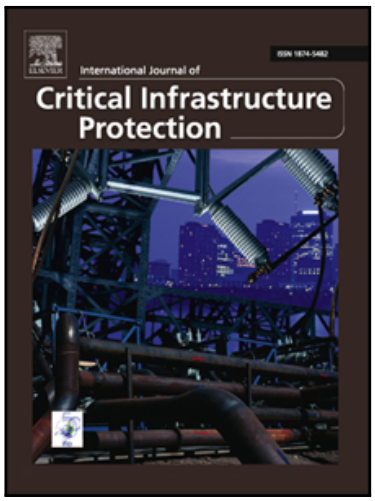

Evaluation of Vulnerable Path: Using Heuristic Path-finding Algorithm in Physical Protection System of Nuclear Power Plant

Zou Bowen , Yang Ming , Zhang Yuxin , Benjamin Emi-Reynolds , Tan Ke , Wu Wenfei , Yoshikawa Hidekazu

PII: S1874-5482(17)30013-6
DOI: https://doi.org/10.1016/j.ijcip.2018.08.006
Reference: IJCIP 265

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 18 February 2017
Revised date: 16 May 2018
Accepted date: 3 August 2018

Please cite this article as: Zou Bowen , Yang Ming , Zhang Yuxin , Benjamin Emi-Reynolds , Tan Ke , Wu Wenfei , Yoshikawa Hidekazu , Evaluation of Vulnerable Path: Using Heuristic Path-finding Algorithm in Physical Protection System of Nuclear Power Plant, *International Journal of Critical Infrastructure Protection* (2018), doi: https://doi.org/10.1016/j.ijcip.2018.08.006

Evaluation of Vulnerable Path: Using Heuristic Path-finding Algorithm in Physical Protection System of Nuclear Power Plant

Zou Bowen [a,*], Yang Ming [a,b,*], Zhang Yuxin [b], Benjamin Emi-Reynolds [b], Tan Ke [c], Wu Wenfei [c], Yoshikawa Hidekazu [a,b]

[a] *School of Electric Power, South China University of Technology, Guangzhou 510641, China*

[b] *Fundamental Science on Nuclear Safety and Simulation Technology Laboratory, Harbin Engineering University, Harbin 150001, China*

[c] *China Guangdong Nuclear Power Engineering Design Co. Ltd., Shenzhen 518116, China*

Abstract: A novel heuristic path-finding method named "Heuristic Path-finding for the Evaluation of PPS effectiveness, HPEP" was proposed for the evaluation of a vulnerable intrusion path in Physical Protection System (PPS). According to the design basis threat (DBT), HPEP takes the detection probability and interruption probability as heuristic information to analyze the vulnerable adversary path. Moreover, HPEP can find the shortest path for the response force to reach the target in the first attempt and guarantees interruption of an adversary intrusion. Three types of simulation experiments are studied for the feasible analysis of HPEP method. The analysis of main parameters in the simulation results will provide detailed and comprehensive technical information for the redesign and upgrade of the PPS.

Index Terms: Heuristic path-finding algorithm, safeguard application, Physical protection system

1. Introduction

A Physical Protection System (PPS) (also called security system) integrates people, procedures, and equipment to protect assets and facilities against theft, sabotage, and other malevolent human attacks [1]. The main threats for nuclear materials and facilities are however natural disasters rather than malicious human actions since human adversaries must learn and adapt to intrude nuclear power plants (NPPs). The security of nuclear materials and facilities became key protection objects for most countries in the 1970s, and some relevant conventions on the PPS entered into force.

The PPS analysis methodology named "Design and Evaluation Process Outline, DEPO" is the design and evaluation process for PPS that starts with determining objectives, then designing a system to meet the objectives, and ends with an evaluation of PPS effectiveness to verify that the system performs well compared to the objectives [2]. So far, some methods for the evaluation of PPS effectiveness have been proposed. The basic established analysis method used in the DEPO was "Estimate of Adversary Sequence Interruption, EASI" approach that was developed by Sandia National Laboratory (SNL) in the 1970s [3].

In the 1980s, SNL developed another method called "Systematic Analysis of Vulnerability to Intrusion, SAVI" which was on the basis of the EASI approach for the evaluation of multi-path in PPS [4]. If the detailed data of the threat, target, facility, site-specific PPS elements, and the response force time is confirmed, the 10 most vulnerable paths can be calculated by the SAVI platform. Later, for the analysis of the threat from insiders and outsiders, a comprehensive method named "Analytic System and Software for Evaluating Safeguards and Security, ASSESS" was developed by the Department of Energy (DOE) [5].

The aforementioned evaluative methods and software tools were only used in the one-dimensional model. The researchers of Korea Institute of Nuclear Non-proliferation and Control presented a novel method named "Systematic Analysis of Physical Protection Effectiveness, SAPE" which can be used in two-dimensional models [6].

In previous work, an integrated platform for analysis and design (IPAD) was proposed to evaluate the PPS effectiveness in three-dimensional models [7]. By combining the functions of three-dimension modeling of PPS with two-dimension drawing (such as CAD drawings) generation, IPAD provides designers with comprehensive and visualized information of

PPS in one platform and enables a quick and convenient design of PPS. However, IPAD adopts EASI approach as the basic theoretical analysis method to analyze the PPS effectiveness. Moreover, IPAD applies a heuristic approach (HAPPS) [8] for the evaluation of Physical Protection System Effectiveness, which is combined EASI approach and Ant Colony Optimization (ACO) algorithm. If the assignment of parameters are not appropriate, ACO algorithm as a heuristic algorithm is easy to cause the results do not convergence, local optimum, and time-consuming.

In this paper, a modified method is presented on the basis of SAPE and EASI approaches. In the PPS, the evaluation of vulnerable path can come down to path-planning. Different design basis threat (DBT) signify different intrusion path. SAPE method uses A* algorithm as heuristic path-finding approach to evaluate the PPS effectiveness.

Different from the SAPE method, a novel and comprehensive method named "Heuristic Path-finding for the Evaluation of PPS effectiveness, HPEP" presents another intrusion mode. Heuristic information only considers detection probability. In this paper, contrastive analysis of the value of the heuristic information will help analysts to select the best way. Using A* algorithm for path-finding will not seek the most vulnerable intrusion path if heuristic information is considered. However, for non-heuristic information, A* algorithm will be equivalent to the Dijkstra algorithm [9] that can seek the most vulnerable intrusion path which is described in detail.

