DIntrusion Detection in WSN with an Improved NSA Based on the DE-CMOP

Weipeng Guo[1], Yonghong Chen[1,2,*], Yiqiao Cai[1], Tian Wang[1], and Hui Tian[1]
[1] College of Computer Science & Technology, Huaqiao University, Xiamen, China
[e-mail: 18965618074@163.com]
[2] Department of Electrical Engineering and Computing Systems, University of Cincinnati, Cincinnati, OH, 45221-0030,USA
[e-mail: agrawadp@ucmail.uc.edu]
*Corresponding author: Yonghong. Chen [e-mail: djandcyh@163.com]

Received June 11, 2016; revised December 27, 2016; accepted June 4, 2017; published November 30, 2017

Abstract

Inspired by the idea of Artificial Immune System, many researches of wireless sensor network (WSN) intrusion detection is based on the artificial intelligent system (AIS). However, a large number of generated detectors, black hole, overlap problem of NSA have impeded further used in WSN. In order to improve the anomaly detection performance for WSN, detector generation mechanism need to be improved. Therefore, in this paper, a Differential Evolution Constraint Multi-objective Optimization Problem based Negative Selection Algorithm (DE-CMOP based NSA) is proposed to optimize the distribution and effectiveness of the detector. By combining the constraint handling and multi-objective optimization technique, the algorithm is able to generate the detector set with maximized coverage of non-self space and minimized overlap among detectors. By employing differential evolution, the algorithm can reduce the black hole effectively. The experiment results show that our proposed scheme provides improved NSA algorithm in-terms, the detectors generated by the DE-CMOP based NSA more uniform with less overlap and minimum black hole, thus effectively improves the intrusion detection performance. At the same time, the new algorithm reduces the number of detectors which reduces the complexity of detection phase. Thus, this makes it suitable for intrusion detection in WSN.

Keywords: WSN, Intrusion detection, Negative Selection Algorithm, Multiobjective optimization problem, Differential Evolution

This work is supported by the National Natural Science Foundation of China (NO.61370007, 61572206, U1405254),and the Program for New Century Excellent Talents in Fujian Province(2014FJ-NCET-ZR06).

https://doi.org/10.3837/tiis.2017.11.022 **ISSN : 1976-7277**

1. Introduction

Wireless sensor networks (WSN) is a special kind of stand-alone wireless network, which has been widely used in monitoring environmental, military, health control, forest fire monitoring and so on [1]. Compared to the conventional wireless networks, each sensor node of a WSN is characteristics with restricted energy, limited computational resources and small storage space, which make it vulnerable to various attacks. The scarcity of effective security mechanism has become a major obstacle to its further applications. As an important measure of WSN security, the intrusion detection system (IDS) is very effective against addressing the security of WSN. However, as the WSN is constrained by the limited resource, it is particularly critical to design an intrusion detection system in WSN with low computational complexity, low energy consumption and effective detection performance [2].

Over the past few years, researchers have been shown great interest in developing biologically immune inspired algorithms and techniques for intrusion detection in WSN, for underlying features such as self-organization, adaption and fault tolerance are similar to the wireless sensor network desired characteristics of a WSN [3].

Negative Selection Algorithm (NSA), which is one of the most well-known immune inspired algorithm, has been widely used in intrusion detection [4]. However, there exists some problems of the original NSA about the uneven distribution of detector, black hole, overlapping, and so on [5]. It results in very low detection efficiency, especially when the WSN suffers from deceptive attack, that false negative rate become high. What’s more, the original NSA generates a large number of detectors, which necessitated a large computation in the detection phase. However, it is a great challenge to the resource constraint WSN.

Therefore, how to keep generation of fewer number of detectors to cover more area becomes the key objective of the NSA when utilized for WSN intrusion detection. We need to increase the coverage of abnormal area and reduce the number of detectors. That this is a obviously multiple objectives problem and multiobjective optimization is a way to address this kind of problem [6].

Our objectives is to maximize coverage of detectors and minimize the overlap, a Differential Evolution based Constrain Multiple-Objective Optimization Problem (DE-CMOP) way is used to improve the Negative Selection Algorithm to optimize generation of the detectors. Our improved algorithm generates more efficient detectors through multiobjective optimization technology and by employing the differential evolution [7], which provides ability of global search. The detectors can cover the abnormal area in a comprehensive and avoids the problem of black hole (uncover abnormal area) effectively. It is appropriate for intrusion detection in WSN.

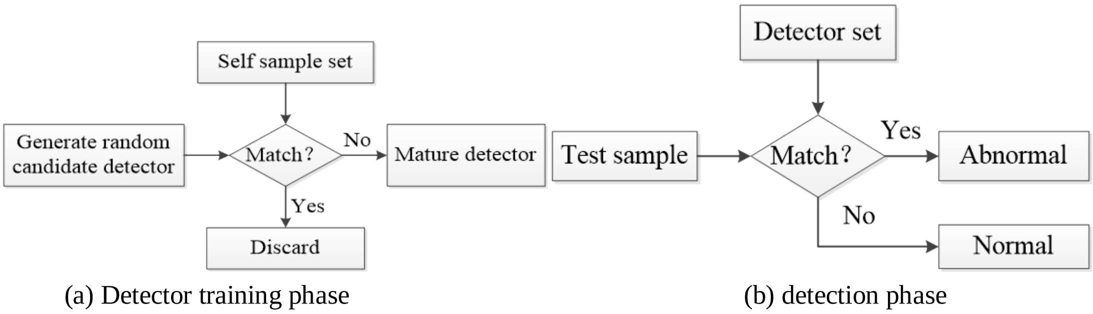
The experiment results indicate that our proposed algorithm can generate highly efficient detector set. It covers more abnormal area with fewer detectors,which improve the detection performance of the WSN intrusion detection largely. As the WSN suffers from deceptive attack, the false negative rate is reduced. In addition, as the distribution and effectiveness of the detectors is optimized that reduces the number of the detector, thereby minimizing the computational complexity of the detection phase,making it suitable for the resources constrained fewer WSN.

The remainder of this paper is organized as follows: Section 2 discusses preliminaries to the NSA with applications for anomaly detection in WSNs. Section 3 introduces the background knowledge about multiobjective optimization problem and differential evolution. Section 4 details DE-CMOP based NSA. Section 5 includes the computer simulations result. In Section 6, some conclusions and remarks are added.

