Asian Journal of Applied Sciences (ISSN: 2321 – 0893)
Volume 07 – Issue 03, June 2019

Providing Security in CPSs with Evolutionary Algorithms

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

ABSTRACT---- ***Because of the significant role of Cyber-Physical Systems (CPSs) in our lives, the security of these systems is of paramount importance. Due to the complexity of inside CPSs components, current methods need special skills to understand their workflow. The approach available in this regard, more than comfortability, have the ability to adapt to the network conditions. In this research, we present the secure routing problem of CPSs as a multi-objective optimization model and then solve it through three Evolutionary Algorithms (EAs). The main reason four using EA is that it allows satisfying the time constraints in the routing. Multi-objective optimization produces optimum values for objectives simultaneously.***

Keywords---- Cyber-Physical Systems, Multi-Objective Optimization, Evolutionary Algorithm

1. INTRODUCTION

Networked data play an important role in Cyber-Physical Systems (CPSs). There are three problems to apply sufficient security for data transmission: physical and technological limitations, complexity due to large-scale networked components, and unforeseen threats from cyberspace. There are two different aspects for CPSs: 1) CPSs are controlled systems with a high degree of automation and 2) CPSs can receive data from physical components. Providing a bridge between two different aspects of CPSs is a problem because the most control methods work in a discrete manner when the most physical components work in a continuous manner. Thus, attacks may be done while extracting data in sensors and sending them to remote controllers.

The aim of this paper is to provide an approach to secure routing of CPSs. The presented approach has some features:

- It is easy to understand, so it can be used by both administrators and users with any skill.
- We use probability distribution in our approach, so it can be adapted to the dynamism of the network structure.
- The presented approach is based on the multi-objective optimization model that can be extended to the more objects.

There are four techniques to detect attacks in CPSs: 1- Bayesian detection, 2- weighted least square approach, 3- x^2 detection, and 4- quasi-FDI. The last three approaches need to measure data, but it is impossible in high data spectrum. Bayesian detection technique is chosen for this paper because the fundamental of Bayesian probability is studied; indeed, it is a common method to approximate the unforeseen conditions same as the network structure.

Cyber-physical systems are integration between computing intelligent and physical world. Due to the inside structure of CPSs (for example, installing patches or numerous system updates), traditional information technologies methods are not sufficient to protect CPSs. In this regard, the traditional approaches lack any suitable framework. For example, Failure Mode and Effect Analysis (FMEA) is a famous method to analyze the security with Risk Priority Number:

$$\mathrm{RPN} = \mathrm{Risk} \times \mathrm{Probability\ of\ Occurence} \times \mathrm{Detection}$$

Here, the risk is adapted to the CPSs structures because the probability of occurrence for different components of CPSs is not the same. The most dangerous situation of CPSs is tampering information as systems cannot work correctly. The first step to protect against cyber attacks is the identification of attack probability. Therefore, the objective of this study is to provide an extension of Bayesian detection such that it can detect the attack probability for different CPSs' components. For this purpose, we used Multi-Objective Optimization (MOO) and also some Evolutionary Optimization (EO) Algorithms. MOO allows considering multiple parameters independently and adapts the EO to the network conditions.

The remainder of this paper is organized as follow: Section 2 presents the principles of CPSs. Section 3 reviews some related works. In Section 4, the proposed algorithm and its result are explained. Finally, Section 5 provides concluding remarks.

2. PRINCIPLE OF CYBER-PHYSICAL SYSTEMS (CPSS)

The process in cyber-physical systems is controlled and monitored with computers. The cyber-physical systems include smart grids, water plants, chemical plants, oil and natural gas distribution systems, transportation systems, and so on. The failure of CPS security affects deeply human lives and also industrial products. There are two groups of variables in the CPSs: measurement variables and control variables. The distance between measured variables and optimum values is calculated and then the result values are sent to actuators to keep the closer to the optimum state. The operators of the CPSs are aware of the current state with a graphic interface. We can depict the CPSs with two layers (Figure 1): the first layer includes a corporate network, control network and demilitarized zone (DMZ); the second layer includes sensors, actuators, and physical devices.

