Solving Security of Cyber-Physical Systems with Multi-Objective Optimization Algorithms

Seyed Mahmood Hashemi
Beijing University of Technology
Chaoyang, Beijing, CHINA
Email: hashemi2138 [AT] yahoo.com

ABSTRACT--*Cyber-physical systems (CPS), as a significant set of the Internet of Things (IoT), play a key role in our life. CPS has a wide range of applications. Regardless of the benefits of CPS, they need a secure approach to communication. In this paper, an approach to CPS security is proposed. Usability of the proposed approach is the major characteristic of it because it employs a multi-objective model (MOM) of security. In this study, three algorithms were used to solve MOM (Multi-Objective Imperialist Competitive Algorithm, Multi-Objective Automata, Multi-Objective Bee Colony), because the evolutionary structure of the proposed algorithms causes the best adaptation on the network.*

Keywords--*Cyber-Physical System, Security, Multi-Objective Optimization.*

1. INTRODUCTION

Cyber-Physical Systems (CPSs) are critical components in the Internet of Things (IoT). “A CPS is an integration of physical processes, ubiquitous computation, efficient communication, and effective control” [1]. CPSs are seen in different aspects of the real world, from daily life to business process management. Different applications work with CPSs. Development of computing and also sensors technologies (e.g., ubiquitous wireless network, high volume of data, and data from media) have resulted in a tremendous increase in CPSs. A major reason for broad application of CPSs is the insufficient traditional application for modern life. Common methods for various duties such as recording or community are not effective for Big Data. CPSs create new opportunities such as network transportation, smart grids, and water/gas distribution. Indeed network technology allows using industrial actuators as a subgroup of CPSs. “CPSs are large-scale, geographically dispersed, federated, heterogeneous, and life-critical systems in which embedded devices such as sensors and actuators are networked to sense, monitor, and control the physical world” [2]. There are three highlight tasks for CPSs:

- Control/sampling actions properly.
- Sturdy implementation in the distributed environment
- The feedback loop between physical processes and computations to verification and validation

Notwithstanding the benefits of the CPS, the main problem that limits the usability of CPS is the security. Although security for the communication has a special importance, it is critical for CPS because of IoT applications.

Due to a sophisticated structure in the most of traditional approaches, they cannot be appealing for non-skilled users. The other problem of common approaches is related to the network structure. Since the network structure changes constantly and rapidly, the static approaches are not usable. The aim of this paper is to propose an approach with two characteristics: 1) simple to comprehend 2) adaptability to the network circumstances.

The remainder of this paper is organized as follow: Section 2 reviews the related works. In Section 3, the preliminaries of the proposed approach are explained. Section 4 describes the proposed approach. Finally, Section 5 provides the conclusion.

2. RELATED WORKS

The Internet of things (IoT) effects on humans life deeply. Although the new IoT functionality of smart devices results in a better life for the human, there are traditional cyber threats and also new threats. However, there are many works on the IoT security, most of which being not Use-Centric. Unlike the previous works, the approach proposed in the present work is based on the interaction with users, so it is User-Centric completely. In a broad view, we divide IoT networks into two categories: 1- consumer and 2- industrial. While we use IoT devices in a smart home, we emphasize the smart point of the IoT devices. In other words, the ultimate goal of IoT devices is communicated with and adjusting to other physical devices in the home. When a set of smart home devices has a particular behavior or need for special decision making, we call them as user-centric IoT (UCIoT). Akatyev et al. investigated heterogeneous IoT devices [3]. They used the data flow diagram to represent the dependencies between users and information. Patient-Centered Care (PCC) was coined by "Picker/Commonwealth Program developed by the Picker Institute in 1988" [4]. Khan et al. categorized IoT security issues into three groups: 1) low level, 2) intermediate level, and 3) high-level and then studied the security mechanism for each of them [5].

Although E-communication has some benefits, there are numbers of threats such as hackers, firms, and so on. Individuals need the right software, the right equipment, and also the right procedures to provide security. All nodes in the network carry a cost including the cost to provide security and cost for routing, etc. When adversary makes the decision to attack a specific node, if that node provides security then all nodes would survive.