2. Preliminaries of NSA in WSN

2.1 Negative Selection Algorithm

According to the process of T-cells maturation in thymus for immune system, only those T-cells which do not bind the self, can remains to defense against the pathogen [8], Forrest et al. [4], developed a Negative Selection Algorithm. As shown in **Fig.1 (a)(b)**, the NSA can be represented as two phases: detector training phase and detecting phase.



(a) Detector training phase (b) detection phase

Fig. 1. The process of NSA

As illustrated in **Fig. 1(a)**, the algorithm generates the detectors randomly and trains the detectors through self set. Only detectors that do not match anything self becomes mature detectors and can be saved. After the detector training phase, the system turns into detection phase. As shown in **Fig. 1(b)**, in this phase, the system recognizes any abnormal through the detectors as those samples that match the detector is defined as abnormal.

2.2 NSA for Abnormal Detection in WSN

As a classical AIS algorithm, NSA has been widely used in WSN intrusion detection [9-13]. In [11], AIS was used for detecting anomalies in a WSN. It basically employs one-to-one mapping between thymus and sensor node as the sensor node is responsible for training the detector set and detecting the intrusion locally. Liu et al. [12] were inspired by the immune system, applied the techniques of negative selection algorithm and clonal selection algorithm for the intrusion detection in a WSN. To detect the anomaly, all node in the network are equipped with the detection module, with capabilities of self acquisition, detector generation, detection and clonal selection. Each sensor node monitors the behavior of neighboring sensor nodes to train the detectors and utilize the clonal selection technique to store the effective detector of memory to improved detection performance. To detect anomalies in WSNs, Rizwan et al.[10] utilized NSA of AIS, NSA employing a detector set that contains anomalous packets with that identifies certain anomalies. Fu et al. [13] proposed a hierarchical anomaly detection framework based on an immune danger theory and the NSA. This framework consists of three layers: local danger sensor, global detection, and detection controller. It is adaptable and flexible in abnormal detection in a WSN.

It can be seen that there are two main strategies to utilize the AIS for a WSN intrusion detection. The first one is a direct one-to-one mapping between thymus and the sensor node. A fulfilled detection instance is run on a sensor node, containing detector training module and detection module. Another approach is a hierarchical architecture. In this way, the base station is responsible for training the detector set and the sensor node is responsible for detecting the abnormal. Considering the constraint on sensor node, we adopt a hierarchical architecture in this paper.

In our proposed framework, intrusion detection system is a hierarchical-cooperative system with intrusion detection services distributed among the sensor nodes, sink, and the cluster heads level. In the BS, BS training is done for the detector set according to the normal sample and distribute the detectors to the cluster head, which serves as the detection node. A common sensor node collects the information and used for anomaly detection.

2.3 Description of Shortcoming about NSA

Since the NSA was introduced, its use has grown rapidly, as it is ability to detect any non-self. In the original NSA, elements in the shape space and the detectors (matching rules) are used in the form of binary strings [11]. However, for most application, as binary representation fails to capture the structure of the problem. The binary representation is also not suitable for the intrusion detection. Gonalez et al. [15] proposed a new RNSA scheme based on a real value representation making it suitable for the real application. Based on this, Zhou et al. [14] proposed a V-detector algorithm in 2004, which can generate detectors with variable size. It can cover the non-self space with less detector, thus improving the detection performance.

To describe more intuitively, we analyze the algorithm with 2-dimensional data. **Fig. 2** [27] shows a 2-dimensional problem space, in which the blue circles are the self sample. The white circles are the detectors that generated according to the principle of the real value v-detector.

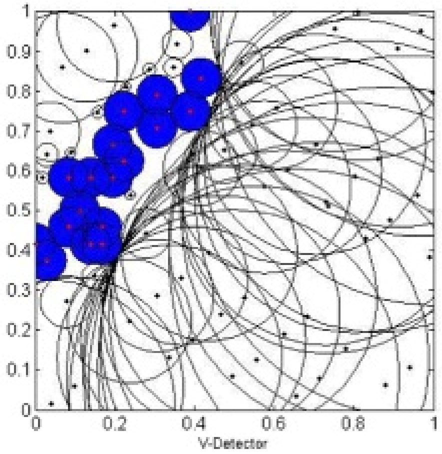


Fig. 2. 2-Dimensional problem space

It can be seen that due to this randomly detector generation mechanism, the overlap between the detectors is severe. A large amount of detectors is generated, which results in computational intensity and reduce the effectiveness of the detection mechanism. Beside, there still exist many abnormal spaces that uncovered by the detectors, which is named as the black hole. The test sample that fall into black hole, will not be detected, resulting in false negative. In WSN, the attackers are catchy that they always pretend the attack behavior as the normal,which make it difficult to detection.

To solve the problem of the NSA discussed above, researchers have proposed some solutions varying from optimizing the generation of detector set to optimizing the detection method. The researchers consider that the detector generation mechanism of NSA is constrained by the random search rule, which results in incomplete coverage of the non-self space and a lot of overlap. By means of an excellent search ability of evolutionary algorithms,researchers have proposed an optimization in the detector generation mechanism. Fabia Gonzalez [16] utilized the simulated annealing algorithm to find out a good distribution of the constraint sized detectors. However, in variable-sized detectors, each detector should be represented by a variable radius donated as d=(c,r), which means that during the process of optimization, more than one variable factor should be take into consideration. Ostaszewski et al. [17] optimize the detectors with a coordinated evolution way. Gao et al. [5] utilized the genetic operators to optimize the detector generation mechanism, which improves the ability of global search. However, it will premature convergence or degenerate sometimes, as it only considers global search. In addition, from the point of the optimize the detection method, Fu et al. [18] proposed a Fuzzy logical based Negative Selection Algorithm (FNSA). By utilizing a fuzzy decision rule, the algorithm can detect the antigen that are dropped into the black hole. However, there still exist a large amount of detectors, creating great burden on the resource constrained sensor node.

Therefore, to make the NSA algorithm more suitable for WSN intrusion detection, optimizing the detector generation mechanism becomes a key issue of the algorithm.

As it has been stated that the main objectives of optimization are to cover more abnormal area and to limit the number of the detectors as far as possible. It is obvious that the two objectives are contradictory. More detectors are needed to cover more area. Recently, detector distribution can be optimized and the effectiveness of the detector becomes a compromise idea. Multiple objective optimization is a way to solve this kind of problem. Beside, any appropriate optimization must follow the principle of negative selection. Therefore, in this paper, a DE-CMOP based NSA is proposed to improve the NSA generation mechanism, with detail about the optimization is described in the following sections.