Hypothetically, HPEP method only considers an adversary intruding the NPPs and the basic function of PPS is to protect NPPs. If a group of adversaries intrude NPPs, the response forces have a main responsibility to interrupt the intrusion actions when the PPS detects the adversaries. This paper assumes that insiders only provide intrusion of convenience such as some sensors fail to detect and the delay devices are out of action. Also, the primary targets in this paper are assumed as physical assets, electronic data, or anything that could impact the critical facilities operations. The secondary targets are some PPS components, defense devices, detection devices, or others can reduce the PPS effectiveness [1].

The simulation model for the path-finding of PPS will be briefly introduced. HPEP method includes three path-finding modes. It uses detection probability and interruption probability as heuristic functions to seek the vulnerable intrusion path and takes the response force time as heuristic information to find the shortest path for the response force reaching the target in time. This is discussed in detail. Moreover, three simulation experiments study on the PPS evaluation will be presented.

2. Simulation Modeling

In this paper, take Autodesk Computer Aided Design (AutoCAD) as a preliminary model tool for the design drawings of PPS. This is the common method used in NPPs and has been used in the previous work. It is convenient to interactively invoke CAD drawings [10] and identify the controls (equipment) of the models for the evaluation of PPS effectiveness. During the PPS design stage, designers by means of CAD secondary development, transfer equipment data as extended data stored in each equipment, which will be easy for third-party simulation platforms to load the drawings data. Also, two-dimension CAD drawings and three-dimension CAD drawings can be mutually transformed for a thorough bird's-eye view of PPS showed in figure 1.

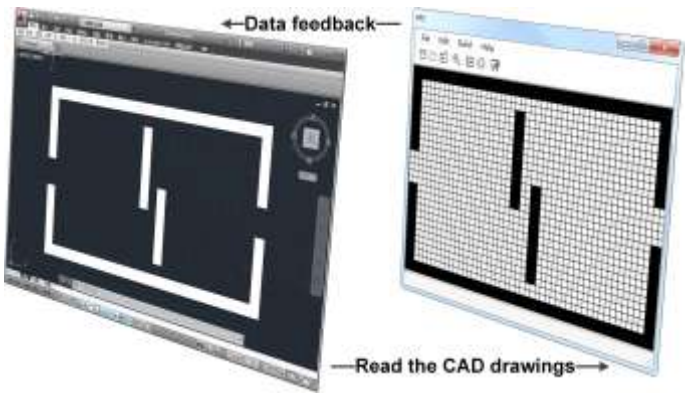

Figure 1. The CAD drawing mutually transform for a thorough bird's-eye view of PPS.

The primary PPS functions are delay, detection, and response. The value or parameters of two protection devices,

including delay devices and detection devices. As shown in the figure 2, the delay devices delay adversary intrusion progress by people, barriers, locks, and activated delays; the detection devices detect the adversary action including covert or over actions.

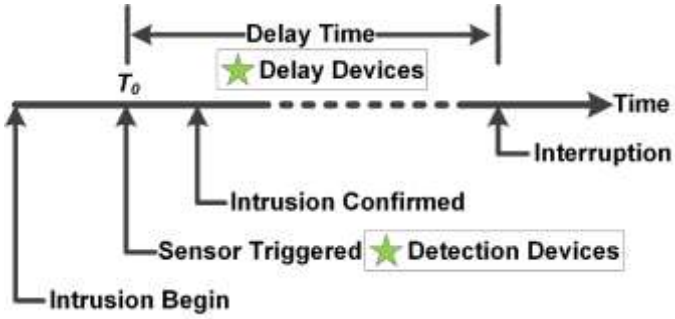

Figure 2. The role of protective devices for the prevention of adversary intrusion.

Delay devices: the main function of delay devices is to delay the adversary intrusion for the addition of a response force time. In this paper, the analysis data sources can be invoked by device properties such as delay time, install regions, devices category or barrier types, etc.

In the NPPs, access delay barriers are composed of passive barriers, security guards and dispensable barriers. Passive barriers include structural elements such as doors, locks, vents, walls, floors, fences, ducts, etc. which will be assigned relevant values to illustrate the impact on the PPS effectiveness. Security guards can detect adversaries in a patrolling area and provide delay measures to reduce further threat. The dispensable barriers include some delay facilities such as chemical smokes, fogs, foams, irritants, etc., which can be deployed rapidly to delay adversary intrusion when necessary.

The delay devices have low value for the PPS before the sensors detect the adversary intruding NPPs. According to the previous work, the delay time of inner layer protective devices should be more than the outer layer protective devices because the inner layer protective devices are more sensitive than the outer ones.

Detection devices: to detect adversary intrusion events and give an alarm for response forces to interrupt it. The detection devices comprise some sensor devices used in NPPs such as active and passive infrared sensors, microwave sensors, sonic sensors, vibration sensors, and video cameras. In this paper, only infrared sensors are considered and it was assumed that the detection probability decreased with detection distance linearly but does not change with time in a fixed area. Regardless of the coverage model of sensors, the detection probability is dependent on the distance between the sensors' location and a particular area point [11], which will be saved in the mesh properties.

The properties of the detection devices are detection probability, detection region, detection category, detection area, etc. Different from delay protective devices, the earlier an adversary intrusion is detected, the faster the response force will reach the target to interrupt the adversary. Thus, the detectability of outer layer sensors should be higher than the inner layer sensors.

3. Fundamentals of HPEP method

3.1 Basic A* algorithm for path-finding

The HPEP method adopts heuristic path-finding algorithm to reduce the computer resource in a large two-dimensional model. When a virtual character moves from the current position to the next position, the HPEP method can judge its actions such as where it leaves and where it will reach, and calculate a rough path. It then refines the rough path in each region.

A* algorithm is applied in a static grid for path planning. Compared with other path-finding algorithm, the A* algorithm has high search efficiency on seeking the shortest path. A* algorithm selects path according to the minimum value of

$$F(n) = G(n) + H(n) \tag{1}$$

where n is the last node on the path; $G(n)$ is the cost function of the path from the start node to n node (known function, it is breadth-first search); $H(n)$ is a heuristic that estimates the cost of the cheapest path from n node to the target node (unknown function, it is depth-first search). For the algorithm to find the actual shortest path quickly, the

heuristic function $H(n)$ should be more accurate.