Cerdeir et al. presented a partial characterization of the network to analyze welfare under equilibrium and then induced full protection [6]. Wu et al. studied the security detection in fusion-based methods. They used a Game Theory-based approach to verify their proposed mechanism [7].

Wireless Sensor Networks (WSNs) have two major benefits: They are user-friendly and their development involves low costs. Thus, WSNs have found a broad range of applications. We can divide the security mechanisms of WSNs into three different layers according to their targets: In the lowest layer, the physical security is set such that to guarantee network connectivity and reliability of the nodes; in the middle layer, there is a mechanism to ensure the nodes of WSNs are infrastructure; in the top layer, security mechanism must protect the data.

Yuan Gao et al. proposed a security mechanism based on the sensor nodes [8] that reduced the possibility of the attack effects. They divided nodes into two groups: 1) nodes exposed to attacks from credentials and 2) unauthorized nodes. In [9], the Bayesian Network was applied to the realistic model of assessment, so their framework is probabilistic and flexible. The channel gain is considered constant in [10]. For each transmission, power gain is multiplied by a random variable. Authors defined secrecy by assigning upper bound for the transmission powers.

Filtering is a useful tool to power control of IoT because it tries to avoid noise. The highest cost of the communication links can be attributed to the "time delay". Indeed, a low degree of confidentiality and availability can be viewed as "missing measurement". Thus, we can abbreviate the security performance of the network communication into two parameters: 1) time delay and 2) missing measurement.

Huanhuan Yuan et al. proposed some formulas to quantify the security. The foundation of their proposed approach is knowing about probability distribution and trust it to be static [11].

3. PRELIMINARIES

Three Evolutionary Multi-Objective Optimization (EMOO) algorithms are used in this paper; i.e., Multi-Objective Imperialist Competitive Algorithm (MOICA), Multi-Objective Automata, and Multi-Objective Bee Colony (MOBC). In the following, these algorithms are described.

3.1. Multi-Objective Imperialist Competitive Algorithm (MOICA)

Swarm optimization is a major class of optimization algorithms, which include several algorithms to solve the optimization problems. Imperialist Competitive Algorithm (ICA) is a modern approach in Swarm Intelligence Algorithms, which can be used in different optimization problems.

Social events are inspirational for ICA [16, 17, 18], so any components of ICA as a swarm optimization algorithm is named based on its sociality. In the initial step, there is a population of individuals as a potential solution. An individual is referred to as a country and is set randomly. Countries are divided into empires. $\mathrm{N}_{\mathrm{country}}$ and $\mathrm{N}_{\mathrm{empire}}$ are numbers of countries and empires, respectively. In each empire, power is calculated with the following formula:

$$\mathrm{power}_{\mathrm{j}} = \sum_{\mathrm{p}=1}^{\mathrm{M}} \sum_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{cost}_{\mathrm{i}}\left(\mathrm{country}_{\mathrm{p}}^{\mathrm{j}}\right) \qquad (1$$

where power is the same fitness in other optimization algorithms. According to Eq. (1), the power of the jth empire is the summation of k objective functions on M countries in an empire.

In each empire, the country with the most power is selected as the imperial and other countries are called colonies.

In each loop of the ICA algorithm, colonies try to be the same as the imperial. Fig. 2 displays this event. The angle and the length of individual changes are set with (2).

$$\mathrm{x} \sim \mathrm{U}(0, \beta \times \mathrm{d})\,, \theta \sim (-\gamma, \gamma) \qquad (2$$

where β and γ are random numbers that improve the search area of colonies around the imperial. Power of colonies in the empire is changed with x, θ.

Figure 1: Imperials and colonies

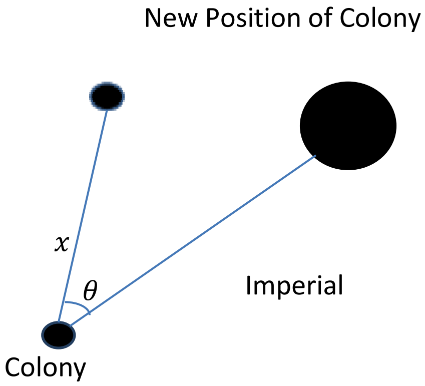

Figure 2: Movement of colony toward imperial

ICA is the evolutionary algorithm, so has some loops. In each loop, empires have different colonies. The ability to absorb the colonies is probabilistic and is defined based on the power of the empire.

$$\mathrm{prob_j} = \frac{\mathrm{power_j}}{\mathrm{SumPower}} \qquad (3$$

After assigning the colonies to the empires, it is needed to reevaluate the power of countries according to objective functions.