3. Related Background

3.1 Multiobjective Optimization Problem

Multiobjective Optimization Problem (MOP), also called as multi-standard optimization problem, is defined as searching for optimal decision variables that satisfy the constraints as per the conflicting objective functions. In this study, maximization of multi-objective optimization problem is involved, which can be stated as follows [16]:

$$\begin{cases} \max F(x)=(f_1(x), f_2(x),\cdots, f_k(x))^T \\ subject\ to\ g_i(x)\leq 0 \qquad i=1,2,3,\cdots,p \end{cases} \tag{1}$$

Where $x=(x_1,x_{2,\ldots,}x_n)$ is the n dimensional decision vector in Ω (the feasible region in decision search space). $F(x)$ is a k dimensional objective vector where $k\geq 2$ is the number of objective functions. And $g_i(x)\leq 0$ is the constraint function, p is the number of constrains.

Here are some important definitions:

(1). Dominance [19], which is an important concept for MOP. Considering the MOP proposed, assume x_a and x_b is the decision vector in the feasible region Ω,only when the following relationship is satisfied. We can define that a decision vector x_a dominates another vector x_b,denoted as $x_a \succ x_b$.

$$\begin{aligned} &\forall i \in \{1,2,\cdots,k\},\ f_i(x_a) \le f_i(x_b) \\ &\wedge \exists j \in \{i,\cdots,k\},\ f_i(x_a) < f_i(x_b) \end{aligned} \tag{2}$$

if there is no decision vector $x \in \Omega$ that $x \succ x^*$,$x^* \in \Omega$ we can say that decision vector x^* is a Pareto solution.

(2). Pareto Set (PS) [19], which it is a set of the Pareto solutions, defined as:

$$P^* = \{x^* \in \Omega | \neg \exists x \in \Omega, x \succ x^* \ \} \tag{3}$$

(3). Pareto Front (PF) [20]. And a Pareto set are defined as the relevant image in the objective function area that hold the following:

$$PF^* = \{F(x^*) \,|\, x^* \in P^*\} \tag{4}$$

As multiple objective optimization algorithms can find a series of the solutions close to the PF, we can use the same way in our proposed algorithm in this paper to improve the effectiveness of the detectors. In many classical multiple objective optimization algorithms, each unity in the population is related to a grade value. However, we only care about the non-dominated individuals(Pareto solution) in this paper.

(4). MOP with Constraints (CMOP). Different from the unconstrained multiobjective optimization problem, the search space of CMOP consists of both feasible and infeasible regions. Penalty method, which is always used to solve CMOP [21], and is considered as the effective method to solve such problems.

The main idea of the penalty method is to reform the CMOP to an unconstrained one. A penalty function is introduced into one of the original objective function. The penalty function can be considered as a parameter that is based on the violation degree,which means the distances from one individual to the boundary of the feasible set. With the theory of penalty function, the maximum multi-objective optimization problem can be reformulated as the following unconstrained multiobjective optimization problem:

$$\begin{aligned} &max\ F(x,\sigma) = (f_1(x),\cdots, f_{k-1}(x), f_k(x,\sigma))^T \\ &f_k(x,\sigma) = f_k(x) + \sigma P(x) \\ &P(x) = \sum_{i=1}^{p} [\min(0, g_i(x))]^2 + \sum_{j=1}^{l} h_j^2(x) \end{aligned} \tag{5}$$

3.2 Differential Evolution

Differential Evolution (DE) is a population difference based random search algorithm proposed by R. Stom and K. Price [7]. Due to the advantage of simple principle, less controlled parameter and robustness, it has been widely used in multiple objective optimization problem. The DE searches the optimal decision on the feasible space through three key operations: mutation, crossing and selection.

(1). Mutation operation

DE implements the mutation of the individual through the differential strategy, which is different from the Genetic Algorithm [5]. The mutation component is defined as the difference vector of the parent generation. A common difference vector is defined as follows:

$$\begin{aligned}&v_i(g+1)=x_{r1}(g)+F*(x_{r2}(g)-x_{r3}(g)),\\&where\ \ i\neq r1\neq r2\neq r3\end{aligned} \tag{6}$$

Where F is the scaling factor, $x_i(g)$ represent *i-th* individual of the *g-th* population. It should be mentioned that the value of F has a drastic impact on the performance of the algorithm, while the value too large will slow down the convergence, and too small will reduce the population diversity and lead to partial optimization. Generally, the value of F varies as [0,1.2] **[5].**

(2). Cross operation

The cross operation combines the mutation vector and the target vector to improve the diversity of the mutation vector. The new vector $u_i=[u_{i1},u_{i2}...u_{in}]$ can be generated as follows:

$$u_{ji}=\begin{cases}v_{ji}(g+1), & rand\leq CR\ or\ \ j=randr\\ x_{ji}(g), & rand\leq CR\ or\ \ j\neq randr\end{cases} \tag{7}$$

$$i=1,2,...,w;\ \ j=1,2,...,n$$

where *rand* is a random value of [0,1],*CR* is a constant between [0,1], commonly known as crossover probability factor. The larger value of *CR is* greater is the possibility of cross. *CR=0* means that there is no cross over. *randr* is a random integer value of [1,*n*], that promise u_i can get an element from $v_{i.}$ Otherwise, no new vector can be generated,and the population will no change.

(3). Selection operation

After the operation of mutation and cross over, child population is generated. To choose the superior to the next generation,an one to one championship is performed to the individual child and parent according to the greedy way as follows:

$$x_i(g+1)=\begin{cases}u_i(g+1), f(u_i(g+1))\leq f(x_i(g))\\ x_i(g),\quad others\end{cases} \tag{8}$$

where $x_i(g+1)$ represents *i-th* individual of the *(g+1)-th* population and f is the fitness function.

4. Optimization of NSA based on DE-CMOP

In order to solve the problem of NSA, a Differential Evolution Constraint Multiobjective Optimization Problem based Negative Selection Algorithm (DE-CMOP based NSA) is proposed in this section that improves NSA detector generation mechanism for intrusion detection in WSN. The algorithm firstly established normal behavior of the network by building a normal library and then generates an initial detector set. Then differential evolution constraint is utilized for multiple objective optimization problem that optimizes the detector distribution and effectively improves the detection performance. In this section,we firstly introduce the main objective of the proposed algorithm. Then, detail involved steps are now described.

4.1 Definition of Objective Functions and Constraints

The goal of detector optimization in aforementioned NSA is to produce a series of detectors with optimal distribution and efficiency. For the multiobjective optimization problem, the first step is to define the objective functions. In this DE-CMOP based NSA, two essential objectives are used to describe the demands of this kind of problem.