Assume $H(n)=0$, that is without considering the heuristic information, A* algorithm into Dijkstra algorithm enumerates all the possible paths and seeks the most vulnerable one. Take the simplified case shown in figure 3 to illustrate the analysis process of the Dijkstra algorithm as follows:

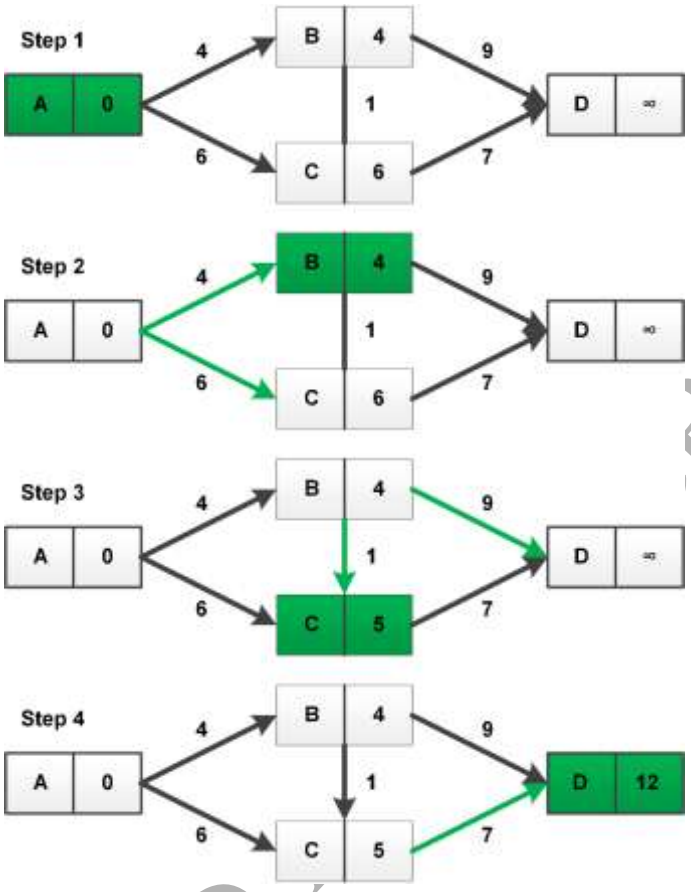

Figure 3. A simplified case for the explanation of Dijkstra algorithm.

Definition: S is the set of the certain shortest path points, U is the set of the uncertain shortest path points. According to the value between two points, the following parameters are initialized; A=0, B=4, C= 6, D = ∞.

Step1: select A as start point, then S=<A>, the shortest path is A->A, and A is the intermediate point.

U=<B, C, D>, A->B=4 and A->C=6, so A->B is the shortest path, select B point. Mark B=4, and C=6.

Step2: S=<A, B>, B is the intermediate point.

U=<C, D>, A->B->C=5 and A->C=6, so the shortest path is A->B->C, select C point. Mark C=5.

Step3: S=<A, B, C>, C is the intermediate point.

U=<D>, A->B->C->D=12 and A->B->D=13, so A->B->C->D is the shortest path. Mark D= 12.

Step4: U is empty, end.

3.2 Modified A* algorithm in the HPEP method for PPS

According to the different heuristic information, including detection probability and EASI approach, A* algorithm is modified for the evaluation of the adversary intrusion path. Use the response force time as heuristic information for the analysis of the guard path.

1) Path-finding: Detection probability in the HPEP method

Detection probability of sensors is only considered to estimate whether the adversary intrusion path is vulnerable or not. Wang B. has summarized the sensors coverage problem of finding penetration paths and presented a survey on various coverage problems in sensor networks [11], including 1. Maximal Breach Path, which is a way to find the least detection probability path, and was used by Meguerdichian S. et al [12] and Megerian S. et al. [13]. 2. Maximal Support Path method

uses the Euclidean distance between some area and its closet sensor as the coverage measure to seek the highest detection probability path [13]. 3. Exposure path is used to detect a moving target and find a path with the minimum exposure connecting two areas. It takes some measures to provide more network coverage that can increase the path exposure and decrease intrusion success probability. 4. Detection Path is applied to calculate the detection probability of a penetration path. In order to seek the maximal breach path, this paper uses A* algorithm as heuristic search function as follows.

In the search process, A* algorithm can be controlled to estimate a best path rather than blindly searching a path. If there exits $G(n) \le G^*(n)$, ($G^*(n)$ is the minimum estimate of $G(n)$ by A* algorithm) and $H(n) \le H^*(n)$, ($H^*(n)$ means the minimum estimate of $H(n)$ and depends on the heuristic information, which is termed the evaluation function), A* algorithm will find a best (vulnerable) path when the value of $F(n)$ is a minimum. Assuming that the criterion of intrusion event failure is the adversary being detected, then formula (1) is $P(D) = P(D)_G + P(D)_H$, where $P(D)_G$ is $G(n)$ and $P(D)_H$ is $H(n)$.

$$P(D)_G = P(D_1) + P(D_2) \times [1 - P(D_1)] + P(D_n) \times \prod_{i=1}^{n} [1 - P(D_{n-1})] \tag{2}$$

$$P(D)_H = \prod_{i=1}^{n} [1 - P(D_n)] \times h(p) \tag{3}$$

$P(D)_G$ is regarded as cost function of A* algorithm ($G(n)$). $G(n)$ is a constant value for real-time computing the detection probability from the start node to node n. n is the current node that the adversary intruded, t is the target node. i is one of the intermediate nodes which has been intruded and real-time represent adversary intrusion actions. $h(p)$ is impact factor for evaluating the $H(n)$. If $h(p) = 0$ for all grids, A* will be equivalent to Dijkstra algorithm which will reduce the search efficiency. Here, analogy analysis of Manhattan Distance which means the distance between (n_x, n_y) and (t_x, t_y) is $|n_x - t_x| + |n_y - t_y|$ in the Cartesian Coordinates, and $h(p)$ is detection probability between two points in a grid based on a strictly horizontal and vertical path. $h(p)_{X \to Y}$ means the calculation of detection probability along with the imaginary line marked $X \to Y$ as shown in figure 4, $h(p)_{Y \to X}$ is the calculation of detection probability along with the imaginary line marked $Y \to X$.

$$\begin{cases} h(p)_{X \to Y} = P(D_{n+1}) + P(D_{n+2}) \times [1 - P(D_{n+1})] + P(D_t) \times \prod_{i=1}^{t-m-1} [1 - P(D_{n+i})] \\ h(p)_{Y \to X} = P(D_{n+1}) + P(D_{n+2}) \times [1 - P(D_{n+1})] + P(D_t) \times \prod_{i=1}^{t-m-1} [1 - P(D_{n+i})] \\ h(p) = \dfrac{h(p)_{X->Y} + h(p)_{Y->X}}{2} \end{cases} \tag{4}$$