This process continues until reaching the termination conditions.

In the multi-objective state, the scenario is different because there are some non-dominated individuals. We propose an external memory (Archive) to keep non-dominated countries then the algorithm can use them in the next loop (Figure 3).

3.2. Multi-Objective Automata

Learning algorithms for automata can be divided into two broad groups: 1) standard algorithms and 2) model algorithms. The probability of select an action is computed with the following formula:

$$\mathrm{P(n + 1) = T[P(n), \alpha(n), \beta(n)]} \qquad (4$$

where T is the learning parameter that determines whether the algorithm is linear or non-linear. (4) may have two states. In the first state, the response is desired, so probability to select action is improved based on α. In the second state, the response of the algorithm is not desired, so the probability to select decrease based on β (Figure 4).

We can consider various values for α and β, but in this paper, we decide $\alpha = \beta$.

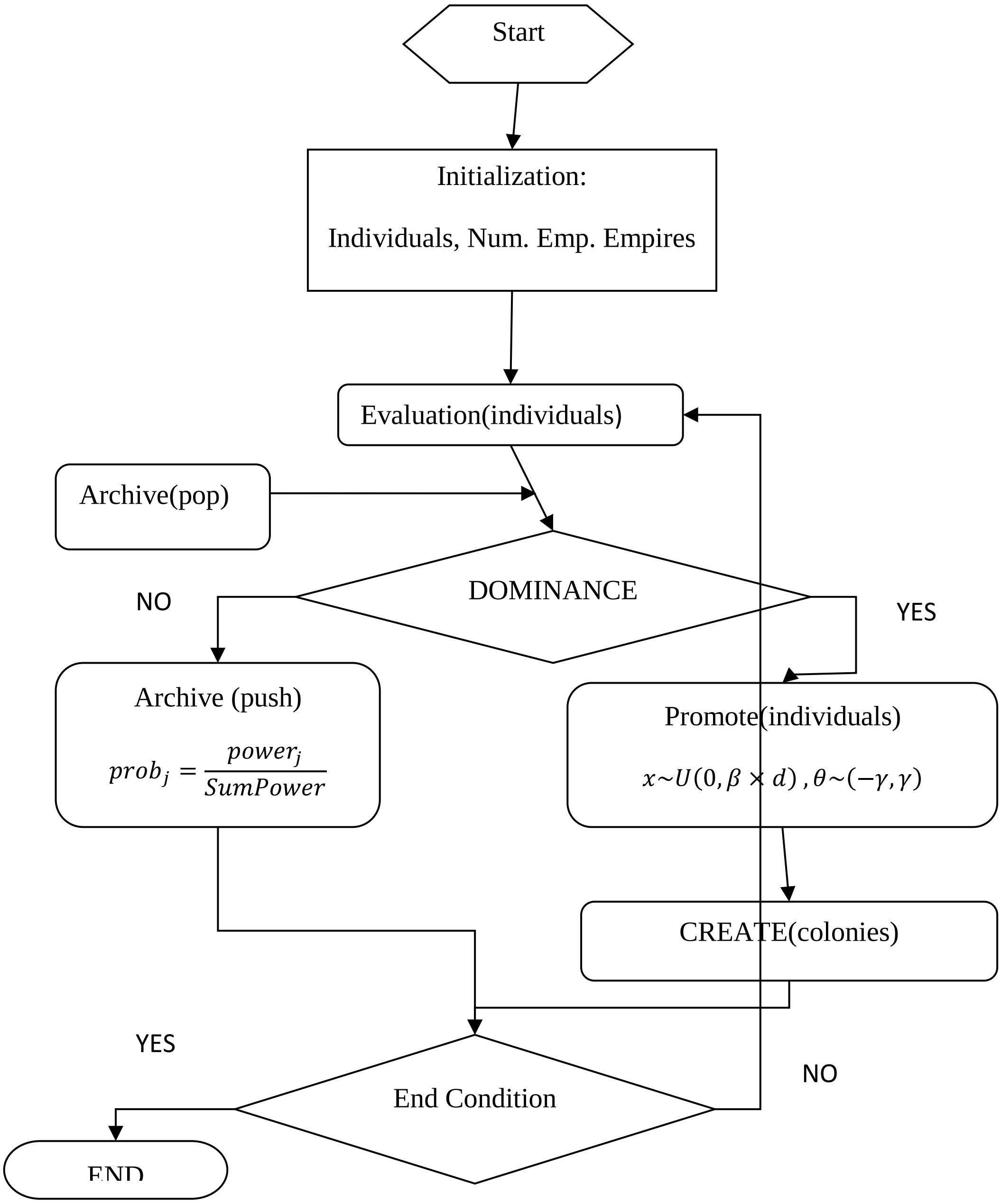

Figure 3: Flowchart of Multi-Objective Imperialist Competitive Algorithm

Three situations may occur in the multi-objective state of learning automata [17, 18]:

- First: one potential solution (individual) may dominate other individual(s). Therefore, the associated probability will increase.
- Second: The potential solution (individual) is dominated by other individual(s). Thus, the associated probability will decrease.
- Third: the individual is non-dominated with other individuals. Thus, it is kept in the Archive.