The first objective function is *Coverage(d)* (donated by *Cov(d)*), which is based on the coverage of the non-self area (abnormal area) with certain detectors. The second objective function *Overlapping(d)* (donated by *Lap(d)*) is based on the overlap between detectors. In this paper, taking the spirit of maximized objectives, the objective functions and the constraints can be described as follow:

$$\begin{aligned} &\max F(d) = (f_1(d), f_2(d))^T \\ &\qquad f_1(d) = Cov(d),\ \ f_2(d) = \varphi - Lap(d) \\ &subject\ to\ g_1(d) = \mathrm{Distance}(c, c_s) - r_s > 0 \\ &\qquad g_2(d) = \frac{\mathrm{Distance}(c, c_d) - r_d}{r_d} > 0 \end{aligned} \tag{9}$$

where φ is a large positive value (used φ=500 in this paper) that is used to change a minimal optimization problem into a maximal one in $f_2(d)$. The constraint function $g_1(d)$ implies that detectors must not fall into the self space, and constraint function $g_2(d)$ claims that the detectors need to avoid to be covered by other detectors as much as possible.

(1). Coverage function *Cov(d)*

It is difficult to accurately calculate the coverage of the detector set accurately due to associated uncertainty of the detector generation. In this paper, *Cov(d)* is defined based on the method of statistical estimate of coverage by hypothesis testing method, proposed by Zhou [18].

According to the hypothesis testing method [22], assume that d_{num} is the theoretical number of detector, the maximum coverage can be achieved as p_{max}=1-5/d_{num}. To guarantee the central limit theorem correctly, we approximate the normal distribution as binomial distribution. Therefore, we should assume that np>=5 and $n(1-p)$>=5 is also valid. Therefore, we can choose the sample size by n=max{5/p,5/(1-p)}. According to Zhou [18], only more than y candidates can be covered continuously by sampling n times and the maximum coverage can be satisfied.

$$y = \sqrt{np_{\max} q}\,(z_\alpha + \sqrt{\frac{np_{\max}}{q}}) \tag{10}$$

Where α is the significant level. Both α,and z_a can be obtained from the normal distributed table.

Therefore, we can conclude that if there only $\bar{y}$ candidates that are continuously covered by the existing detectors, the current coverage of detector d is:

$$Cov(d)=\frac{\overline{y}\times p_{\max}}{y} \tag{11}$$

(2) Overlap function *Lap(d)*

Considering the overlap function *Lap(d)* in *f*$_2$*(d)*, we utilize the estimation method [23]. The overlapping between the *i-th* detector and the *j-th* detector can be approximated as:

$$Overlapping(d_i,d_j)=\{\begin{matrix} 0 & if\ \left\|c_d^i-c_d^j\right\|\geq r_d^i+r_d^j \\ (\exp(\frac{r_d^i+r_d^j-\left\|c_d^i-c_d^j\right\|}{r_d^i+r_d^j})-1)^n & if\ \left\|c_d^i-c_d^j\right\|<r_d^i+r_d^j \end{matrix} \tag{12}$$

The *Lap(d*$_i$*)* can be defined as the max value of overlap about the *i-th* detector d_i with others:

$$Lap(d^i)=\max\{lap(d^i,d^1),...,lap(d^i,d^{d_{num}})\} \tag{13}$$

(3). Reforming constraint function

For the constraint functions phase,we reform the constrained multiobjective functions to an unconstrained one according to the penalty method and the problem can be described as follows:

$$\begin{aligned} &\max F(d,\sigma,\eta)=(f_1(d),\overline{f_2}(d,\sigma,\eta))^T \\ &\overline{f_2}(d,\sigma,\eta)=f_2(d)-\sigma(\min\{0,g_1(d)\})^2 \\ &\qquad\qquad\qquad -\eta(\min\{0,g_2(d)\})^2 \\ &\sigma=f_2(d)/g_1(d)\ \ and\ \ \eta=500/g_2(d) \end{aligned} \tag{14}$$

It can be seen that the objectives are conflicting in nature, as reducing the effectiveness of one objective improves the other. Improving the coverage of abnormal may result in increased overlap between the detectors. In this paper, a Differential Evolution based Multiobjective Optimization Problem method is used to obtain the optimal number of detector.

4.2 DE-CMOP based Negative Selection Algorithm

In this section, we highlight DE-CMOP based NSA. The detail steps involved are discussed. Assume the self sample (normal behavior) is donated as $s=(c_s,r_s)$, where c_s is a w dimension node ($c_s=[u_1,u_2,...u_w]$) representing the center of the vector, and r_s represents the self threshold. Similarly, the detector is donated as $d=(c,r)$. **Fig. 3** show the main loop of the proposed algorithm.

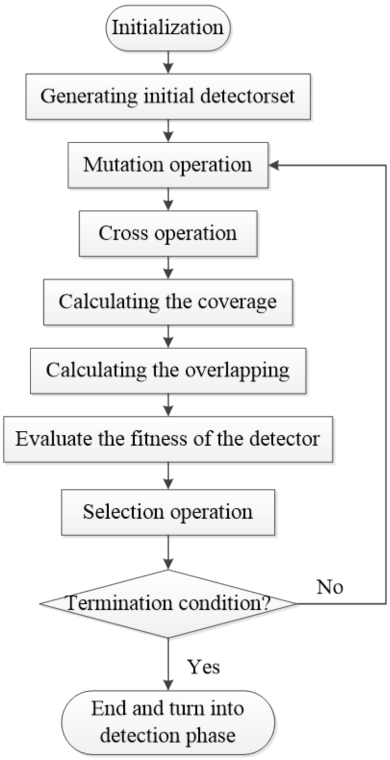

Initialization
Generating initial detectorset
Mutation operation
Cross operation
Calculating the coverage
Calculating the overlapping
Evaluate the fitness of the detector
Selection operation
Termination condition?
No
Yes
End and turn into detection phase

Fig. 3. DE-CMOP based Negative Selection Algorithm

The basic steps for DE-CMOP based NSA that optimize generation of the detectors are given as follows:

1) Initialization. In this step, setting the parameters include: scaling factor *F*,the maximum number of iterations G_{max},cross factor *CR*, normal threshold r_s, proportion of the detector set and the expected coverage. Parameters of G_{max} and expected coverage are set as the termination condition.
2) Generating the initial detector set as the parent detector set according to the principle of V-detector algorithm [14]. The parent generation detector set is donated as:

$$DS(g)=\{d_1(g),d_2(g),\cdots d_n(g)\},\ \ g=0$$

where *n* is the proportion of the detector set and d_k is the *k-th* detector.
3) Mutation operation. It is a way to optimize the distribution and to reduce the overlap of the detectors. According to the differential mutation strategy [21], the mutation detector of the parent is as follows:

$$dv_i(g+1)=d_{r1}(g)+\lambda(d_{r3}(g)-d_i(g))+F(d_{r2}(g)-d_i(g)) \tag{15}$$

where $d_{ri}(g)$ represent the *ri-th* detector of the *g-th* generation population. And F is the scaling factor. By utilizing the differential vector, the searching ability has been improved.
4) Cross operation. In this phase,combining the mutation vector and the target vector are combined to improve the diversity of the mutation vector. The new detector center $du_i=[u_{i1},u_{i2,..}u_{iw}]$, can be generated as follows:

$$du_{ij} = \begin{cases} dv_{ij}(g+1), & rand \le CR \text{ or } j = randr \\ d_{ij}(g), & rand > CR \text{ or } j \ne randr \end{cases} \tag{16}$$

$$i = 1,2,..w;\ j = 1,2,..,n$$

where *rand* is a random value of [0,1], and *CR* is the crossover probability factor. *randr* is a random integer value between [1,*n*]. To enable search ability and ensure convergence sped, in this paper, *CR* is set as 0.6 as per [24].

5) Step 5, calculates the coverage of the detector d. According to the objective function $f_1(d)$ defined in eq (11). It is a problem that maxims we expect the largest coverage of the detector.
6) Calculating the overlapping of the detector with other detector according to the objective function $f_2(d)=p\text{-}Lap(d)$ defined in eq. (13). Where *p* is a peak value that is used to transfer the function *Lap(d)* into a maximum problem.
7) Then evaluate the fitness of the detector. In this paper, we access the fitness of the detector by max-min function [20]. Detail are as follows:

Firstly, executing the max function of the objective function, is:

$$\max_{i=1,2}\{f_i(s) - f_i(t)\} \tag{17}$$

Then, executing the min function of the vector s and other decision vector is :

$$\min_{j=1,2,..N,s\ne t}\{\max_{i=1,2}\{f_i(s) - f_i(t)\}\} \tag{18}$$

The fitness can be defined as :

$$f_{\max\min} = \min_i\{\max_i\{f_i(s) - f_i(t)\}\} \tag{19}$$

8) Selection operation. In this step, find out all the detectors that follow Pareto solution to build up the dominance detector set. After the operation of mutation and cross, the child population is generated. To choose a superior to the next generation, one to one championship is performed between the child and the parent detectors. From the procedure of the max-min function,we can see that the value of f_{maxmin} which is larger than zero, is the Pareto solution. According to the fitness value evaluated above, the DE-CMOP selects the better ones following the next generation of a greedy solution as:

$$d(g+1) = \begin{cases} du_i(g+1), & f_{\max\min}(du_i(g+1)) > f_{\max\min}(d_i(g)) \\ d_i(g), & others \end{cases} \tag{20}$$

Then, update the non-domlist (Pareto solution set);

9) Determine whether the detector set that could satisfy with the termination condition. If not, repeat step 3 to step 8 until satisfied with the termination condition provided in step 1.
10) Once the detector set is ready, the system turn into detection phase.

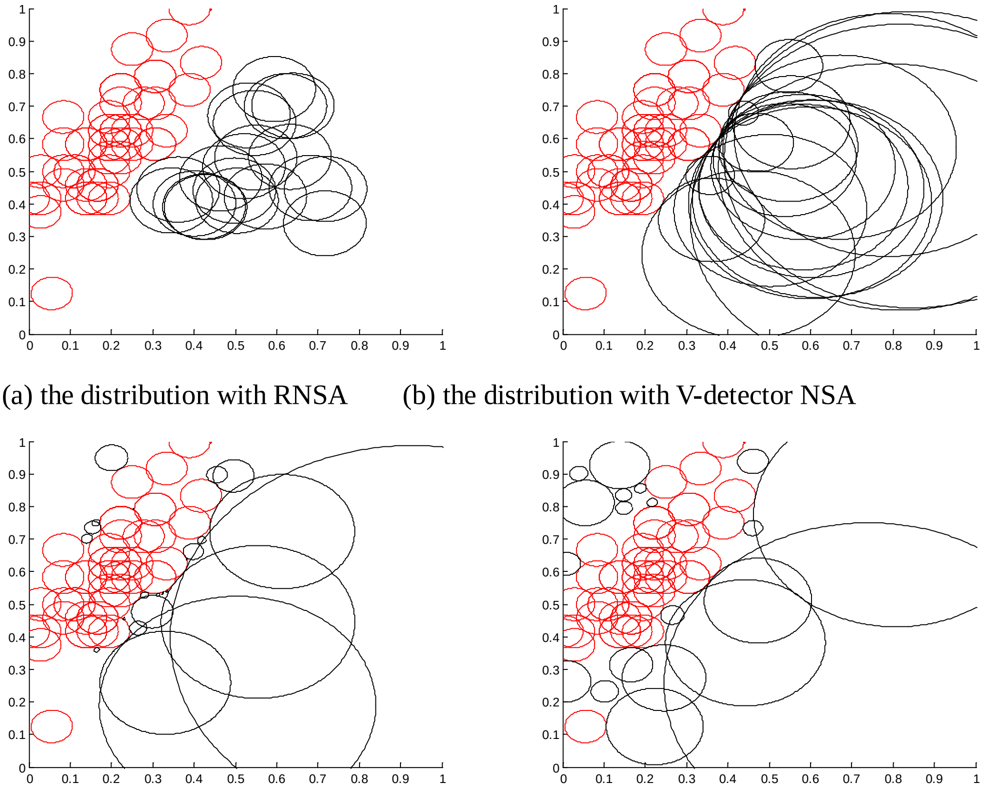
5. Simulation Results and Analysis

In this section, the simulation results are presented to demonstrate the performance of our new algorithm. Both Fisher's Iris data set [25] and WSN simulation are used in experiments to analysis the improvement in performance of the detector set and detection.

5.1 Results on Fisher' Iris Data Set

In this paper, in order to analyze the excellent ability of the DE-CMOP based NSA in optimizing the distribution of detector and improving the detection performance, we firstly analyze an improved algorithm performance through the *Fisher's Iris* data set. It's a common data set that need to be used for anomaly detection. The data set contains three categories: setosa, versicolor and virginica. Each category contains 50 samples, and each of the sample is described by four features: sepals width, sepals length, petal length, and petal width. In this paper, we choose the sepals width and length as the detection feature. The setosa set is chosen as the self set that used for training the detector set. The other two categories are treated as abnormal set that are reserved for testing.