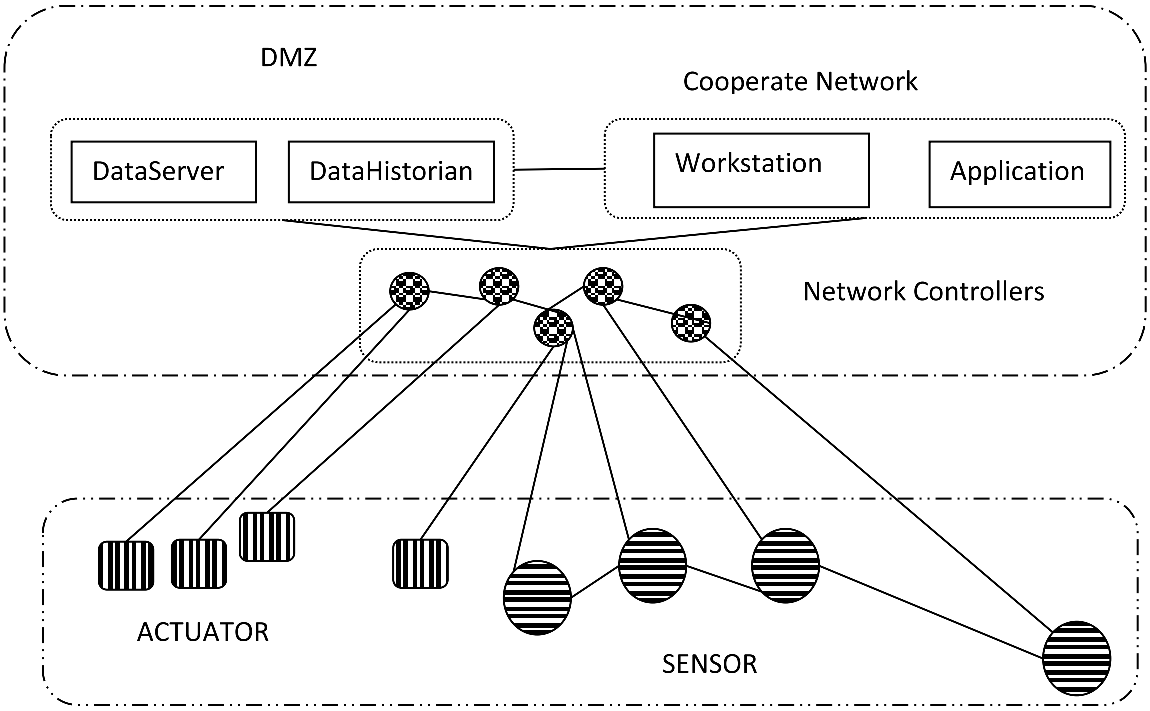


Figure 1: Components of CPSs

There are three types of communication in CPSs:

- Sensor-sensor: Information from the environment is extracted, collected, and sent to controllers.
- Controller-actuator: Control commands are sent to an actuator for applying on the CPS.
- Controller-controller: Controllers communicate among themselves to fabricate a correct set of commands.

The major problem of CPSs is security includes confidentiality, integrity, availability, and cost. Actually, constructing and deployment and maintenance of CPS are a tradeoff between various benefits and prices. Although CPSs have benefits for both servers and clients, they have some tolls as well. Since there are constraints on two sides (clients and servers) for tolls, there is a need to consider an independent parameter for it.

For the sake of simplicity and avoid loss of generality, we consider communication types in CPSs in two categories: 1) inner; including controller-controller communication and 2) outer; including controller-actuator/sensor communication. Providing security in CPSs refers to providing security in inner and outer communication.

3. RELATED WORKS

Various approaches have proposed for CPS security. Orojloo et al. used a decision-making trial and evaluation laboratory (DEMATEL) method to solve the security problems of CPSs [1]. Their proposed method has some parameters that are required to be tuned. Authors tune the control parameters according to the system dynamics. Derui Ding et al. presented a scheme to provide security on CPSs based on the control theory [2]. Lopez et al. presented an approach based on the analysis of the full range requirements for access control [3]. Stefanov et al. enhanced the capability of cyber security using the Supervisory Control And Data Acquisition (SCADA). They modeled large-scale cyber-physical systems [4].

The reliability of CPSs is related to network components, cyber medium, network topology, and routing. Liu et al. offered an approach to analyze CPSs with flexible factors. They divided reliable assets into two groups: equipment and systems [5].

Nourian et al., by modeling the attacks, presented a theoretic framework for CPSs [6]. They applied the System Theoretical Accident Model and Process (STAMP) for this purpose.