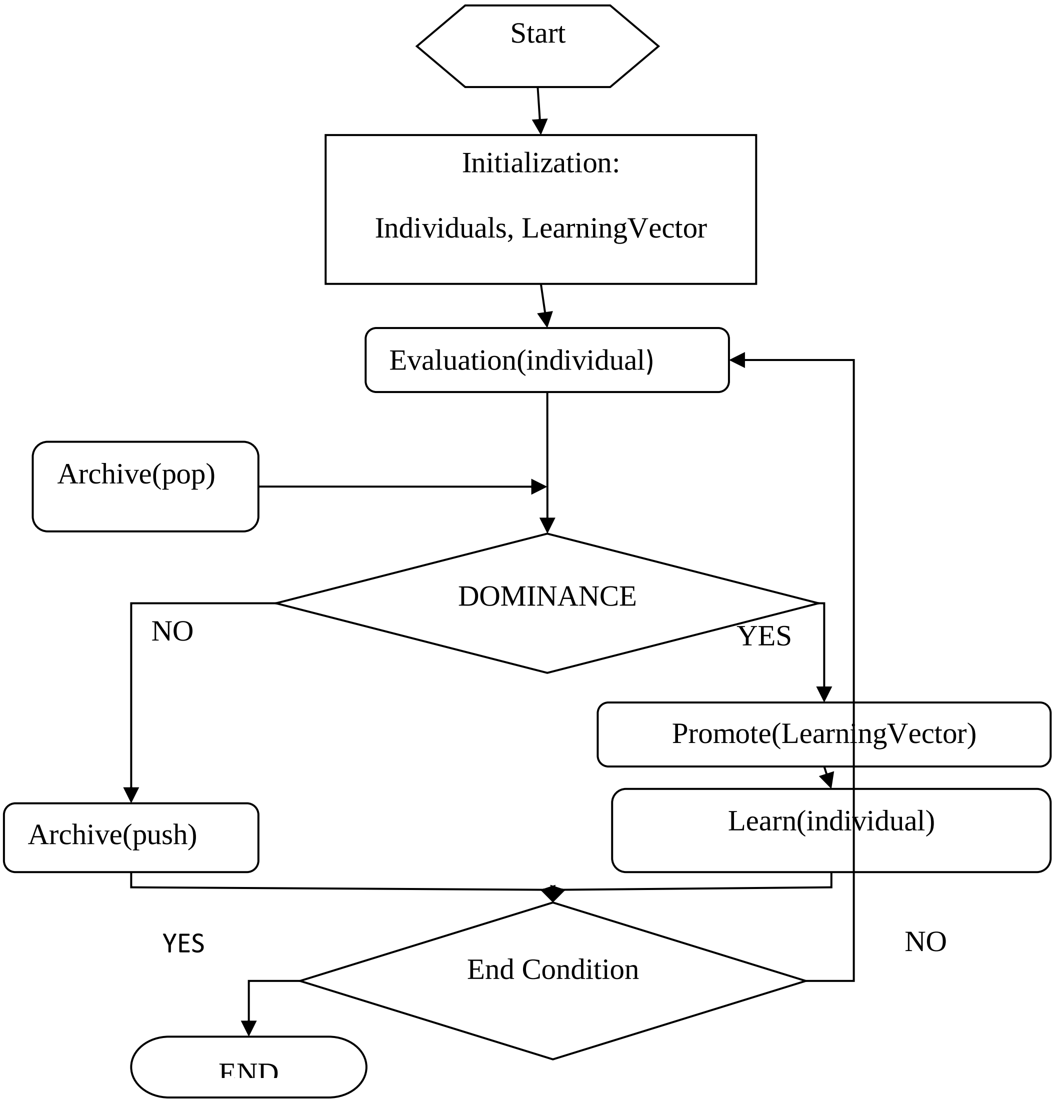

Figure 4: Flowchart of Multi-Objective Learning Automata

3.3. Multi-Objective Bee Colony (MOBC)

The MOBC algorithm is inspired from the foraging conduct of bees. The foraging behavior of bees is characterized with some steps. The first step is called Waggle Dance that is done by bees to communication about characters of source food same as direction, distance, and quality.

When a food fount is known, a bee begins to dance in a figure of eight patterns. The second step in the foraging conduct is the result of communication and it is identified with bees' function. In this step, the bees that waited in the hive follow the dancer bee. The number of bees in a specific path is determined according to the quality of the path. In the third step, follower bees return to the hive. If the path is still good enough, more bees are sent to the source food. If the quality of the path is poor the gathering process is stopped.

We can use foraging behavior to solve the optimization problem by dividing its characters into two phases. The first phase involves the construction of path. In this phase, a bee explores entirely the feasible area and finds a food source. When a bee does exploration, which is displayed as a tour with all possible variables, it performs the Waggle Dance. Other bees use this information, expressed as:

$$\mathrm{Pf_i} = {}^{1}/_{\mathrm{L_i}},$$

