a scheme to ensure the security and privacy of the administrator and users. Providing security is different to providing privacy, because their goals differ. Security is based on organization goals, but privacy is based on user goals. Providing security and privacy must be according to organization constraints. The most important constraints in any organization are economic issues. A useful scheme must consider all these requirements. In this paper, we present a scheme that provides security and privacy and considers various constraints. We model the problem as a multi-objective optimization problem.

Keywords: Multi-objective distributed constraint optimization problem, multi-objective optimization, PGP, single-objective distributed constraint problem

1 Introduction

Obviously, security is an important issue for any system. High levels of security for Internet communications usually restrict access to data to accredited individuals or organizations. Paradoxically, these security measures, themselves, invade personal privacy and organizational needs for confidentiality.

The main concepts for security are Confidentiality, Integrity and Availability (CIA). Privacy means protection of personal information. Of course, the official meaning of security and privacy are similar, but if we note the origins of each, we can understand the difference between them. Security is a high priority of an organization. In other words, governing bodies want to keep their information in a secure state, but privacy is an expectation of users. Protection of personal information (such as personal pages or mail, etc.) is attractive for users.

On the other hand, the major advantage of networking is user productivity. Thus any network system must provide access to assets for users. User productivity and costs of the implementation of a system are two points that play a major role in the success of a system in the real world. The objective of this paper is to provide a scheme for system developers with optimum levels of security, privacy, user productivity and cost.

In this paper, we present a Multi-objective Distributed Constraint Optimization Problem (MO-DCOP), which is an extension of the Single-Objective Distributed Constraint Problem (DCOP). In MO-DCOP, different aspects of a distributed system are optimized simultaneously. The presented model is decentralized, so there is not any agent needed to maintain information.

The rest of this paper is organized as follows: Section 2 is assigned to related works. In Section 3, we describe four concepts that are used in this paper: polling system, business intelligence, fuzzy systems and multi-objective optimization. Section 4 defines our problem. In Section 5, we present our proposed algorithm. Experimental results are presented in Section 6 and finally Section 7 presents the conclusion.

2 Related Works

The evolution of the current industrial context and the increase of competition pressure, has led companies to adopt new concepts of management [2]. The implementation of the most important part of the plan phase, consisting of the definition of an appropriate global management plan QSE (Quality, Security and Environment) has been proposed [3]. This implementation is based on the multi-objective influence diagrams (MIDs) [30]. The proposed approach has three phases: Plan phase, Do phase and Check & Art phase. The first phase gathers all quality, security and environmental objectives issued from the requirements, and then analyzes them. In this phase we can define a global management QSE plan. The second phase has the input of the global management plan QSE

and the corresponding global monitoring plan generated from the plan phase and will also implement the selected treatments. In the third phase, finalization of the process of integration occurs through measuring the effectiveness of different decisions. Neubauer et al. provide a structured and repeatable process that includes: defining evaluation criteria according to corporate requirements, strategy, assessing and/or refining the existing IT security infrastructure, identifying stakeholder preferences (risks, boundaries), determining the solution space of all efficient (Pareto optimal) safeguard portfolios, and interactively selecting the individually "best" safeguard portfolio [32]. This paper tries to combine different benefits and costs into one formula. This presents a problem because the authors do not present a multi-objective optimization problem. Kumar et al. focus on PGP (pretty good privacy) [26], which was shown by Zimmerman in 1991 to provide security with available cryptographic algorithms [37]. Algorithms are chosen according to the user requirements of time, cost and required security level. Kumar et al. answer the question: How do you choose appropriate algorithms, from the available pool, to suit the user requirements of time, cost and security? They assign a security level to an algorithm according to its performance [39] investigate security models, which consider risk assessment approaches to be applied for threat modelling, network hardening and risk analysis. Overall, security models can be classified based on the methodologies used to optimally invest into computer security. We have specified the following:

- Risk assessment models;
- Cost-benefit models;
- Game models;
- Multi-objective decision support models.

Cost-benefit analysis looks into intangible costs/returns and addresses the perspective of time. The simplicity of the frameworks can give suitable investment solutions for low risk investments. However, these methods do not consider uncertainty and give misleading indications for long-term investments. In [40], the risk assessment involves a calculation of risk in relation to financial returns, rather than the defined risk of possible losses related to degradation of information security. They demonstrate a novel approach of selecting security countermeasures with respect to both investment cost and the risk of possible degradation of CIA. Their security countermeasure is represented as a binary value. Also, they thought "security solutions can be classified based on the function they provide". The main challenge Information System (IS) managers face is to strike an appropriate balance between risk exposure and the opportunity to mitigate risk through investments in security. Thus, the authors of [23] propose a decision analytical approach, but the paper does not present a formula for multi-objective optimization. Service provisioning (SP) is defined as the set of interrelated decisions in order to select a service (by a server) to attend to a request (by a client). In [34], the results of the author's case study provides evidence in support of the notion that the use of imitation (recall) in DPSP's (dynamic provider of service provision) cipher selection process reduces its overheads dramatically. In paper [33], the authors introduce a novel presentation for cyber security problems using the formalization of a Multi-objective Distributed Constraint Optimization Problem (MO-DCOP). An MO-DCOP is the extension of a mono-objective Distributed Constraint Optimization Problem (DCOP) which is a fundamental problem that can formalize various applications related to multi-agent cooperation. They develop a novel algorithm called Branch and Bound search algorithm (BnB) for solving a cyber security problem. This algorithm utilizes the well-known and widely used branch and bound technique and depth-first search strategy and finds all trade-off solutions. The purpose of any risk analysis is providing decision makers with the best possible information about the probability of loss [5]. Behnia et al. compare several different approaches for risk analysis and declare the weakness and strength for each of them.

3 Preliminaries

Our scheme has different parts and we need to have specific science to solve the problem in each part. In this part, we describe things which are needed for the proposed algorithm.

3.1 Polling System

There is need for a system which can satisfy all stakeholders' opinion. We say stakeholder for anyone who has any role in developing a team. The polling system is an appropriate method for keeping votes [20].