The lack of security in CPSs may have catastrophic consequences. For example, an unstable communication channel for power grid causes large-scale cascade blackout. Indeed CPSs privacy is important because CPSs needs to collect data from wide geographic areas to make decision and breaches in collecting data process cause leakage.

Wurm et al. considered different layers of CPSs in a current structure [7]. They analyzed the CPSs security with cross layer view and depicted different layers of CPSs in smart homes.

Rahman et al. offered a robust Intrusion Detection System (IDS) to maintain the integrity and reliability of the system when conditions change rapidly [8]. They presented a distributed multi-agent framework to provide security on the system of power grids. Since the presented system is multi-agent, the presented formula are also multiple as a matrix. These authors established limitations for various aspects of a multi-agent system.

In physical systems, security is the same as goat herder while administrator must control the access to assets (goat) and monitor the mechanism (herder). In cyber-system state, security shows a combination of username, password, and cryptography. In CPSs, information leaks have an important role. Although the determination of security domains (SDs) is easy for purely physical systems, it is a difficult task in CPSs it is hard because SDs may overlap or disjoint from each other. Providing security in CPSs includes two steps: The analysis of user access to physical assets and securing the flow of information between physical and cyber components. Howser et al., based on the information flow of users within security domains (SDs), developed a model for the system to integrate the computational and physical aspects of CPSs [9]. The presented model was based on The Multiple Security Domain Non-deducibility (MSDND) model.

Surveying a number of methods, Choo et al. mentioned that a gap between transparently of a sensitive environment and CPSs security in existing methods [10]. Giraldo et al. classified different security concepts for CPSs [11].

Security index determines the minimum needed number for tampering in malicious attack to bus networking in the linear estimator. Although the determination of the security index is an NP-hard problem, many algorithms have been proposed for solving it. Shames et al. proposed an approach to detect an adversary using $\mathcal{H}2$ norm [12]. They considered finding a point to inject an attack as an optimization problem.

Security protection methods can be categorized into two major groups: signature-based or anomaly-based. In signature-based, Intrusion Detection is performed on a database. Thus, a signature-based method is not effective for unknown attacks. In the anomaly-based approach, Intrusion Detection is done by comparing the expected system behavior with the current tendency. CPSs often have predictable behavior, so they are desired in the anomaly-based Intrusion Detection. Yang et al. presented an approach to divide the system states into multiple zones and then investigated each zone for error or anomaly [13].

4. PROPOSED ALGORITHM

As mentioned in "Principal of Cyber-Physical Systems" section, the communications in CPSs can be divided into two major parts: 1) between sensors and actuators to the network controllers and 2) between controllers and DMZ and cooperators. It has to be noted that security in both categories of communication of CPSs components is important because it ensures users about the performance of CPSs. Regarding the large number of available CPSs components communication ways (such as distance, bandwidth, and so on), we have to consider the security of them independently. Multi-Objective optimization (MOO) is a suitable method to optimize multiple parameters simultaneously.

The first step is to construct a MOO model for the problem. Let denote the communication ways in the first part with $a_i; i \in [1, \cdots, m]$ and the communication ways in the second part with $b_j; j \in [1, \cdots, n]$.

$$\begin{aligned}\text{Optimize } & \mathrm{CONF}\left(\textstyle\sum_{i=1}^{m} a_i\right), \mathrm{INT}\left(\textstyle\sum_{i=1}^{m} a_i\right), \mathrm{AVA}\left(\textstyle\sum_{i=1}^{m} a_i\right), \mathrm{COST}\left(\textstyle\sum_{i=1}^{m} a_i\right), \\ & \mathrm{CONF}\left(\textstyle\sum_{j=1}^{n} b_j\right), \mathrm{INT}\left(\textstyle\sum_{j=1}^{n} b_j\right), \mathrm{AVA}\left(\textstyle\sum_{j=1}^{n} b_j\right), \mathrm{COST}\left(\textstyle\sum_{j=1}^{n} b_j\right) \qquad (1\end{aligned}$$

where CONF, INT, and AVA are confidentiality, integrity, and availability, respectively. COST denotes a tradeoff between benefit and price for the communication ways from an economic perspective. In other words, the model optimizes different aspects of security for all communication ways simultaneously.