where $\mathrm{Pf_i}$ is the profitability of a $\mathrm{bee_i}$ and $\mathrm{L_i}$ is its tour. For a set of n bees, the profitability of bees is computed with Eq. (5)

$$\mathrm{Pf_{colony}} = \frac{1}{n}\sum_{i=1}^{n} \mathrm{Pf_i} = \frac{1}{n}\sum_{i=1}^{n} {}^{1}/_{\mathrm{L_i}} \qquad (5)$$

The communication behavior of any bee is given by:

$$D_i = K * {}^{Pf_i}\!/_{Pf_{colony}} ,$$

where K is the profitability rating and is adjusted according to the lookup table given in Table 1.

TABLE 1: 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 MOBC includes path reconstruction. In this phase, bees in the hive communicate with the explored bee to 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:

$$\rho_{ij}(t) = \begin{cases} \lambda, & j \in F_i(t) \\ \frac{1-\lambda|F_i(t)\cap A_i(t)|}{|A_i(t)|-|F_i(t)\cap A_i(t)|} & ,j \notin F_i(t)' \end{cases} \qquad (6$$

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 [16], [17], [18] and [19].

Now, we can examine all paths based on domination. We define the dominance of all paths according to Section 2.2.1. Thus, each path is classified by conforming to one of three situations:

- dominates another path(s),
- is dominated by another path
- is non-dominated by any other path

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:

$$P_{ij}(t) = \frac{[\rho_{ij}(t)]^{\alpha} * \left[\frac{1}{d_{ij}}\right]^{\beta}}{\sum_{j\in A_i(t)}[\rho_{ij}(t)]^{\alpha} * \left[\frac{1}{d_{ij}}\right]^{\beta}} \qquad (7$$

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.