The polling system consists of a source for the service and a number of queues for clients with a policy for assigning service to the client. For example, in Figure 1, $\lambda 1$, $\lambda_2, \cdots, \lambda_N$ are clients and $S_1, S_2, \cdots, S_N$ are assignment policies.

The polling system can be a system with time sharing and N terminals. In that system, the central computer votes to terminals based on their requirements for data. Data transfers from terminals to the central computer through a voting scheme. Default:

1) Processes enter into the queues with a Poisson distribution;
2) Clients are served during the time as a random variable;
3) After servicing to a queue, the server assigns to other queues with a switch-over time [27].

Common polling systems are [24, 43]:

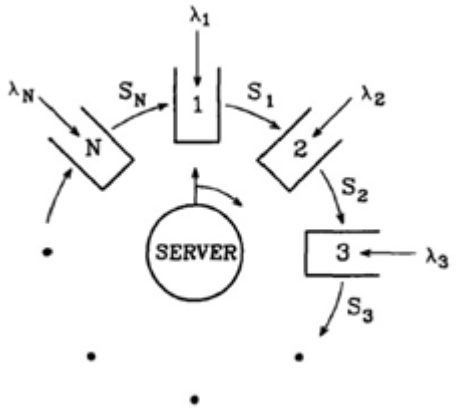

Figure 1: Polling system

Exhausted: Server is assigned to a queue for all clients in that queue.

Gated: Server is assigned to a queue with a specific time range.

Limited-1: Predefined clients which can give server.

Polling system has various applications.

Token Ring Networks: In a cyclic net, terminals need acceptance of the central computer [6].

Robotic Systems: A robotic system consists of a central robot and various inputs. For modelling this system, we can use the polling system where the robot is the server and the inputs are clients. Clients are set in queues based on their types.

Various Non-generic Computers and Communication Systems: In these systems, one processor serves to a particular type of task. A common way is to accumulate tasks into different types. In the model, tasks are clients and the processor is the server [28, 42].

Transportation (Automated Guide Vehicle): In these models, many vehicles must be carried in a narrow way. The polling system consists of automated vehicles with default paths. In this model, transportation transforms clients from various queues to specific destinations [17].

Stochastic Economic Lot Scheduling Problem (SELSP): This application is about producing by using a machine with limited capacity where the requirements produce stochastic [12, 13].

Health Care: An emergency in a hospital can be modelled with a polling system. Tasks are set in queues with an unlimited buffer.

Random Polling: The best examples for these models are distributed control systems. There is no central control, so deciding about the next terminal is done with polling.

There are some notes in the polling systems: stability, priority, structure for polling, definition of limitations and waiting time.

3.2 Business Intelligence

In the above part, we talked about the Polling System which allows us to utilize all stakeholders' opinions to improve the security of system, but on the other hand, there are users that want privacy. The balance between security and privacy is a challenging discussion. First of all, there is a need for a system which determines what level of privacy is needed [21].

Business Intelligence (BI) is a set of disciplines that include extracted data, combinations of data, the analysis and knowledge discovered which enables the system to comprehend the input/output environment [7, 9]. The aim of BI is to prepare a document for verification by the system, a prototype for deployment and obtaining a strategic and applicable knowledge base from a scientific view [44].

BI has five layers as shown in Figure 2. Also, BI helps developers to [16]:

Fast data processing: BI can access, select and modify any time. The speed is guaranteed.

Intelligent correlation analysis: BI uses mathematical models and declares scientific rules.

Multi-dimensional analysis: BI gets a combinational analysis in the format of products, brands and K, then constructs a multi-dimensional data structure.

BI uses various intelligent tools such as: tools to gather implicational data and extract business knowledge [8], and competing intelligent tools which try to get data from competing environments [9]. Constructing a BI system includes the following steps [14]:

1) Planning and direction;
2) Gathering released information;
3) Gathering resources from users;
4) Analysis;
5) Report and inform.

There are two taxonomy types in BI: one-dimensional data and two-dimensional data [29]. A list of results from hyperlinks belongs to one-dimensional data. Tree data and networking data belong to two-dimensional data. Two-dimensional data allows people to search based on human abilities.

Special text is displayed in the BI system within three phases [36]. Firstly, according to users' attractive, necessary characteristics of text. This phase can be named

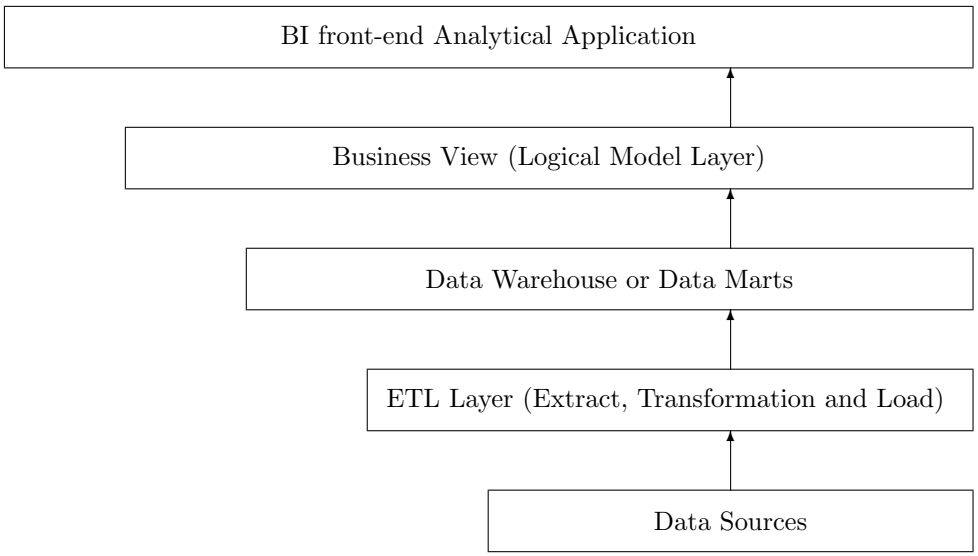

Figure 2: Layers of BI

'Analysis'. In this phase, some search techniques for the analysis of text in the network are used. These techniques have the responsibility to discover resources and patterns from the network [11]. In the second phase, which is named 'Algorithm', an applicable and flexible structure with clustering is constructed. Algorithms can be divided into two categories [22]: 1) hierarchical and 2) partitional. The final phase is 'visualization' where data is displayed to users. Visualization means display of coding data in a special format as understanding with human eyes.