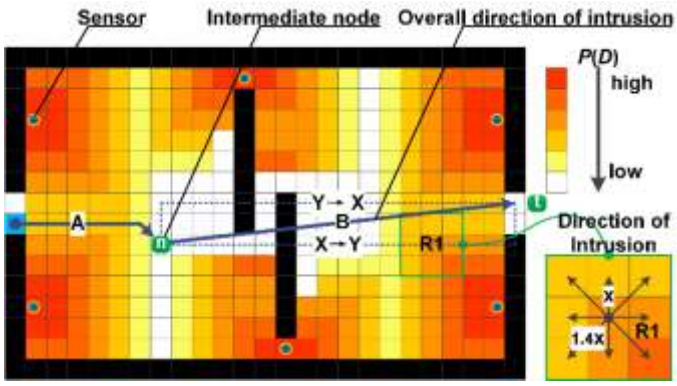

Figure 4. Sketch map for the grid generation, the detection distribution, and direction of movement.

The figure 4 is a sketch map for the grid generation, the detection distribution, and the direction of movement. Sensors are regarded as detection devices to detect the adversary actions and take the black areas as defense devices to delay the adversary intrude critical infrastructure. The detection probability $P(D)$ is attenuated with the detection distance that showed as the red to the white color in figure 4. The bottom right corner of the figure 4 shows the adversary has eight intrusion directions to access the target.

Thus, the basic steps of A* algorithm are: using two lists, OPEN list and CLOSED list, to store the data. One array is initialized to store the non-detection probability of where the adversary moved. Use the OPEN list to store unanalyzed node (region) and the CLOSED list to store parsed node. The pseudocode of A* algorithm for searching vulnerable path:

1. Create a search graph G as shown in figure 4, adding the initial position into the OPEN list;
2. Analyze the OPEN list

(1) If the data is in the OPEN list, select the minimum value of $P(D)$ as the current node, remove it from OPEN, and put it on the CLOSED list. For example, if the adversary moved to the R1 (region m), there are seven directions to be selected for the next intrusion. Then, multiply non-detection probability $\prod_{i=1}^{n}[1-P(D_{n-1})]$. Calculate the detection probability from R1 to the target as formula (3). Finally, count up $P(D)_G$ and $P(D)_H$ to select the minimum $P(D)$ for the next path-finding.

(2) If the OPEN list is empty, exit with failure;

(3) If the current node is the target, vulnerable path finding is successful and go to step 4.

3. Analyze the directions of adjacent node

(1) If the node prohibits passage or is already in the CLOSED list, skip this step;

(2) If the node is not in the OPEN list, put it on OPEN list;

(3) If the node is already in the OPEN list, using the value of formula $P(D)$ to check whether the new path is more vulnerable than current adversary path, update the value of $P(D)_G$ and $P(D)$.

4. According to the node information in the CLOSED list, backward extract the vulnerable adversary path.

2) Path-finding: EASI approach in the HPEP method

On the basis of the EASI approach [2][3], the probability of interruption is used for the comprehensive evaluation of the PPS effectiveness. The higher the probability of interruption, the more effective the PPS protects the nuclear facilities and materials. In this section, EASI approach and A* algorithm are used to evaluate the effectiveness of PPS. The calculation steps are the same as the mentioned path-finding for adversary intrusion but the heuristic information is different.

If the response force wants to interrupt the adversary intrusion, the response force time (RFT) should be lower than the time remaining (TR) for the adversary to reach the target, that is

$$\frac{TR}{RFT} > 1 \tag{5}$$

For the calculation of the probability of response force arrival prior to the end of the adversary's action sequence ($P(R|A)$), Norichika Terao and Mitsutoshi Suzuki presented a novel method [14] which takes the random variables TR and RFT as a gradually decreasing probability distribution, rather than the normal distribution. Using Poisson distribution to describe the distribution of $P(R|A)$ as expressed in equation (6).

$$P(X=k)=\frac{\lambda^k e^{-\lambda}}{k!} \tag{6}$$

where k is natural number and indicates the number of times the events occurred and λ is a positive number which indicates the average occurrence rate. That is, the probability of $P(R|A)$ that an event occurred k times under the average occurrence rate (λ times).

$$P(R|A_i)=1-e^{-\lambda_i} \tag{7}$$

For the adversary intrusion path, assuming λ_i is a calculated value to measure RFT_i and TR_i at the i^{th} barrier, which is

$$\lambda_i = \frac{TR_i}{RFT_i} \tag{8}$$

Thus, $k = 0$ means events will not occur, $P(X = 0) = e^{-\lambda}$. In the case events happened, the probability of $P(R \mid A)$ is

$$P(R \mid A_i) = 1 - P(X = 0) = 1 - e^{-\lambda_i} \tag{9}$$

Hence, for a single detection sensor device, the probability of interruption is given by

$$P(I) = P(D) \times P(C) \times P(R \mid A) \tag{10}$$

where, $P(C)$ is the probability of communication to the response force.

As shown in figure 5, for multiple detection sensor devices in one adversary path, if the pre-regions did not detect adversary intrusion action and the current region did, then the interruption probability is updated as

$$\begin{aligned} P(I)_t &= P(D_1) \times P(C_1) \times P(R \mid A_1) \\ &+ \sum_{i=2}^{t} P(D_i) \times P(C_i) \times P(R \mid A_i) \prod_{j=1}^{i-1} (1 - P(D_j)) \end{aligned} \tag{11}$$

Assuming $P(I)$ is a heuristic formula, then $P(I)$ will be decomposed to two parts, $P(I)_G$ and $P(I)_H$.