In order to highlight the ability of optimizing the distribution of the detectors, and to ensure the fairness, we should set the size of the initial detector set is comparable. Therefore, in this part of the experiments, we set the number of the initial detector set d_{num}=20 and analyze the distribution. Following the reference [5], other parameters in these simulations are set as follows: the self sample threshold r_s=0.05, and detector's radius in RNSA is set as 0.1.



(a) the distribution with RNSA (b) the distribution with V-detector NSA

(c) the distribution with GA based NSA (d) the distribution with DE-CMOP based NSA

Fig. 4. The distribution of detectors obtained by different NSA with $d_{num}=20$

Fig. 4 shows the comparison results of the RNSA, V-detector NSA, GA based NSA and our proposed DE-CMOP based NSA. It is obvious that MOP strategy has a drastic effect on the distribution of detectors. **Fig. 4(a)** and **Fig. 4(b)**, illustrate the detectors that seriously overlap and keep the self area far away. Nevertheless, as for our proposed DE-CMOP based NSA, the algorithm can optimize the detectors' distribution and effectiveness because of the using of CMOP strategy. **Fig. 4(d)** shows that the distribution of detectors is more uniform and closer to the self area in our scheme. Beside, due to the use of differential evolution strategy, the black hole (uncovered abnormal area) between the detectors and self area is also reduced. What's more, compare to **Fig. 4(c)**, which is the single objective optimization based NSA. A more reasonable assignment of large and small detectors is feasible through our proposed DE-CMOP based NSA. It reduces the black hole to some extent. The result shows that as compared to the single objective optimization based NSA, and the multiple objective optimization based NSA can obtain a global optimal detector set, not just an independent optimal detector, which is appropriate for the NSA.

On the other hand, the experiment results also demonstrate that under the same conditions on the number of detectors, the coverage of our improved NSA is larger than the other method due to the excellent searching ability of DE-CMOP. In other words, we can cover abnormal areas with fewer detectors, which reduces the complexity of the detection phase,thus make it suitable for intrusion detection in resource constraint WSN.

Consider abnormal detection performance of our algorithm. It is obvious that the difference of self area and self radius(self threshold) may lead to different detection results. Following reference [5], the parameters are set as follows: excepted coverage is 0.9, the max generation is 20, hypothesis testing significance level α is 0.1 and cross factor used in differential evolution, has been discuss before. **Fig. 5** shows the detection performance result of RNSA, V-detector,GA and DE-CMOP based NSA with self sample threshold changed from 0.01 to 0.1.

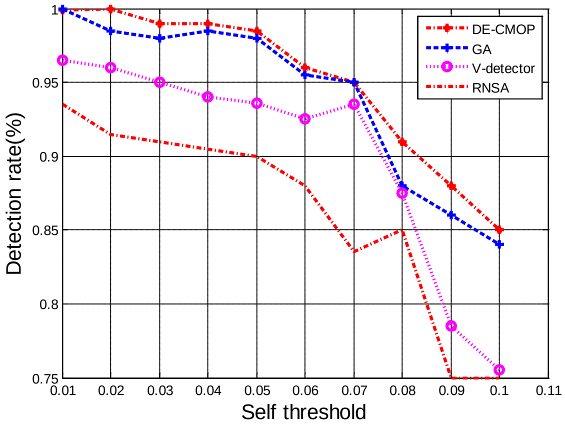


Fig. 5. Detection performance with self threshold various from 0.01 to 0.1

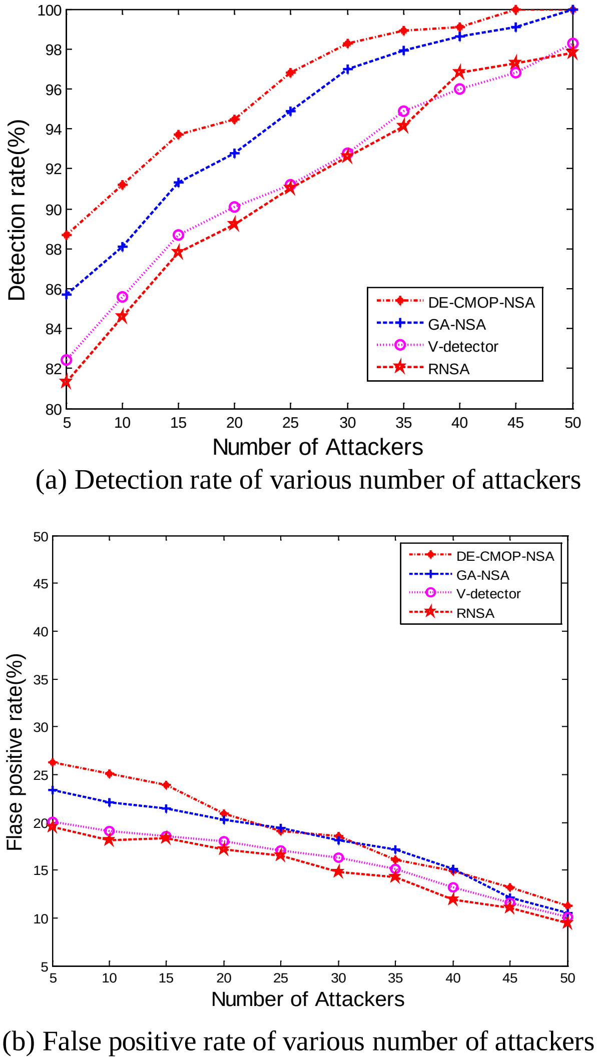
Fig. 5 shows that with an increase in the self threshold, the detection rate is decreased as self area has invaded to the abnormal area. Compared to RNSA, V-detector and GA based NSA, DE-CMOP based NSA has a slight advantage in detection rate than other methods as it reduces black hole of the detector. Moreover, the DE-CMOP offers great advantage when the self threshold is small because of the bigger coverage and more uniform distribution of the detectors.

5.2 Results on WSN Intrusion Detection

To evaluate the performance of the proposed algorithm in intrusion detection in a WSN. In this paper, the Network Simulation (NS-2) is used to evaluate the system performance.