3.3 Fuzzy Systems

Fuzzy systems are knowledge-based systems or rule-based systems [41]. A fuzzy system consists of a number of rules. Each rule relates input(s) to output(s). Input(s) and output(s) in fuzzy systems are recognized in fuzzy sets. Let a system with uncertainty have the input-output relation $y = f_s(x)$, where $y \in R$, and $y \in R^{nX}$. A fuzzy system represents the knowledge related to inputs and outputs by nC fuzzy rules $R_1, \cdots, R_C$ which are expressed in the form

$$R_i: \text{ If } (x_{k,1} isr A_{i,1}) \text{ and } (x_k, nX) \text{ then } (y^*_{k,i} isr B_i), \quad (1)$$

where $y_k = f_s(x_k)$ is an observation vector (x_k, y_k) of the system; $x_{k,j}$ is the j^{th} variable of x_k; $A_{i,j}$ is the membership function of the fuzzy set for the j^{th} variable in the i^{th} rule, which determines a fuzzy number for the j^{th} variable of input space; $y^*_{k,i}$ is the estimate of $y_k = f_s(x_k)$ by R_i; The operator "and" denotes the t-norm operation between two membership values; and "isr" denotes the belonging of an object into a fuzzy set. An important contribution of fuzzy systems theory is that it provides a systematic procedure for transforming a knowledge base into a non-linear mapping.

The objective of a non-linear mapping is producing output(s) with input(s). Mapping is done when there is a relation. Producing a relation (formula) from rules is the role of the Inference Engine. Researchers have proposed many inference engines and each of them has their own features (strengths/weaknesses).

A fuzzy system has two advantages. First, we can combine different votes or opinions with the formula of the inference engine. Second, the use of multiple fuzzy sets allows the proposed algorithm to be strong against changes.

3.4 Multi-objective Optimization

MOO is necessary when multiple cost functions are considered in the same problem. The aim of MOO is tuning the decision variables to satisfy all objective functions F_i to an optimum value. This class of problems is modelled by Equation (2).

$$\begin{aligned} &\text{Optimize } [F_1(X), \cdots, F_k(X)] \\ &\text{Subject to } g_i(X) \leq 0, h_j(X) = 0; \\ &\quad i = 1, \cdots, m; j = 1, \cdots, p \end{aligned} \quad (2)$$

where k is the number of objective functions; X is the decision vector; m is the number of inequality constraints and p is the number of equality constraints.

This goal causes a difference between these algorithms and their ancestor Single-Objective Optimization, which is based on the concept of best, while the multi-objective optimization uses the concept of dominance. Dominance is defined in [10]:

$$\begin{aligned} &\overrightarrow{U} = (u_1, \cdots, u_k) \prec \overrightarrow{V} = (v_1, \cdots, v_k) \\ &iff \ \ \forall i\{1, \cdots, k\} u_i \leq v_i, \exists j\{1, \cdots, k\} u_j < v_j. \end{aligned} \quad (3)$$

In words, a vector $\overrightarrow{U}$ of variables dominates another vector of variables $\overrightarrow{V}$ if and only if $\overrightarrow{U}$ can reach an op-

timal value for some criteria without causing a simultaneous non-optimal value for at least one criterion. If two vectors cannot dominate each other, they are called non-dominated vectors.

4 Problem

The phenomenon of networks has advantages and also disadvantages for our life. The main advantage of a network is User Productivity. A network provides access to information for users. On the other hand, there are two concepts which are related to the Free Flow of Information. Users expect Privacy. Governments want Security. Both privacy and security are against the free flow of information. Moreover, producing any module in a software system produces a cost. There are four significant criteria for network systems: user productivity, privacy, security and economics. We think any network system will fail without considering the follow threads:

- Any network system which does not have User Productivity will not be welcome by users.
- Users are interested in systems which protect their information.
- Providing confidentiality, integrity and availability is important for any organization.
- Financial resources of any organization are limited, so they cannot support any software.

There needs to be a system with different components. Since the system is designed for a distributed environment, components can be done in separated places and communicate to each other in general, but we show this in one figure for simplicity.

There is a directional and acyclic graph $G = (V, E)$, where V is a set of nodes that represents computer systems and E is the set of edges that represent the connection between nodes (Table 1). This graph is a popular approach to model the network. Let there be 10 nodes as in Table 1 which represents the graph, where 0 represents that there is no connection between two nodes (in column and row) and 1 vice versa.

Each edge has a number of features:

Security: represents the degree of security. All members of the developing team vote to all paths according their experience of security.

Privacy: represents the degree of privacy. Users, based on their experiences recognize the degree of privacy.

User productivity: represents how much users can have access to their necessary information.

Cost: represents how much cost is needed for creating and maintenance a connection. There are 5 fuzzy sets to recognize the cost (See Figure 3).

Table 1: Graph for model of the network

0	1	1	1	0	0	1	1	1	0
1	0	1	0	0	1	1	0	0	0
1	0	0	0	1	1	0	0	1	1
0	1	1	0	1	0	0	1	1	0
0	1	0	1	0	1	1	0	0	1
0	0	0	0	1	0	1	0	1	1
1	0	1	1	0	1	0	1	1	0
1	0	1	1	0	1	1	0	0	1
0	1	0	0	1	0	1	1	0	1
1	1	0	0	1	0	0	1	1	0