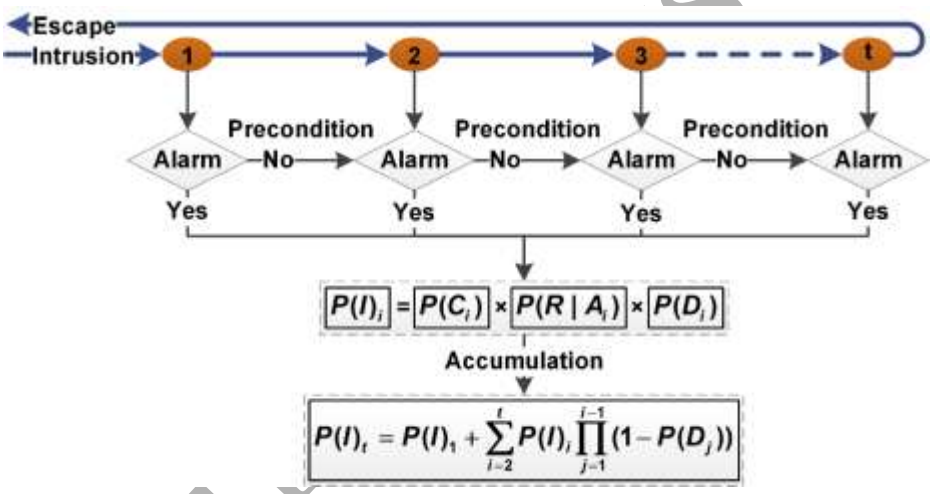

Figure 5. Adversary path. In order to intrude successfully, the adversary should go through n regions and escape the facility.

$$\begin{aligned} P(I)_G &= P(D_1) \times P(C_1) \times P(R \mid A_1) \\ &+ \sum_{i=2}^{m} P(D_i) \times P(C_i) \times P(R \mid A_i) \prod_{j=1}^{i-1} (1 - P(D_j)) \end{aligned} \tag{12}$$

$$P(I)_H = 0 \tag{13}$$

and $P(I) = P(I)_G + P(I)_H$.

$P(I)_G$ is regarded as cost functions of A* algorithm ($G(n)$), which is used to compute the probability of effectiveness from the start node to n.

$P(I)_H$ is equaled to the heuristic function $H(n)$ and it is difficult to find an optimal function to describe it because more than one parameter should be calculated. Thus, $P(I)_H = 0$.

As shown in the figure 4, the movement time T between two adjacent grids is

$$T = \begin{cases} \dfrac{1.4 \times x}{v} & \textit{if path is diagonal in the mesh} \\ \dfrac{x}{v} & \textit{otherwise} \end{cases} \tag{14}$$

The time remaining TR is accumulated by multiple T. This paper defines TR as $TR = d/v$, where v is adversary

intrusion velocity which will be assigned different values in the different regions according to the simulation circumstance and d is the Manhattan Distance from the current location to the target. Also, TR is the cumulative value from the current position to the target position, which can be the accumulated conservative delay time of the inside protective region.

3) Path-finding: Response Force Time

Path-finding for the response force to reach the target the first time and guarantee to interrupt the adversary intrusion. Different from adversary intrusion, path-finding algorithm only considers some specific area and determines whether the response force can pass or not. Take moving time as heuristic information to seek a shortest path, which is calculated according to formula (14) and the moving velocity assigned the realistic value.

Assuming that the shortest path means the time cost least, then the formula (1) can be equivalent to $RFT = RFT_G + RFT_H$, which RFT_G is $G(n)$ and RFT_H is $H(n)$.

$$\begin{cases} RFT_G = \sum_{i=1}^{n} RFT_i \\ RFT_H = \begin{cases} \dfrac{\sqrt{(n_x - t_x)^{\wedge 2} + (n_y - t_y)^{\wedge 2}}}{v} & \text{Euclidean distance} \\ 0 & \text{Non-heuristic} \end{cases} \end{cases} \tag{15}$$

where, n_x, n_y is the current position, and t_x, t_y is the target position. Using Euclidean distance to calculate the heuristic distance, the heuristic response force time will be calculated.

The calculation steps are the same as the path-finding for adversary intrusion. For the non-heuristic information, the accurate shortest path will be sought, but is time consuming. If considered, the heuristic information, such as Euclidean distance, Manhattan distance, etc. the path may not be the shortest but saves time for the analysis of the response path.

4. Simulation Experiments for the Feasible Analysis of HPEP method

In this paper, according to the different levels of DBT needed to conduct two experiments, the first experiment considers the low level of DBT (such as outsiders who do not know the detailed information of NPPs) and evaluates the lowest detection probability of the adversary intrusion path; the second experiment considers the high level of DBT which may be colluded with insiders and evaluates the lowest interruption probability like the experiment one. The Insider is defined as anyone who has knowledge of the NPPs operations or security system and has unescorted access to the critical facilities or security interests [1]. Depending on the capacity of insiders, insiders can be divided into three sub-categories:

1) Passive, the insiders only provide information such as targets and security system;

2) Active nonviolent, the insiders help the adversary to intrude quickly and secretly into the facility and disable alarms and communications along the adversary path. The simulation data such as detection probability, the communication probability can decrease to simulate this reality;

3) Active violent, the insiders participate in a violent attack personally, which means some relatively protective devises and sensors are put out of action.

Thus, case I is for the low threat level, case II is for the high threat level. The third experiment is to seek the shortest path for the response force.

In the figure 4, the black grid means the block grid where the adversary cannot go through; the different color grid means the detection probability distribution. The red grid means high detection probability and the white grid shows low detection probability.

In the PPS, the probability of communication to the response force $P(C)$, mean time and standard deviation of the response force time are given in table 1. The value of $P(C)$ and response force time can be obtained by reality security training and assigned a constant value.

Table 1

The hypothetical simulation parameter data from NPPs security department.

Probability of Communication to the response force $P(C)$	Response Force Time (Seconds)	
	Mean Time	Standard Deviation
0.95	100	90

Sensors	$P(D)$	Attenuation rate (linear)	Install location
IR1	0.95	-0.085	L1
IR2	0.95	-0.085	L2
IR3	0.95	-0.085	L3
IR4	0.95	-0.085	L4
IR5	0.95	-0.085	L5
IR6	0.95	-0.085	L6

4.1 Hypothetical Case I

In this paper, case I considers detection probability as the heuristic information. In most cases, the detection probability is attenuated with the distance between an area point and sensors. Some researchers proposed different sensor coverage models, including Boolean sector coverage models [15], attenuated disk coverage models [16] [17], truncated attenuated disk models [18], detection coverage models [19] [20], and estimation coverage models [21] [22]

For the simplification calculation, assuming that the detection probability attenuated with detection distance linearly, $\frac{\partial P(Detection)}{\partial Distance} = constant < 0$. The hypothetical simulation parameter data of sensors include the highest detection probability, attenuation rate (linear), and install location as shown in table 1. Monte-Carlo simulation method is used for the hypothesis of the sensors data, so that all conditions which may occur will be traversed in reality.

The impact of non-heuristic path planning and heuristic path planning on the adversary intrusion path is then analyzed. As shown in the figure 6.A and figure 6.C, the green grid means the possible intrusion grid where the algorithm is already searched and the blue grid shows the adversary intrusion path.