4. PROBLEM AND PROPOSED APPROACH

Suppose there is a network with V =5 nodes $(v_1, v_2, \cdots, v_N)$ and $E = 10$ $(e_1, e_2, \cdots, e_N)$ links. The network is directional, meaning that the link $[a, b]$ is unequal with $[b, a]$. The links between nodes have three weights that display the values for Confidentiality, Integrity, and Availability respectfully. We denote confidentiality as conf., integrity as into., and availability as avai. The network is stochastic, so the weights vary with time. The changing of weight links is approximated with the Gaussian function, which is the general function for the probability. The degree of the network, which is the maximum number of links to the network nodes, is $N = 20$. Data packets have a counter that decreases with visiting a node. Thus the maximum length of paths is $M = 10$. The problem is finding the suitable path; i.e., the path with optimum values of confidentiality, integrity, and availability of links. Suppose the optimal path has P links. We can model the problem as follows:

$$\text{Optimize} \qquad \mathrm{C, I, A, Cost}$$

$$\mathrm{C} \equiv \sum_{i=1}^{P} \mathrm{conf.}\,(l_i)\,;\, \mathrm{I} \equiv \sum_{i=1}^{P} \mathrm{inte.}\,(l_i)\,;\, \mathrm{A} \equiv \sum_{i=1}^{P} \mathrm{avai.}\,(l_i)\,;\, \mathrm{Cost} \equiv \sum_{i=1}^{P} \mathrm{cost}(l_i)$$

$$\text{Subject To: } \mathrm{C} \geq \mathrm{Pre(C)}, \mathrm{I} \geq \mathrm{Pre(I)}, \mathrm{A} \geq \mathrm{Pre(A)}$$

where l is the link in the path, so conf. (l) means the confidentiality of link l. Pre is the predefined value. Thus, C must be greater than or equal to the predefined value of summation of link confidentiality, I must be greater than or equal to the predefined value of summation of link integrity, and A must greater than or equal to the predefined value of summation of link availability.

In this paper, three Evolutionary Multi-Objective Optimization (EMOO) algorithms were used. The first algorithm is Multi-Objective Imperialist Competitive Algorithm (MOICA). The second one is Multi-Objective Automata. Learning Automata is a common intelligent algorithm, which is used in various fields. Optimization is a famous field that uses Learning Automata, but Multi-Objective Automata (MOA) is not common. The third algorithm is Multi-Objective Bee Colony (MOBC). The difference between the first algorithm with the second and the third algorithms is referred to a special space which is called archive and this space is not in the other algorithms. In the Multi-Objective Automata, we change the probability of evolution, but in MOICA and MOBC, individuals are changed directly.

Used algorithms have two characteristics: they are evolutionary and iterative. The evolutionary character of these algorithms means that their initial values are random (or semi-random) while an iterative feature of these algorithms suggest that they may produce better results with more iteration. We need a special number of epochs as a termination condition for iterative algorithms. Therefore, we cannot claim which algorithm is better. Table 2 presents the final results of used algorithms. The numbers are between 0 and 10.

TABLE 2: Experimental Results

	C	I	A	Cost
MOICA	9.89	9.15	8.64	1.03
MOA	7.32	7.9	5.49	4.57
MOBC	8.56	8.41	8.06	3.29

Actually, the final results for the MOICA are better than others. Another criterion to find appropriate algorithm is the needed iteration to reach the steady state that the algorithm results do not change after that state. Following chart shows the needed iteration for the steady state of each algorithm (MOICA, MOA, MOBC respectively).

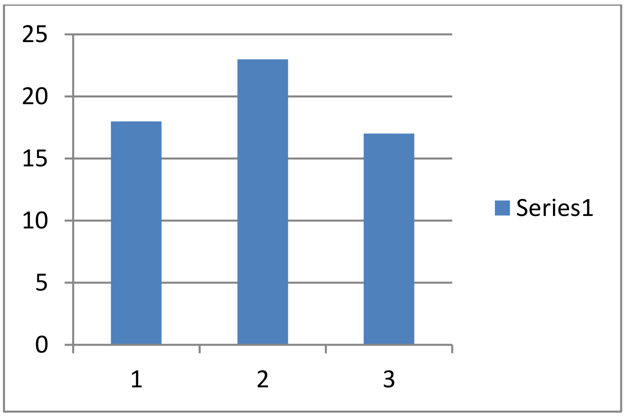

Figure 5: Numbers of Needed Iterations

5. CONCLUSION

The aim of this work is proposing an approach for Cyber-Physical System (CPS) security. The CPS security is viewed as a multi-objective optimization problem and then three algorithms are used to solve it are used. The structure of proposed algorithms is evolutionary and also stochastic. Thus, the final outcomes of the proposed algorithms are different in various executions.