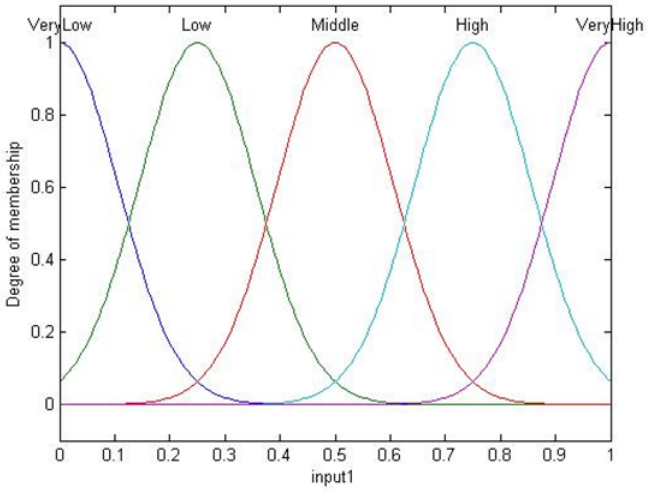

Figure 3: Fuzzy sets for cost

The main goal of this paper is to present an approach that finds an optimum path (which is created with the connection of a number of paths). Since there are many objectives at issue, we have to use multi-objectives or multi-task methods. Our research must have the following characteristics:

- Research must be based on a probabilistic view, because the behavior of the network (environment) is not predictable.
- Research must follow a bottom-up approach. This approach recognizes that the lack of security is the result of the interaction of complex nodes. In contrast, a top-down approach focuses on the whole of the system. A bottom-up approach is better than a top-down approach for presenting attack, because attack is performed on the interaction between nodes and not the whole of the system.
- Research must be based on an analysis of threat sources. Schneier states that the term "security" is meaningless if the question "secure from whom?" is not addressed [35].
- Research must be based on the grouping decision. The opinion of all corporate team members in developing the final decision needs to be sought.

This research has two major elements. One of them is a Polling System and another one is a Business Intelligence System. The polling system allows us to combine all stakeholders' opinion, so security will be became the responsibility of all system stakeholders and not only the administrator. However, providing privacy needs recognition of requirements. Actually the best way for recognition is indirection. Business Intelligence is a suitable approach to recognize user requirements.

5 Proposed Algorithm

In the proposed scheme we must consider all notices which are mentioned in the "problem" section. Firstly, there is need for a system to counter security. We propose a Polling System for this goal (See Figure 4). In our polling system, queues are used as a number for the types of stakeholders. Each stakeholder can vote in its queue. Since the stakeholder is a role, someone may vote in several queues. The core of the polling system is a Fuzzy System. We use a Product Inference Engine to combine the votes from queues,

$$f(x) = \frac{\sum_{l=1}^{M} \bar{y}^l (\prod_{(l=1)}^{n} \mu_{A_i^l}(x_i))}{\sum_{l=1}^{M} (\prod_{(l=1)}^{n} \mu_{A_i^l}(x_i))} \quad (4)$$

where $f(x)$ is output; M the number of rules; n the number of rules incipience and μ is the membership degree for input variable x in the fuzzy set A. In the proposed system, the input variable is the vote and the rule is a queue. The output is the final result from the polling system.

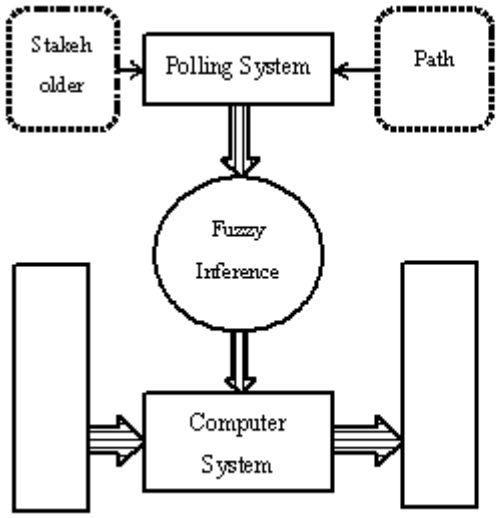

Figure 4: Proposed polling system

Secondly, there is need for a system to counter user productivity. We propose a Business Intelligence (BI) system for this goal. BI allows us to know the leaning of each user indirectly. Actually, the performance of BI is deeply dependent on the approach of information gathering. BI produces a number, with its fuzzy system as a result.

Finally, there is need for a multi-objective optimization formula to model the whole of the scheme. We propose the following optimization model for our problem:

$$\begin{aligned} &\text{Optimize } S, P, UP, C \\ &\text{Subject to: } C \leq LP, S \geq DS, P \geq DP, \end{aligned} \quad (5)$$

where S is security; P is privacy; UP is user productivity and C represents the total cost. Total cost must be less than or equal to the limited cost. Security and privacy must be greater than or equal to the default level of security and the default level of privacy, respectively. In other words, the model formula says that all parameters of a computer system (security, privacy, user productivity and cost) must be optimized simultaneously. Optimization means maximization of security, privacy and user productivity and minimization of cost. In this paper, we use tree algorithms to solve the multi-objective Problem (5):

1) Multi-objective simulated annealing;
2) Multi-objective genetic algorithm;
3) Multi-objective bee colony algorithm.

5.1 Multi-objective Simulated Annealing (AMOSA)

The basic concept in simulated annealing is the evolution of the solution by simulating decreasing temperature (tmp) in the material, where a higher temperature

denotes greater modification of the solution in a generation. If the temperature of a hot material decreases very quickly, its internal structure may change and the material could become hard and brittle. Decreasing the temperature slowly yields higher homogeneity and less brittle material. Evolution of the solution occurs at specific temperature profiles. In the first few iterations, a diverse set of initial solutions for the problem are produced at a higher temperature. These solutions are then evolved while the temperature decreases to obtain their local optima. In a multi-objective situation, there are non-dominated solutions that must be kept in the archive as candidates for the optimal solution.

AMOSA was proposed in [4]. During the execution of the AMOSA algorithm, two solutions exist: the current-so and new-so. Comparison of the two solutions yields one of three states: 1) current-so dominates new-so, 2) current-so and new-so are non-dominated with respect to each other, and 3) new-so dominates current-so.