In this paper, the WSN consists of 500 nodes randomly distributed in a field of 1000*1000m and a base station (BS) is located in (0,0). In this network, each node has a transmitting range of 50 meters and data packet is sent to the BS periodically. To promise the hierarchical structure, we use LEACH protocol as the routing protocol. Beside, considering the balance of energy consumption, 10% of the nodes is selected as the cluster head. The total simulation time is 2 hours. At the beginning, the network has a learning period of 30 mins. After this period, adversaries start their attacks randomly every 10 second. In this paper,the intrusion is achieved by a Jamming attack,which is a DoS attack of the WSN. Attackers broadcasting worthless packets in the wireless sensor network periodically to hamper the communication between nodes in the network. It affects the wireless communication and consumes large amount of energy. In this paper, various strength of attacks are simulated to analyze the performance of the proposed IDS. All the results shown in this paper are an average of 10 repeated experiments.

According to [26], parameters such as the node throughput, packet dropping ratio, packet average delay and so on, to stay in a certain range when the network is under a normal state. However,when the WSN suffers an attack, it results in abnormal changes in these parameters obviously. In this paper, packet sending rate, packet receiving ratio and node throughput are chosen as the detection characteristics.



(a) Detection rate of various number of attackers

(b) False positive rate of various number of attackers

Fig. 6. Detection performance of various number of attackers

Firstly, the attack interval is set as t=1s, various attackers varying from 5 to 50 are simulated to evaluate the anomaly detection performance of our proposed algorithm. **Fig. 6** shows that the DE-CMOP based NSA proposed in this paper offer a slight advantage in detection rate than other existing methods.

As shown in **Fig. 6**, with an increase in attackers, the harmful to the network becomes serious,thus making the detection rate become even higher. When the hamper become more and more severe, the attack features become easy to be detected in our methods with no outstanding advantages on the detection rate. However, when the network is under fewer number of attacker, our improved algorithm offers much better performance than other existing scheme. This is because generated detectors generate in our method are more effective and more uniform that they cover more abnormal area and reduce the false negative rate.

As for false positive rate, **Fig. 6(b)** shows that as the harmfulness become more serious, the false positive rate is decreased. However, when they are less harmful, because of the detectors in our proposed method is closer to the self area, the false positive rate is slightly higher than the other method. The reason of this phenomenon is that the threshold of the self sample is set at a fix value, thus influence the training of detector. Therefore, it is worth to studying the problem of setting the self threshold of NSA in our future work.

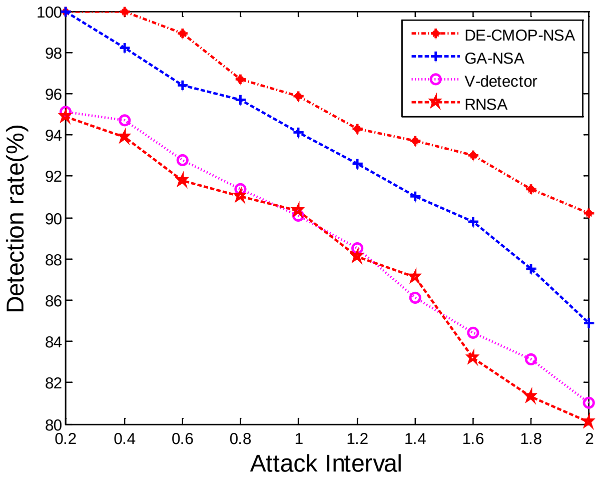


Fig. 7. Detection rate of various strength of attack

Network attack and defense is a trade off between the attacker and protector. The attacker learns the normal behavior of the network and behave similar to the normal, which make it difficult to be detected. In fact, the black hole in the NSA represents this kind of problem. The attacker try to make the attack behavior in the black hole so as to avoid to be detected. In this part of experiment, five attack nodes are set in the network and the attack interval various from 0.2 to 2s, which becomes similar to a normal behavior.

Fig. 7 shows the detection result of the abnormal condition. It can be seen that as the attack behavior becomes similar to a normal behavior, the detection rate of RNSA and V-detector algorithm based method decrease drastically as there exist a large amount of detector black hole. As for our proposed DE-CMOP based NSA, the detection rate also decreases but still keep in a higher level than the other existing methods due to the reduction in black holes.

6. Conclusion

Considering the shortcomings of NSA about black hole,overlap and a large amount of detectors when utilized in WSN intrusion detection. In this paper, a new Differential Evolution Constrained Multiple Objective Optimization based Negative Selection Algorithm is proposed that optimizes generation of detector in NSA and improves the intrusion detection performance in WSN. The experiments demonstrate that based on differential evolution and constrained multiple objective optimization problem, improved NSA can generate the detectors with more effectiveness and more reasonable distribution with fewer number of detectors as compared with other existing schemes. The algorithm improves the detection performance to some extend as it is more suitable for the resource constrained WSN. Beside the generation mechanism of the NSA, detection performance is also related to the detection rule and self threshold. Therefore, to reduce the false alarm rate, we will focus on the improvement of the detection rule and optimize the self set in our future work.

References

[1] Chee-Yee Chong, S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247-1256, August, 2003. Article (CrossRef Link)

[2] I. Butun, S. Morgera, R. Sankar, "A survey of intrusion detection systems for wireless sensor networks," *IEEE Communications Surveys Tutorials*, vol. 6,no. 1, pp. 266-282, May, 2014. Article (CrossRef Link)

[3] H. M. Salmon, C. M. D. Farias, P. Loureiro, L. Pirmez, "Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques," *International journal of wireless information networks*, vol. 20, no. 1, pp. 39-66, March, 2013. Article (CrossRef Link)

[4] S. Forrest, A. S. Perelson, L. Allen, R. Cherukuri, "Self-nonself discrimination in a computer." in *Proc. of the 1994 IEEE Computer Society Symposium on IEEE*, pp. 202-212, May 16-18, 1994. Article (CrossRef Link)

[5] X. Z. Gao, S. J. Ovaska, X. Wang, "Genetic algorithms-based detector generation in negative selection algorithm," in *Proc. of 2006 IEEE Mountain Workshop on Adaptive and Learning Systems,*pp. 133-137, July 24-26, 2006. Article (CrossRef Link)

[6] Z. X. Cai, W. Yong, "A multiobjective optimization-based evolutionary algorithm for constrained optimization," *IEEE Transactions on Evolutionary Computation*, vol. 10, no. 6, pp. 658-675, November, 2006. Article (CrossRef Link)

[7] R. Storn, P. Kenneth, "Differential evolution–a simple and efficient heuristic for global optimization over continuous spaces," *Journal of global optimization*, vol. 11, no. 4, pp. 341-359, December, 1997. Article (CrossRef Link)