The second step is using Evolutionary Optimization (EO) algorithms is to solve the constructed model. Despite the large number of EO algorithms, we used three of them in this work; i.e., Vector Evaluated Genetic Algorithm (VEGA), Multi-Objective Genetic Algorithm (MOGA), and Random-weighted Approach (RWA).

4.1 Vector Evaluated Genetic Algorithm (VEGA)

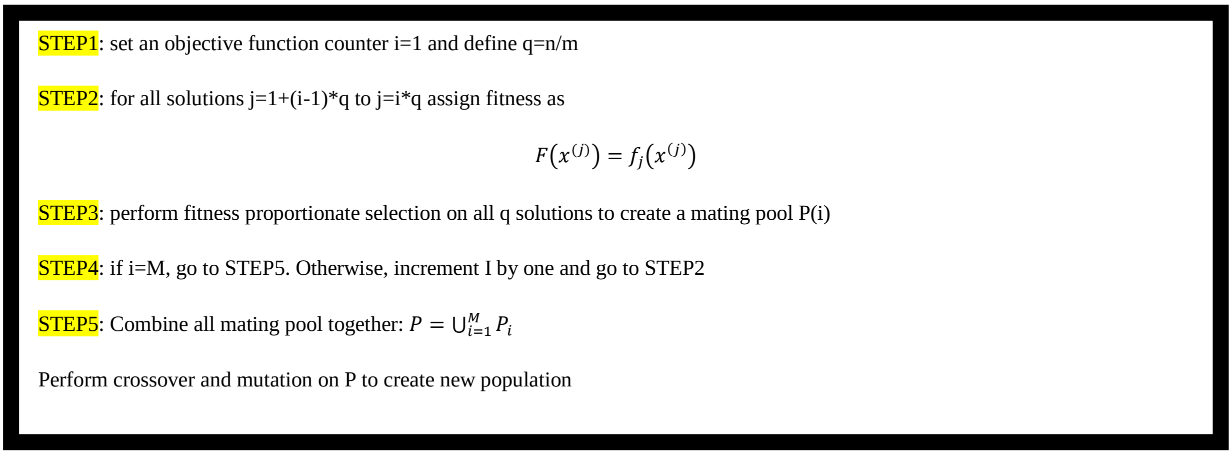
VEGA is the first notable approach on solving MOP problems. This algorithm uses a vector fitness measure to create the next generation (Figure 2).

The selection step in each generation becomes a loop. Each time, the loop selects the appropriate fraction of the next generation, or subpopulation, is selected based on each objective.

The entire population is shuffled thoroughly to apply crossover and mutation operators. This shuffling is performed to achieve the mating of individuals of different subpopulations. Dividing the population into M equal blocks for M objectives at every generation causes to each block is reproduced with one objective function. The entire population participates in crossover and mutation proportionate selection operator is used in order to reduce the positional bias in the population. For this purpose, it is better to shuffle the population before it is partitioned.

4.2 Multi-Objective Genetic Algorithm (MOGA)

The method proceeds by sorting the population according to the ranks, through which ties may be broken by random choice (Figure 3). In the first epoch, all individuals are of the same rank, but in the next epochs some of them dominate others and take different ranks. The required computation in MOGA is heavy compared with other EOs.



```
STEP1: set an objective function counter i=1 and define q=n/m
STEP2: for all solutions j=1+(i-1)*q to j=i*q assign fitness as
        $F(x^{(j)}) = f_j(x^{(j)})$
STEP3: perform fitness proportionate selection on all q solutions to create a mating pool P(i)
STEP4: if i=M, go to STEP5. Otherwise, increment I by one and go to STEP2
STEP5: Combine all mating pool together: $P = \cup_{i=1}^{M} P_i$
Perform crossover and mutation on P to create new population
```

Figure 2: Pseudo-Code of VEGA

4.3 Random-weighted Approach (RWA)

Murata, Ishibuchi, and Tanaka (1998) proposed a Random-Weight Approach (RWA) for obtaining a variable search direction toward the Pareto frontier.

The fixed-weight approach gives the GAs a tendency to sample the area toward a fixed point in the criterion space (Figure 4).

The random-weight approach gives the GAs a tendency to demonstrate a variable search direction, therefore, the ability to sample the area uniformly over the entire frontier.

STEP1: choose a $\sigma_{s\square are}$. Initialize $\mu(j) = 0$ for all possible $j = 1,2,\cdots,N$. Set solution counter $i = 1$.