If new-so is dominated by current-so, there may be solutions in the archive that dominate new-so. New-so is accepted into the archive based on the probability:

$$p = \frac{1}{1 + exp(\triangle \times tmp)} \tag{6}$$

where $\triangle$ is the difference between new-so and the other solutions that dominate new-so. If there are A solutions in the archive,

$$\triangle = \frac{\sum_{i=1}^{A} \triangle_i + \triangle}{A + 1} \tag{7}$$

Solutions can escape from the local optima and reach the neighborhood of the global optima by this probable acceptance. If the new-so is dominated by some solutions in the archive, Equation (7) is modified to:

$$\triangle = \frac{\sum_{i=1}^{A} \triangle_i}{A} \tag{8}$$

If the new-so is not dominated by any of the members in the archive, it is set to the current-so and is added to the archive. If the new-so dominates some solutions in the archive, it is set to the current-so and is added to the archive. In addition, any solutions in the archive that are dominated by the new-so, are removed. If the new-so is dominated by some solutions in the archive, Equation (6) is changed to:

$$p = \frac{1}{1 + exp(-\triangle)} \tag{9}$$

where $\triangle$ is the minimum difference between the new-so and the dominating solutions in the archive. The new-so is set to the current-so with Probability (9). If the new-so is not dominated by any of the solutions in the archive, it is set to the current-so and added to the archive. If the new-so dominates some solutions in the archive, it is set to the current-so and added to the archive, while all dominated solutions are removed from the archive.

5.2 Multi-objective Genetic Algorithm (MOGA)

The MOGA is based on a single-objective genetic algorithm [15, 25, 19], and comprises various stages. In the first stage, a population of individuals (chromosomes) is created. The number of individuals in the population (pop-size) is determined by the programmer. Each individual contains certain fields, where the number of fields in an individual is equal to the number of variables in the problem, which must be optimum. Each individual has the potential to reach an optimum point, at which optimal values are set in the corresponding fields in the individual. In the first stage of MOGA, all individuals in the population are initialized with random values. The algorithm runs until the stopping conditions are met. There are three types of stopping conditions. The first of these is special values; when the values of individuals are equal to the default values, the algorithm terminates. The second type of stopping condition occurs when the values of individuals no longer change. The last type of stopping condition is the number of iterations. When the number of iterations of the algorithm reaches the given threshold value (max-generation), the algorithm terminates.

Given that MOGA is an evolutionary algorithm, it is executed for a number of iterations, where each iteration of MOGA is called a generation, inspired by Darwinian evolutionary theory. The programmer can control the evolutionary nature of MOGA using the number of generations. This means that despite the deterministic optimization method, which is controlled by the number of inputs, the programmer can vary the number of generations. In the first generation, individuals are initialized with random values. The values of individuals are changed in each generation using two operators: mutation and cross-over. In mutation, one field of an individual is changed to a different value. There are a number of different methods for mutation, which describe the quality of the altered values. In cross-over, two individuals are combined to produce a new individual. After the genetic algorithm operators (mutation and cross-over) have been applied, several individuals are selected for the next generation. Selection is done stochastically according to the fitness of the individual.

The goal of the optimization algorithm is to find the optimal point. Optimal points can be divided into two categories: local optima and global optima. A local optimum can be any point that is the optimum of all points within a limited range, while a global optimum is a point that is the optimum of all points in an unlimited range. Because deterministic optimization methods compare the current point with points in a limited range, they may be trapped in a local optimum. The stochastic feature of MOGA allows the algorithm to escape from local optima and achieve the global optimum.

Based on the discussion above, MOGA has two advantages: the programmer can control the execution time and the algorithm has the potential to achieve a global

optimum point.

MOGA finds an optimum point according to the Pareto set; in other words, a point is optimum if it is not dominated by other points. Indeed, the Pareto principle allows a number of objectives to become optimum simultaneously. Each individual is checked for its domination in the population. Individual i is allocated a rank equal to one plus the number of individuals, n_i, dominating individual i. Once ranking has been completed, a raw fitness is assigned to each individual based on its rank using a linear mapping function.

$$F_i = N - \sum_{k=1}^{r_i-1} \mu(k) - 0.5(\mu(r_i - 1)) \tag{10}$$

where μ denotes the numbers of individuals in the rank. MOGA incorporates niching among individuals in each rank. The niche count with σ_{share} is found first. The distance metric is computed with the objective function values. Thus, the normalized distance between any two individuals i and j in a particular rank is calculated as:

$$d_{ij} = \sqrt{\sum_{k=1}^{M} (\frac{f_k^{(i)} - f_k^{(j)}}{f_k^{max} - f_k^{min}})^2} \tag{11}$$

The distance is computed for each pair of individuals. Therefore, the niche count is calculated by summing the shared function values:

$$SH(d_{ij}) = \begin{cases} 1 - \frac{d_{ij}}{\sigma_{share}}, & \text{if } d_{ij} < \sigma_{share} \\ 0, & \text{otherwise} \end{cases} \tag{12}$$

The shared fitness is calculated as $F_i' = F_i / nc_i$, $nc_i = \sum d_{ij}$. Shared fitness is used as a basis for stochastically selecting individuals for the next generation. The above process continues until the stopping condition is satisfied. When the algorithm terminates, the remaining individuals represent the optimum.

5.3 Multi-objective Bee Colony (MOBC)

The foraging behavior of bees is characterized by various steps that are used in optimization. The first step is called the Waggle Dance, which is used by bees to convey information to other bees about the direction, distance, and quality of a food source. Upon finding a food source, a bee begins to dance in a figure of eight pattern. The second step in the foraging behavior is when follower bees that were waiting inside the hive, follow the dancer bee. The number of follower bees assigned to a path is directly proportional to the quality of the path. In the third step, these bees return to the hive. More bees are recruited to the source of the food if the path is still good enough. Bees stop collecting poor-quality food and adjust their strategy for finding food based on information about the location of good-quality food.

Foraging behavior can be used for optimization when it is divided into two phases. The first phase consists of path construction. In this phase, a bee explores the entire food source, but with the exploration limited by constraints. When a bee does a tour (which includes all possible variables), it performs the Waggle Dance. Other bees use this information, expressed as:

$$Pf_i = \frac{1}{L_i} \tag{13}$$

where Pf_i is the profitability of a bee_i and L_i is its tour. If a colony has n bees, the bee colony's average profitability is given by:

$$\begin{aligned} Pf_{colony} &= \frac{1}{n} \sum_{i=1}^{n} Pf_i \\ &= \frac{1}{n} \sum_{i=1}^{n} \frac{1}{L_i} \end{aligned} \tag{14}$$

The dance duration of any bee is given by:

$$D_i = K \times \frac{Pf_i}{Pf_{colony}} \tag{15}$$

where K is the profitability rating and is adjusted according to the lookup table given in Table 2.