6. REFERENCES

[1]. Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang, "A survey on security control and attack detection for industrial cyber-physical systems", ELSEVIER, Neurocomputing 275 (2018) 1674–1683

[2]. Zheng Xu, Yunhuai Liu, Hui Zhang, "Special section on intelligent sensing and applications for cyber-physical systems", ELSEVIER, Future Generation Computer Systems 81 (2018) 382–383

[3]. Nikolay Akatyev, Joshua I. James, "Evidence identification in IoT networks based on threat assessment", ELSEVIER, Future Generation Computer Systems

[4]. Bahar Farahani, Farshad Firouzi, Victor Chang, Mustafa Badaroglu, Nicholas Constant, Kunal Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare", ELSEVIER, Future Generation Computer Systems 78 (2018) 659–676

[5]. Minhaj Ahmad Khan, Khaled Salah, "IoT security: Review, blockchain solutions, and open challenges", ELSEVIER, Future Generation Computer Systems 82 (2018) 395–411

[6]. Diego A.Cerdeir, MarcinDziubi´nski, Sanjeev Goyal, "Individual security, contagion, and network design", ELSEVIER, Journal of Economic Theory 170 (2017) 182–226

[7]. Hao Wu, Zhonghua Wang, "Multi-source fusion-based security detection method for heterogeneous networks", ELSEVIER, computers & security 74 (2018) 55–70

[8]. Yuan Gao, Hong Ao, Zenghui Feng, Weigui Zhou, Su Hu, Wanbin Tang, " Mobile Network Security and Privacy in WSN", ELSEVIER, Procedia Computer Science 129 (2018) 324–330

[9]. Alessio Misuri, Nima Khakzad , Genserik Reniers , Valerio Cozzani, "A Bayesian network methodology for optimal security management of critical infrastructures", ELSEVIER, Reliability Engineering and System Safety 000 (2018) 1–14

[10]. Pedro C. Pinto, João Barros, Moe Z.Win, "Secure Communication in Stochastic Wireless Networks—Part I: Connectivity", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012

[11]. Huanhuan Yuan, Yuanqing Xia, "Secure filtering for stochastic non-linear systems under multiple missing measurements and deception attacks", IET Control Theory Appl., 2018, Vol. 12 Iss. 4, pp. 515-523

[12] Carlos A. Coello Coello, David A. Van Veldhuizen, Gary B. Lamont, "Evolutionary Algorithms for Solving Multi-Objective Problems", Speringer. 2nd Ed. , 2007.

[13] Cristopher Dimopoulos, "A Review of Evolutionary Multi-objective Optimization, Application in the Area of Production Research", IEEE. Print ISBN 0-7803-8515-2, DOI 10.1109/CEC.2004.1331072. , 2004.

[14] Carlos A. Coello Coello, "An Updated Survey of Evolutionary Multi-Objective Techniques: State of the art and Future Trends", IEEE. Vol.1, Printed ISBN 0-7803-5536-9, DOI 10.1109/CEC.1999.781901. , 1999.

[15] Zdzislaw Kowalczuk, Tomasz Bialaszewski, "Improving Evolutionary Multi-Objective Optimization Using Genders", Springer. Vol. 4029/2006, DOI 10.1007/1178231-42. , 2006.

[16] Arash Khabbazi, Esmaeil Atashpaz, Caro Lucas, "Imperialist Competitive Algorithm for Minimum Bit Error Rate Beamforming", Inte.J. Bio-Inspired Computation, Vol. 1, Nos.1/2. , 2009.

[17] Esmaeil Atashpaz, Caro Lucas, "Imperialist Competitive Algorithm: An Algorithm for Optimization Inspired by Imperialistic Competition", IEEE. Congress on Evolutionary Computation. , 2008 .

[18] Caro Lucas, Zahra Nasiri-Gheidari, Farid Tootoonchian, "Application of an Imperialist Competitive Algorithm to the Design of a Linear Induction Motor", ELSEVIER. Energy Conversion and Management. 1407–1411, 2010.