STEP2: calculate the number of solution n_i that dominates solution i. Compute the rank of the ith solution as $r_i = 1 + n_i$. Increment the count for the number of solutions in rank r_i by one that is $\mu(r_i) = \mu(r_i) + 1$.

STEP3: if $i < N_i$ increment i by one and go to STEP1. Otherwise, go to STEP4.

STEP4: identify the maximum rank r^* by checking the largest r_i when $\mu(r_i) > 0$. The sorting according to the rank and fitness averaging yields the following assignment of the average fitness to any solution $i = 1,2,\cdots N$.

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

To each solution i with rank $r_i = 1$. The above equation assigns a fitness equal to $F_1 = N - 0.5(\mu(1) - 1)$ which the average value of $\mu(1)$ consecutive integers from N to $N - \mu(1) + 1$. Set a rank counter $r = 1$.

STEP5: for each solution i rank r_i calculate the niche count nc_i with other solutions of the same rank by using

$$nc_i = \sum_{j=1}^{\mu(r_i)} Sh(d_{ij})$$

Calculate the fitness using $F_j = {}^{F_j}\!/_{nc_j}$. To preserve the same average fitness, scale the shared fitness by

$$F_j = \left[F_j \mu(r) \Big/ \sum_{k=1}^{\mu(r)} F(k) \right] F_j$$

STEP6: if $r < r^*$, increment r by one and go to STEP5. Otherwise, the process is complete.

Figure 3: Pseudo-Code of MOGA

Let us assume there is a Cyber-Physical System in a distributed environment. It means that there are multiple ways for the inner/outer communication. The objective is finding the suitable path with an optimum degree of security. In this way, we model the system based on (1) and then use MOGA, VEGA, and RWA. The conditions of the communication ways are changed always and suddenly, so Gaussian formula is used to represent the density of changing.

STEP1: for each objective function j, set upper and lower bounds as f_j^{max} and f_j^{min}.

STEP2: for each solution $i = 1,2,\cdots,N$. Calculate the distance $d_{ik} = [x_w^{(i)} - x_w^{(k)}]$ with all solution $k = 1,2,\cdots,N$. Then calculate the sharing function value as

$$S\square(d_{ik}) = \begin{cases} 1 - \dfrac{d_{ik}}{\sigma_{s\square are}}, & if\ d_{ik} \le \sigma_{s\square are} \\ 0, & ot\square erwise \end{cases}$$

Thereafter, calculate the niche count of the solution i as $nc_i = \sum_{k=1}^{N} S\square(d_{ik})$.

STEP3: for each solution $i = 1,2,\cdots,N$. Follow the procedure bellow. Corresponding to the $x_w^{(i)}$value, identify the weight vector $W^{(i)}$ from the user-defined mapping between the integer variable $x_w^{(i)}$ and the weight vector $W^{(i)}$ assign fitness F_i according to

$$F(x^{(i)}) = \sum_{j=1}^{M} W_j^{x_w^{x(i)}} \frac{f_j(x^{(i)}) - f_j^{min}}{f_j^{max} - f_j^{min}}$$

Calculate the Shared Fitness as $F_i = \frac{F_i}{nc_i}$ for each individual. Then proportionate selection is applied to create the mating pool. Thereafter crossover and mutation operators are applied on the entire string.

In Table 1, the values for parameters are in the range of [0,10]. The table represents the optimum values for eight parameters of CPS. The first four parameters are about inner communication and the last ones are about outer parameters.

Another important factor in the presented approach is the stability time, which means the time needed for the algorithm to be stable. Since CPS works in the distributed environment, the stability time is critical and may determine the effectiveness of CPS. Fig. 5 presents the stability time for algorithms.

TABLE 1: Final Results

	inner-CONF	inner-INT	inner-AVA	inner-COST
MOGA	0.85	0.84	0.79	0.93
VEGA	0.88	0.75	0.92	0.82
RWA	0.32	0.43	0.51	0.28
	outer-CONF	outer-INT	outer-AVA	outer-COST
MOGA	0.68	0.74	0.53	0.72
VEGA	0.62	0.63	0.81	0.92
RWA	0.48	0.74	0.39	0.62

The stability time for VEGA is shorter than that of other algorithms, but obtained results of algorithms showed that MOGA outperforms the others. Indeed, there might be a tradeoff between the quality of the results and the stability time.