Table 2: Lookup table for adjusting profitability

Profitability Rating	K_i
$Pf_i < 0.9Pf_{colony}$	0.60
$0.9Pf_{colony} < Pf_i < 0.95Pf_{colony}$	0.20
$0.95Pf_{colony} < Pf_i < 1.15Pf_{colony}$	0.02
$1.15Pf_{colony} < Pf_i$	0.00

The second phase of the bee algorithm consists of path reconstruction. In this phase, bees in the hive, having received information from the explorer bee, utilize the path. Bees use a transition rule for choosing the appropriate path with the probability denoted by $P_{ij}(t)$, which measures the possibility of moving from $step_i$ to $step_j$ at time t. In a multi-objective sense, the discussed path must be examined for dominance over other paths. Formula (9) takes into consideration the fitness of all paths:

$$\rho_{ij}(t) = \begin{cases} \lambda, & j \in F_i(t) \\ \frac{1-\lambda|F_i(t) \cap A_i(t)|}{|A_i(t)| - |F_i(t) \cap A_i(t)|}, & j \notin F_i(t) \end{cases} \tag{16}$$

where λ is the value (less than one) assigned to the preferred path; $|A_i(t)|$ is the number of allowed next steps, and $|F_i(t) \cap A_i(t)|$ is the number of preferred next steps [1, 18, 31, 38].

Now, we can examine the dominance of all paths, after which each path is classified as conforming to one of three situations: 1) dominates another path(s); 2) is dominated by another path, and 3) is not dominated by any other path.

Table 3: Properties of network

-	0.3, 0.2, 0.5, 0.8	0.4, 0.4, 0.5, 0.8	0.6, 0.7, 0.5, 0.8	-	-	0.1, 0.8, 0.6, 0.7	0.9, 0.7, 0.9, 0	0.2, 0.2, 0.4, 0.5	-
0.8, 0.8, 0.7, 0.9	-	0.3, 0.5, 0.5, 0.6	-	-	0.7, 0.6, 0.5, 0.4	0.7, 0.8, 0.4, 0.2	-	-	-
0.4, 0.3, 0.5, 0.7	-	-	-	0.9, 0.1, 0.8, 0.2	0.2, 0.3, 0.4, 0.5	-	-	0.4, 0.5, 0.7, 0.9	0.3, 0.6, 0.6, 0.8
-	0.7, 0.4, 0.9, 0.8	0.9, 0.3, 0.7, 0.8	-	0.8, 0.7, 0.6, 0.5	-	-	0.6, 0.9, 0.7, 0.3	0.8, 0.2, 0.1, 0.1	-
-	0.8, 0.2, 0.8, 0.3	-	0.9, 0.7, 0.6, 0.8	-	0.9, 0.1, 0.7, 0.3	0.6, 0.7, 0.9, 0.4	-	-	0.8, 0.8, 0.5, 0.5
-	-	-	-	0.7, 0.8, 0.8, 0.9	-	0.9, 0.2, 0.3, 0.1	-	0.8, 0.9, 0.8, 0.8	0.9, 0.4, 0.3, 0.9
0.2, 0.3, 0.3, 0.3	-	0.4, 0.4, 0.5, 0.3	0.8, 0.4, 0.7, 0.6	-	0.7, 0.8, 0.9, 0.1	-	0.4, 0.2, 0.9, 0.7	0.3, 0.5, 0.6, 0.8	-
0.8, 0.4, 0.2, 0.7	-	0.2, 0.5, 0.8, 0.4	0.8, 0.4, 0.3, 0.1	-	0.6, 0.4, 0.8, 0.3	0.7, 0.5, 0.3, 0.2	-	-	0.9, 0.6, 0.4, 0.2
-	0.2, 0.6, 0.7, 0.7	-	-	0.3, 0.6, 0.7, 0.4	-	0.7, 0.5, 0.7, 0.9	0.8, 0.4, 0.3, 0.2	-	0.1, 0.4, 0.8, 0.2
0.9, 0.8, 0.4, 0.3	0.1, 0.4, 0.8, 0.3	-	-	0.5, 0.7, 0.7, 0.7	-	-	0.9, 0.7, 0.9, 0.8	0.6, 0.7, 0.3, 0.8	-

In the first situation, the path is stored in the archive. In the second situation, the path is destroyed, and in the third situation, the path is stored in the archive with the following probability:

$$P_{ij}(t) = \frac{[\rho_{ij}(t)]^{\alpha} \times [\frac{1}{d_{ij}}]^{\beta}}{\sum_{j \in A_i(t)} [\rho_{ij}(t)]^{\alpha} \times [\frac{1}{d_{ij}}]^{\beta}} \quad (17)$$

where d_{ij} is the distance between $step_i$ and $step_j$, α is a variable that influences the fitness, and β is a variable that influences the distance. A is a collection of all steps that can be reached from the previous step.

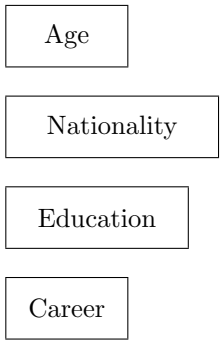

Figure 5: Proposed EI

6 Experimental Results

Let security and cost be set in [0,1] for each path. The value of security is determined by using a polling system, which allows stakeholders to give their opinions. The final result of the polling system is entered into a fuzzy system. In the fuzzy system the final value is produced with Equation (4).

However, there are two measures: User Productivity and Privacy. Both of them are related to the whole of the system (not for each selected path) and are set in [0,1]. User Productivity is determined with a Business Intelligence (BI) system. The performance of (BI) is fully dependent on indirect questions. The responsibility of BI is to mine the favorites of users from indirect questions. We focus on "indirect", because users do not usually like to state their favorite. Since this paper is just a proposal scheme, we prefer only four questions.