1. Non-heuristic information for A* algorithm, ($h(p)=0, H(n)=0$)

A* algorithm will be equivalent to Dijkstra algorithm on the premise of non-heuristic information. According to the Dijkstra algorithm, the accurate adversary path will be sought. The Real line means the calculation value of the cost function in the algorithm and the Detection line is the detection probability of each grid in the adversary intrusion path as given in figure 6.B.

According to the intrusion grids, mark the vulnerable area and enhance the detection probability of sensors time by installing more sensors or upgrading to high performance sensors. In figure 6.A and figure 6.B, the detection probability of intrusion increased with the intrusion distance and the adversary path tends to the low detection probability area. If there are no insiders giving assistance, the adversary intrusion path is composed of low detection area in reality, which only can prevent the adversary who is a lower DBT.

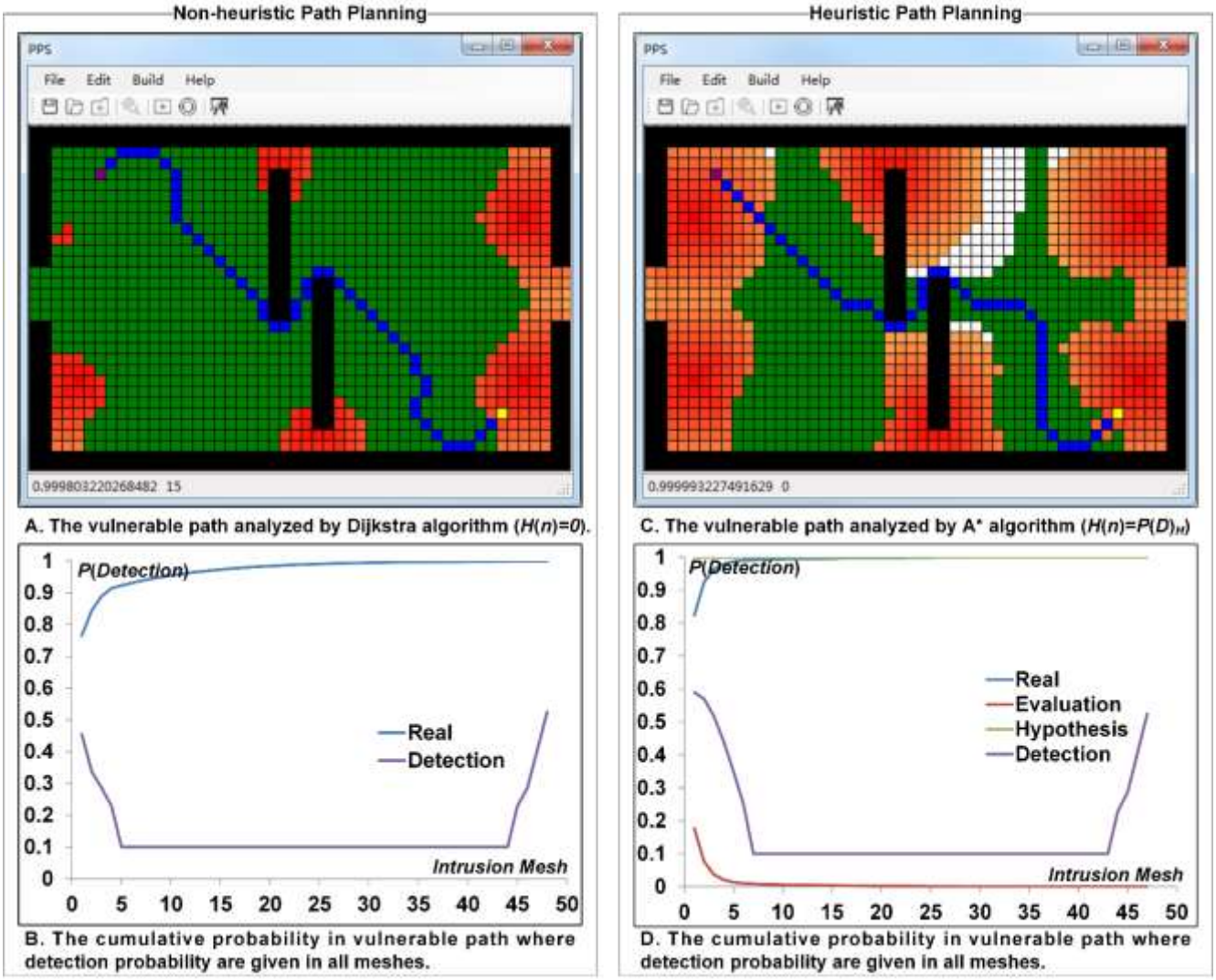

Figure 6. Non-heuristic path planning and heuristic path planning for the evaluation of PPS effectiveness.

2. Heuristic information for A* algorithm, ($h(p) \neq 0, H(n) \neq 0$)

As a mentioned method for the calculation of heuristic formula analogy, analyze the standard Manhattan distance to get a relatively accurate heuristic information. According to the figure 6.C and figure 6.D, the Hypothesis line is the calculation value of the heuristic function ($P(Detection)$), the Evaluation line means the results of a heuristic that estimates the cost of the cheapest path from the current node to the target node.

The cumulative detection probability of non-heuristic information in A* algorithm (Dijkstra algorithm) is less than A* algorithm has heuristic information. The search field and search time are less than the non-heuristic search method, but the intrusion path is not the most vulnerable path.

Table 2

The simulation results for the Non-heuristic path planning and heuristic path planning of A* algorithm.

A* algorithm	Distance (grid)	Time(s)	Cumulative Probability
Non-heuristic	48	1.26847	0.99980
Heuristic	47	1.19083	0.99999

The search algorithm will search in all directions with an equal probability because of non-heuristic information that will cost the longest time to seek the vulnerable path. The analysis data are given in table 2. As shown in figure 6.A, obviously, the number of green grids is more than figure 6.C. Thus considering for analysis the adversary path without real-time calculation, non-heuristic information for A* algorithm (Dijkstra algorithm) is the best choice for the path-planning. Real-time calculation and analysis of PPS can be used in the virtual training.

4.2 Hypothetical Case II

Using interruption probability as heuristic information which contains more sensitive values for the analysis of adversary intrusion, the effectiveness of PPS also can be analyzed and the vulnerable adversary intrusion path will be sought. According to the EASI approach, the lowest interruption probability of the adversary path represents the most vulnerable path. It is difficult to guarantee the effectiveness of heuristic information because the multiple parameters change with the process of path-finding. Thus, non-heuristic information for A* algorithm path-planning is the best choice for the analysis of PPS effectiveness.