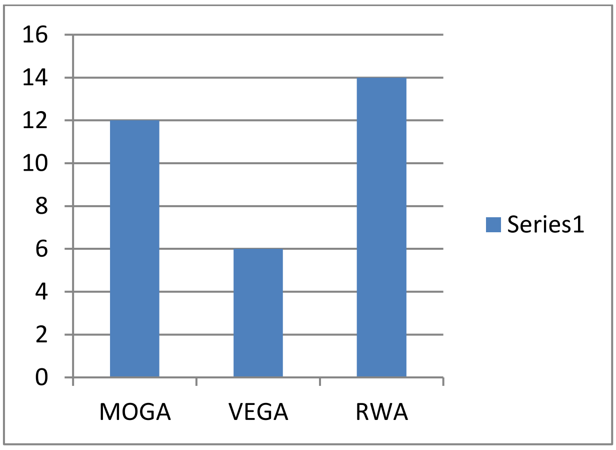


Figure 5: Stability Times

5. CONCLUSION

In this paper, we present an approach to find secure routing for the Cyber-Physical Systems (CPSs). The presented approach is easy to understand and adaptable to the network conditions because it uses probability distribution. Since the structure of Evolutionary Algorithms (EAs) used in the presented approach is stochastic, it is hard to reach a conclusion on EAs performance; however, the approximate Multi-Objective Genetic Algorithm (MOGA) outperforms the other algorithms.

6. REFERENCES

[1] Hamed Orojloo, Mohammad Abdollahi Azgomi, “A method for evaluating the consequence propagation of security attacks in cyber–physical systems”, ELSEVIER, Future Generation Computer Systems 67 (2017) 57–71

[2] 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”, Neurocomputing 275 (2018) 1674–1683

[3] Javier Lopez, Juan E. Rubio, " Access control for cyber-physical systems interconnected to the cloud", ELSEVIER, Computer Networks 134 (2018) 46–54

[4] Alexandru Stefanov, Chen-Ching Liu, "Cyber-Physical System Security and Impact Analysis", Proceedings of the 19th World Congress The International Federation of Automatic Control Cape Town, South Africa. August 24-29, 2014

[5] Jie Liu, Diangang Wang, Cheng Zhang, Zhenyu Tang, Zhuozhen Jiang, Junyong Liub, Yue Xiang, "Reliability Assessment of Cyber Physical Distribution System", ELSEVIER, Energy Procedia 142 (2017) 2021–2026

[6] Arash Nourian, Stuart Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 15, NO. 1, JANUARY/FEBRUARY 2018

[7] Jacob Wurm, Yier Jin, Yang Liu, Shiyan Hu, Kenneth Heffner, Fahim Rahman, Mark Tehranipoor, "Introduction to Cyber-Physical System Security: A Cross-Layer Perspective", IEEE TRANSACTIONS ON MULTI-SCALE COMPUTING SYSTEMS, VOL. 3, NO. 3, JULY-SEPTEMBER 2017

[8] Shihanur Rahman, Apel Mahmud, Aman Maung Than Oo, Hemanshu Roy Pota, "Multi-Agent Approach for Enhancing Security of Protection Schemes in Cyber-Physical Energy Systems", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 13, NO. 2, APRIL 2017

[9] Gerry Howser, Bruce McMillin, "Using Information-Flow Methods to Analyze the Security of Cyber-Physical Systems", IEEE COMPUTER SOCIETY APRIL 2017

[10] Kim-Kwang Raymond Choo, Mehran Mozaffari Kermani, Reza Azarderakhsh, Manimaran Govindarasu, "Emerging Embedded and Cyber Physical System Security Challenges and Innovations" , IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 14, NO. 3, MAY/JUNE 2017

[11] Jairo Giraldo, Esha Sarkar, Alvaro A. Cardenas, Michail Maniatakos and Murat Kantarcioglu, "Security and Privacy in Cyber–Physical Systems: A Survey of Surveys", IEEE, Cyber–Physical Systems Security and Privacy, July/August 2017

[12] Iman Shames , Farhad Farokhi, Tyler H. Summers, "Security analysis of cyber-physical systems using $\mathcal{H}2$ norm", IET Control Theory Appl., 2017, Vol. 11 Iss. 11, pp. 1749-1755

[13] Jun Yang, Chunjie Zhou , Shuanghua Yang, Haizhou Xu , Bowen Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 65, NO. 5, MAY 2018