Suppose the qualities of system on the paths in Table 1, are shown in the following matrix (Table 3). Values in each cell represent "Security", "Privacy", "User Productivity" and "Cost" respectively.

We assume the range of values is [0,1]. This assumption does not limit the generalization. Suppose we want send a packet from node "1" to node "10" and $DS = 2$, $DP = 2$. The optimum values for this transmission based on the optimization algorithm, are represented in following table.

All of these algorithms are stochastic, so their result may be changed in different executions, but we can achieve a general outcome from a comparison of results.

Our research is different to previous works. For example, [33] focuses on the number of messages that are transferred between nodes, but our objectives is optimization of different system aspects simultaneously. Therefore comparison between presented work and other ones

Table 4: Final results

	Selected Path	Security	Privacy	User Productivity	Cost
AMOSA	$1 \to 2 \to 6 \to 10$	1.9	1.2	1.3	1.6
MOGA	$1 \to 3 \to 5 \to 10$	2.1	1.3	1.8	1.5
MOBC	$1 \to 7 \to 3 \to 9 \to 10$	1	2.1	2.6	2.1

is meaningless.

7 Conclusion

In this paper, we propose a scheme to model the network system in a real distributed environment according to security and privacy. Actually, security and privacy are critical concepts for all network systems, but in modelling we must consider their major parameters. In this paper, we recognize "security" and "privacy" based on their originality. Security is promoted by the head of an organization, but privacy is attractive for users. Indeed, users want free access to the assets of systems. Free access of users provides user productivity. Another important concept is that applying a security and privacy algorithm in real systems is an economic issue. We consider it as a "cost".

We optimize all major parameters of a network system (security, privacy, user productivity and cost) with three multi-objective optimization algorithms. AMOSA, MOGA and MOBC are used in this paper. Their results prove that the performances of AMOSA and MOGA are better that MOBC. The AMOSA algorithm can achieve a final result sooner that other algorithms, but the performance of MOGA is more stable.

Acknowledgments

The work in this paper has been supported by the National Natural Science Foundation of China (61272500), National High-tech R & D Program (863 Program) (2015AA017204) and the Beijing Natural Science Foundation (4142008).

References

[1] P. Agrawal, H. Kaur, D. Bhardwaj, "Analysis and synthesis of enhanced bee colony optimization with the traditional bee colony optimization to solve the traveling sales person problem," *International Journal of Computer & Technology*, vol. 2, no. 2, pp. 93–96, 2012.

[2] A. Badreddine, T. B. Romdhane, N. B. Amor, "A new process-based approach for implementing an integrated management system: Quality, security, environment," in *Proceedings of International Conference on Industrial Engineering (IMECS'09)*, pp. 1–6, Hong Kong, Mar. 2009.

[3] A. Badreddine, T. B. Romdhane, N. B. Amor, "A multi-objective risk management approach to implement an integrated management system: Quality, security, environment," in *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*, pp. 4728–4733, San Antonio, TX, USA, 2009.

[4] S. Bandyopadhyay, S. Saha, U. Maulik, K. Deb, "A simulated annealing-based multiobjective optimization algorithm: AMOSA," *IEEE Transactions on Evolutionary Computation*, vol. 12, no. 3, pp. 269–283, 2008.

[5] A. Behnia, R. A. Rashid, J. A. Chaudhry, "A survey of information security risk analysis methods," *Smart Computing Review*, vol. 2, no. 1, pp. 79–94, 2012.

[6] W. Bux, "Local-area subnetworks: a performance comparison," *IEEE Transaction on Communications*, vol. 29, no. 10, pp. 1465–1473, 1981.

[7] R. Carvalho, M. Ferreira, "Using information technology to support knowledge conversion process," in *Proceedings of the 13th WSEAS International Conference on Mathematical and Computational Methods in Science and Engineering*, pp. 176–1817, 2001.

[8] C. W. Choo, *The Knowing Organization*, Oxford University Press, 1998.

[9] W. Chung, W. Chen, J. F. Nunamaker, "Business Intelligence Explorer: A Knowledge Map Framework for Discovering Business Intelligence on the Web," in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, 2003.

[10] C. A. Coello, D. A. Van Veldhuizen, G. B. Lamont, *Evolutionary Algorithms for Solving Multi-objective Problems*, Springer, 2007.

[11] O. Etzioni, "The World Wide Web: Quagmire or Gold Mine?" *Communication of the ACM*, vol. 39, pp. 65–68, 1996.

[12] A. Federgruen, Z. Katalan, "The stochastic economic lot scheduling problem: cyclical base-stock policies with idle times," *Management Science*, vol. 44, pp. 989–1001, 1996.

[13] A. Federgruen, Z. Katalan, "Costumer waiting-time distributions under base-stock policies in single facility multi-item production systems," *Naval Research Logistics*, vol. 43, pp. 533–548, 1996.

[14] L. Flud, K. Sawka, J. Carmicheal, J. Kim, K. Hynes, *Intelligence Software Report 2002*, Cambridge, Flud & Company Inc., 2002.

[15] C. M. Fonseca, P. J. Fleming, "Genetic algorithm for multiobjective optimization: Formulation, discussion and generalization," in *Proceeding of 5th International Conference on Genetic Algorithms*, pp. 416–423, 1993.

[16] T. Gang, C. Kai, S. Bei, "The research & application of business intelligence system in retail industry," in *IEEE International Conference on Automation and Logistics*, pp. 87–91, 2008.

[17] D. Gupta, M. M. Srinivasan, "Polling systems with state-independent setup times," *Queueing Systems*, vol. 22, pp. 403–423, 1996.

[18] M. Gupta, G. Sharma, "An efficient modified artificial bee colony algorithm for job scheduling problem," *International Journal of Soft Computing and Engineering*, vol. 1, no. 6, pp. 303–315, 2012.

[19] A. Haidine, R. Lehnert, "Multi-case multi-objective simulated annealing (MC-MOSA): New approach to adopt simulated annealing to multi-objective optimization," *International Journal of Information Technology*, vol. 4, no. 3, pp. 197, 2008.