The intrusion velocity is fixed to a normal value, $1.5\,m/s$. Different protective regions have different communication probability ($P(C_i)$), but in this paper, we assign the same value. Each grid has its own conservative value of TR, and RFT is a constant value that is assigned 100s.

Using the simulation platform, the analysis results will be graphically displayed, and the vulnerable path can be located the first time as shown in figure 7.A. Even if many factors influence the interruption probability, the HPEP method can provide sufficient visual information for further evaluation of PPS effectiveness by the two-dimensional simulation model.

As shown in figure 7.B, the interruption probability increased with the progress of the adversary intrusion and approached a definite value.

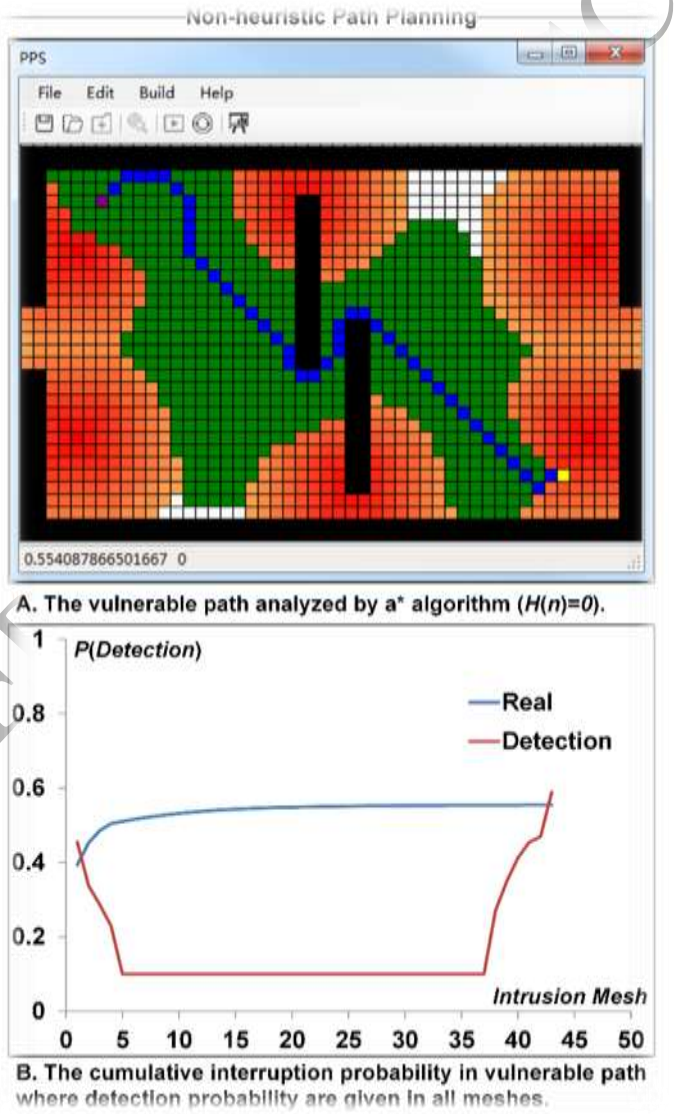

Figure 7. The second heuristic path planning algorithm for the evaluation of PPS effectiveness.

4.3 Hypothetical Case III

Assuming that the minimum response force time represents the shortest path and assigning the response force moving

velocity for the calculation of shortest path, $v = 3m/s$. As shown in figure 8, non-heuristic and heuristic path planning will seek a different path. The non-heuristic path is better than the heuristic path, but costs more time to find it.

For the virtual training, the A* algorithm for the real-time calculation of response force path is the best way. The simulation platform enables users to manually modify the path block or not. The simulation results can be used as standard regulations to check reality training of the response force, whether qualified or not.