[20] S. M. Hashemi, J. He, "An approach for risk management of computer security base on polling system," in *The 16th IEEE International Conference on Communication Technology (ICCT'15)*, pp. 912–918, 2015.

[21] S. M. Hashemi, J. He, "BI-based approach for computer security," *The 3rd IEEE International Conference on New Media*, Indonesia, 2015.

[22] A. K. Jain, R. C. Dubes, *Algorithms for Clustering Data*, Englewood Cliffs, NJ, USA, Prentice-Hall, 1988.

[23] E. Kiesling, C. Strausss, C. Stummer, "A multi-objective decision support framework for simulation-based security control selection," in *Seventh IEEE International Conference on Availability, Reliability and Security*, pp. 454–462, 2012.

[24] L. Klienrock, H. Levy, "The analysis of random polling systems," *Operation Research*, vol. 36, no. 5, pp. 716–732, 1988.

[25] A. Konak, D. W. Konak, A. E. Smith, "Multi-objective optimization using genetic algorithms: A tutorial," *Reliability Engineering and System Safety*, vol. 91, pp. 992–1007, 2006.

[26] D. Kumar, D. Kashyap, K. K. Mishra, A. K. Misra, "Security vs. cost: An issue of multi-objective optimization for choosing PGP algorithms," in *IEEE International Conference on Computer & Communication Technology (ICCCT'10)*, pp. 532–535, 2010.

[27] H. Levy, M. Sidi, "Polling systems: Applications, modelling and optimization," *IEEE Transaction on Communication*, vol. 38, no. 10, pp. 1750–1760, 1990.

[28] T. Li, D. Logothetis, M. Veeraraghavan, "Analysis of a polling system for telephony traffic with application to wireless LANs," *IEEE Transaction on Wireless Communications*, vol. 5, no. 6, pp. 1284–1293, 2006.

[29] X. Lin, "Map displays for information retrieval," *Journal of the American Society for Information Science*, vol. 48, pp. 40–54, 1997.

[30] D. Micheal, Y. H. Yacov, "Influence diagrams with multiple objectives and tradeoff analysis," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 34, no. 3, pp. 293–304, 2004.

[31] R. Murugan, M. R. Mohan, "Artificial bee colony optimization for the combined heat and power economic dispatch problem," *ARPN Journal of Engineering and Applied Sciences*, vol. 5, no. 7, pp. 9–18, 2012.

[32] T. Neubauer, C. Stummer, E. Weippl, "Workshop-based multiobjective security safeguard selection," in *Proceedings of the First IEEE International Conference on Availability, Reliability and Security (ARES'06)*, pp. 366–373, 2006.

[33] T. Okimoto, N. Ikegai, T. Ribeiro, K. Inoue, H. Okada, H. Maruyama, "Cyber security problem based on multi-objective distributed constraint optimization technique," in *43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W'13)*, pp. 1–7, 2013.

[34] J. Raissi, "Performance impact of imitation in multi-objective security service provisioning," in *Proceedings of IEEE*, pp. 1–6, 2013.

[35] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*, New York, NY: Wiley, 2000.

[36] R. Spence, *Information Visualization*, pp. 60–67, ACM press, 2001.

[37] W. Stallings, *Cryptography and Network Security Principles and Practices*, Pearson Education, 2004.

[38] S. Suriya, R. Deepalakshmi, S. Kannan, S. Shantharajah, "Enhanced bee colony algorithm for complex optimization problems," *International Journal on Computer Science and Engineering*, vol. 4, no. 1, pp. 72, 2012.

[39] V. Viduto, W. Huang, C. Maple, "Toward optimal multi-objective models of network security: Survey," in *Proceedings of the 17th International Conference on Automation & Computing*, pp. 6–11, 2011.

[40] V. Viduto, C. Maple, W. Huang, A. Bochenkov, "A multi-objective genetic algorithm for minimizing network security risk and cost," in *IEEE International Conference on High Performance Computing and Simulation (HPCS'12)*, pp. 462–467, 2012.

[41] L. Wang, *A Course in Fuzzy System and Control*, Prentice-Hall International, Inc., pp. 4–7, 1997.

[42] J. A. Weststrate, *Analysis and Optimization of Polling Systems*, Ph.D. Thesis, Tilburg University, 1992.

[43] A. Wierman, E. M. Winands, O. J. Boxama, "Scheduling in polling systems," *Performance Evaluation*, vol. 64, no. 9, pp. 1009–1028, 2007.

[44] L. Wu, G. Barash, C. Bartolini, "A service-oriented architecture for business intelligence," *IEEE International Conference on Service-oriented Computing and Applications (SOCA'07)*, pp. 279–285, 2007.

Biography

Seyed Mahmood Hashemi received his bachelor from Islamic Azad University (Qazvin Branch) in software engineering at 2001 his master from Islamic Azad University (Science and Research Branch) in artificial intelligence at 2003. He is currently PhD candidate in Beijing University of Technology (BJUT). His research interests are Internet of Things (IoT), network security and Artificial Intelligence (AI).

Jingsha He received his Master's and doctoral degrees in computer engineering from the University of Maryland at College Park in the US. He is currently a professor in the School of Software Engineering at Beijing University of Technology (BJUT) in Beijing, China. Prior to joining BJUT in 2003, Prof. He worked for several multi-national companies such as IBM Corp., MCI Communications Corp. and Fujitsu Labs in the US. where he published more than 10 papers and received 12 U.S. patents. Since joining BJUT in 2003, Prof. He has published nearly 240 papers in journals and international conferences, received nearly 40 patents and 30 software copyrights in China and co-authored 7 books. He has been the principal investigators of more than 20 research projects. Prof. He's research interests include information security, wireless networks and digital forensics.

Alireza Ebrahimi Basabi received his Master's degrees in Software engineering from the University of Beijing University of post and telecommunications (BUPT) in the china. He is currently a first year PhD student working under the supervision of Professor JingSha He in the Beijing University of Technology (BJUT). He has a background in system administration and software developer. His research interests include social media, IOT (Internet of Things), Ai (Artificial Intelligence), cloud computing, information assurance and Network security.