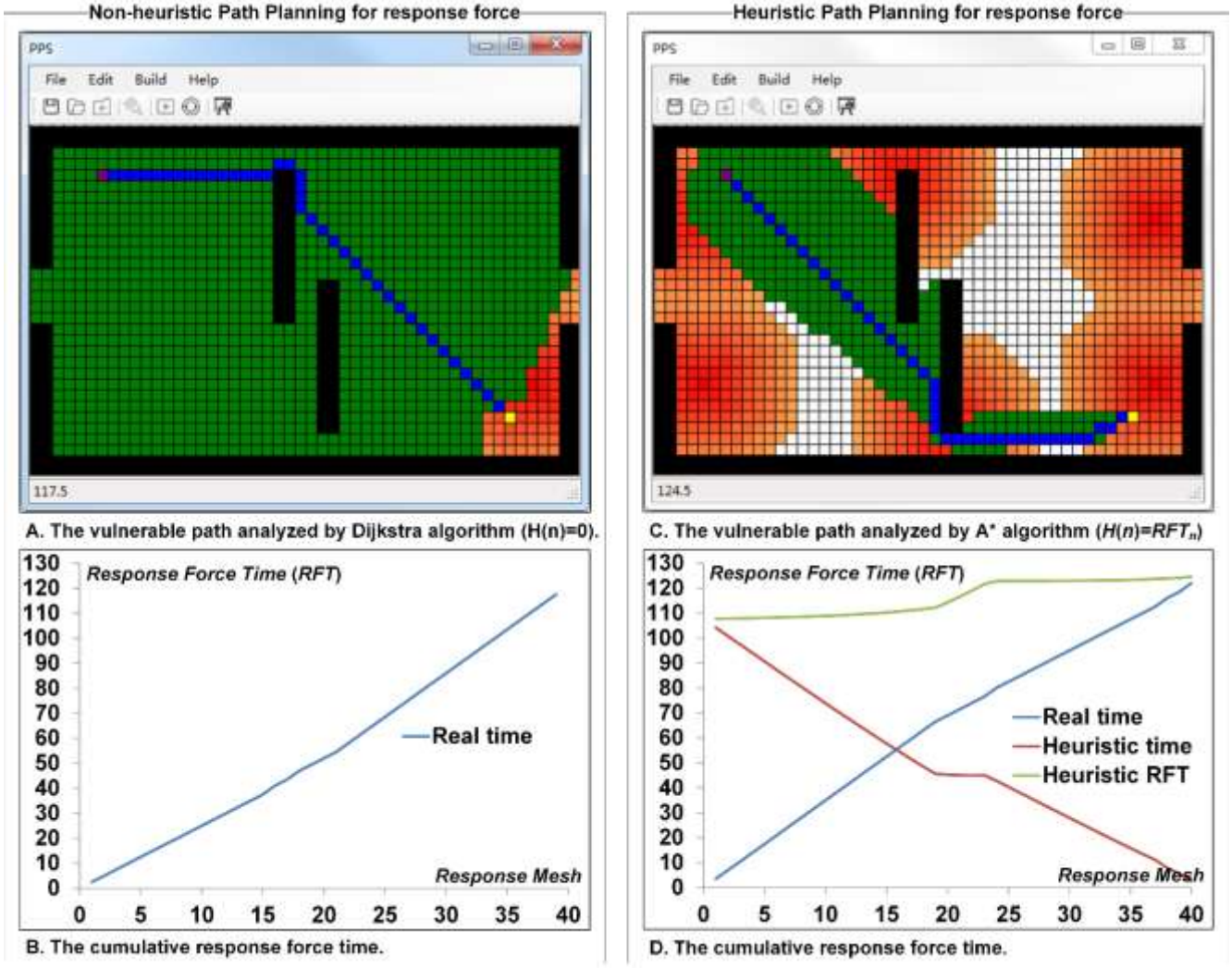

Figure 8. Non-heuristic path planning and heuristic path planning for the calculation of the response force path.

5. Conclusion

The experimental results confirm that the HPEP method for the evaluation of PPS effectiveness is available and successful. For HPEP method, it will be time-consuming to seek an accurate vulnerable adversary path when using non-heuristic information, or time-saving to calculate a relative vulnerable adversary path when using appropriate heuristic information. HPEP has rapid searching capability which is a requirement for some engineering applications such as virtual reality training.

The current study is based on DBT to modify A* algorithm for the analysis of the adversary behavior and use common A* algorithm to calculate a fast path. The simulation results will provide detailed and comprehensive technical information for the redesign and upgrade of PPS. Additionally, using heuristic algorithm for the evaluation of PPS effectiveness can be applied in virtual reality, which will be completed in the following work.

References

[1] M. L. Garcia, Design and evaluation of physical protection systems. 2nd ed. Burlington, MA, USA: Butterworth-Heinemann, 2007.

[2] M. L. Garcia, Vulnerability assessment of physical protection systems. Burlington, MA, USA: Butterworth-Heinemann, 2005.

[3] H. A. Bennett, "EASI approach to physical security evaluation," Sandia Lab., Albuquerque, NM, USA, Tech. Rep. SAND-76-0500, 1977.

[4] J. C. Matter, SAVI: A PC-Based Vulnerability Assessment Program, SAND88-1279. Albuquerque, NM: Sandia National Laboratory, 1988.

[5] R. A. AI-Ayat, T. D. Cousins, E. R. Hoover, "ASSESS Update–Current Status and Future Developments," Lawrence Livermore Nat. Lab., Livermore, CA, USA, Tech. Rep. UCRL-JC-104360, 1990.

[6] S. S. Jang, S. W. Kwan, H. S. Yoo, J. S. Kim, W. K. Yoon, The Tile-map Based Vulnerability Assessment Code of a Physical Protection System: SAPE (Systematic Analysis of Protection Effectiveness), The International Nuclear Information System, Vol. 39(44), 2008.

[7] B. W. Zou, M. Yang, H. Yoshikawa, H. X. Lu, Evaluation of Physical Protection Systems Using an Integrated Platform for Analysis and Design, IEEE Transactions on SMC, Vol. 47(11), PP. 2945-2955, 2016.

[8] B. W. Zou, M. Yang, J. Guo, E. R. Benjamin, W. F. Wu, A heuristic approach for the evaluation of Physical Protection System effectiveness, Annals of Nuclear Energy, Vol. 105, PP. 302-310, 2017.

[9] M. L. Hetland, Python Algorithms: mastering basic algorithms in the Python Language, Apress, 2014.

[10] E. Gindis, Up and Running with AutoCAD 2016: 2D and 3D Drawing and Modeling, Academic Press, 2015.

[11] B. Wang, Coverage problems in sensor networks: A survey, ACM Computing Surveys (CSUR), Vol. 43(4), PP. 1-53, 2011.

[12] M. Cardei, J. Wu, Coverage problems in wireless ad hoc sensor networks, Handbook of Sensor Networks, 2004.

[13] S. Megerian, F. Koushanfar, M. Potkonjak, M. B. Srivastava, Worst and best-case coverage in sensor networks. IEEE transactions on mobile computing, Vol. 4(1), PP. 84–92, 2005.

[14] N. Terao, M. Suzuki, A Probabilistic Extension of the EASI Model, Journal of Physical Security, Vol. 7, PP. 12-29, 2014.

[15] M. Cardei, J. Wu, M. Lu, M. O. Pervaiz, Maximum network lifetime in wireless sensor networks with adjustable sensing ranges, In Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2005), PP. 438–445, 2005.

[16] S. Megerian, F. Koushanfar, G. Qu, G. Veltri, M. Potkonjak, Exposure in wireless sensor networks: Theory and practical solutions, Wireless Networks, Vol. 8(5), PP. 443–454, 2002.

[17] G. Veltri, Q. Huang, G. QU, M. Potkonjak, Minimal and maximal exposure path algorithms for wireless embedded sensor networks, Proceedings of the ACM International Conference on Embedded Networked Sensor Systems, PP. 40–50, 2003.

[18] Y. Zou, K. Chakrabarty, A distributed coverage-and connectivity-centric technique for selecting active nodes in wireless sensor networks, IEEE Transactions on Compuers, Vol. 54(8), PP. 978–991, 2005.

[19] E. Onur, C. Ersoy, H. Delic, Finding sensing coverage and breach paths in surveillance wireless sensor networks, Personal, Indoor and Mobile Radio Communications, 2004, PIMRC 2004, 15th IEEE International Symposium on. IEEE 2004, Vol. 2, PP. 984-988, 2004.

[20] Y. R. Tsai, Sensing coverage for randomly distributed wireless sensor networks in shadowed environments, IEEE Transactions on Vehicular Technology, Vol. 57(1), PP. 556–564, 2008.

[21] J. Venkataraman, M. Haenggi, O. Collins, Short noise models for the dual problems of cooperative coverage and outage in random networks, 44st Annual Allerton Conference on Communication, Control, and Computing, 2006.

[22] R. Wang, W. Cao, Universal information coverage for bandwidth-constrained sensor networks, Robotics and Biomimetics, 2007. ROBIO 2007, IEEE International Conference on. IEEE, 2007, PP. 904-907, 2007.