[8] J. Morteza, M. Hossein, M. Kasra, F. Mohammad, S. Shahaboddin, "A method in security of wireless sensor network based on optimized artificial immune system in multi-agent environments," *Research Journal of Recent Science*, vol. 2, no. 10, pp. 99-106, *August*, 2013. Article (CrossRef Link)

[9] M. Zeeshan, H. Javed, A. Haider, A. Khan, "An immunology inspired flow control attack detection using negative selection with R-contiguous bit matching for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 11, January, 2015. Article (CrossRef Link)

[10] R. Rizwan, F. A. Khan, H. Abbas, S. H. Chauhdary, "Anomaly detection in Wireless Sensor Networks using immune-based bioinspired mechanism," *International Journal of Distributed Sensor Networks*, vol. 11, no. 10, January, 2015. Article (CrossRef Link)

[11] M. Drozda, S. Schaust, H. Szczerbicka, "AIS for misbehavior detection in wireless sensor networks: Performance and design principles," in *Proc. of the 2007 IEEE Congress on Evolutionary Computation*, pp. 3719-3726, September 25-28, 2007. Article (CrossRef Link)

[12] Y. Liu, F. Q. Yu, "Immunity-based intrusion detection for wireless sensor networks," in *Proc. of IEEE International Joint Conference on Neural Networks*, pp. 439-444, June 1-8, 2008. Article (CrossRef Link)

[13] R. Fu, K. Zheng, T. Lu, D. Zhang, Y. Yang, "Biologically inspired anomaly detection for hierarchical wireless sensor networks," *Journal of Networks*, vol. 7, no. 8, pp. 1214-1219, August, 2012. Article (CrossRef Link)

[14] J. Zhou, "Negative Selection Algorithms: from the Thymus to V-detector," *The University of Memphis*, 2006. Article (CrossRef Link)

[15] F. Gonzalez, D. Dasgupta, R. Kozma, "Combining negative selection and classification techniques for anomaly detection,"*in Proc. of Congress on Evolutionary Computation*, vol. 1, no. 11, pp. 705-710, May 12-17, 2002. Article (CrossRef Link)

[16] F. González, D. Dasgupta. "A study of artificial immune systems applied to anomaly detection," *The University of Memphis* , May, 2003. Article (CrossRef Link)

[17] M. Ostaszewski, F. Seredynski, P. Bouvry, "Coevolutionary-based mechanisms for network anomaly detection," *Journal of Mathematical Modelling and Algorithms*, vol. 6, no. 3, pp. 411-431, March, 2007. Article (CrossRef Link)

[18] R. Fu, K. F. Zheng, F. C. You, D. M. Zhang, B. Wu, "Anomaly detection algorithm based on fuzzy and immune theory in wireless sensor networks," *Journal of Nanjing University of Science and Technology*, vol. 36, no. 1, pp. 137-142, 2012. Article (CrossRef Link)

[19] K. Deb, "Multi-objective optimization using evolutionary algorithms," *John Wiley & Sons, Inc*, vol. 16, 2001. Article (CrossRef Link)

[20] R. Balling, "The maximin fitness function; multi-objective city and regional planning." in *Proc. of International Conference on Evolutionary multi-criterion optimization*, vol. 2632, pp. 1-15, April 8-11, 2003. Article (CrossRef Link)

[21] C. A. C. Coello, "Theoretical and numerical constraint-handling techniques used with evolutionary algorithms: a survey of the state of the art," *Computer methods in applied mechanics and engineering*, vol. 191, no. 11, pp. 1245-1287, January, 2002. Article (CrossRef Link)

[22] Z. Ji, D. Dasgupta, "Estimating the detector coverage in a negative selection algorithm," in *Proc. of the 7th annual conference on Genetic and evolutionary computation*, pp. 281-288, June 25-29, 2005. Article (CrossRef Link)

[23] H. Wang, X. Z. Gao, X. Huang, Z. Song, "PSO-optimized negative selection algorithm for anomaly detection," *Advances in Soft Computing*, vol. 52, pp.13-21, 2009. Article (CrossRef Link)

[24] A. W. Iorio, X. Li, "Solving rotated multi-objective optimization problems using differential evolution," in *Proc. of AI 2004: Advances in artificial intelligence*, vol.3339, pp. 861-872, December 4-6, 2004. Article (CrossRef Link)

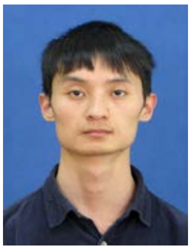
[25] Fisher's iris data is available at ftp://ftp.ics.uci.edu/pub/machinelearning-databases/iris/.

[26] D. M. Farid, N. Harbi, M. Z. Rahman, "Combining naive bayes and decision tree for adaptive intrusion detection," *Internation Journal of Network Security & Its Application*, vol. 2, no. 2, pp.12-25, May, 2010. Article (CrossRef Link)

[27] X. Xiao, T. Li, R. Zhang, "An immune optimization based real-valued negative selection algorithm." *Applied Intelligence*, vol. 42, no. 2, pp. 289-302, March, 2015. Article (CrossRef Link)

Weipeng Guo received the B.E. Degree from Huaqiao University, Quanzhou, China, and is currently pursuing a master degree at College of Computer Science & Technology in Huaqiao University. His current research interests is the study of intrusion detection in wireless sensor network.

Yonghong Chen, PhD, is a professor at College of Computer Science & Technology of Huaqiao University, Xiamen, China. Now, he is a visiting scholar at the University of Cincinnati in the United States. His current research interests include computer network and information security, wireless sensor networks' security, cloud security, intrusion detection and security of Big data



Zhongwen Wang received the B.E. Degree from Xi`an University of Posts & Telecommunications,and is currently pursuing a master degree at College of Computer Science & Technology in Huaqiao University. His current research interests is the study of network security.

Yiqiao Cai received the B.E. degree(2007) from Hunan University, and the M.E. and Ph. D from SunYat-sen University. His current research interests include the artificial intelligent algorithm and its application.

Tian Wang, Ph.D, is a associate professor at College of Computer Science &Technology of Huaqiao University, Xiamen, China. His current research interests include mobile computation, security of internet of thing, social network and big data process.

Hui Tian, Ph.D, is a associate professor at College of Computer Science &Technology of Huaqiao University, Xiamen, China. His current research interests include information and network security, cloud security, media security and intelligent computation.

Dharma P. Agrawal has been the OBR Distinguished Professor at the University of Cincinnati. He is the Fellow of IEEE, ACM, AAAS, NAI, I ACSIT, and WIF. He is a Golden Core member of the IEEE-CS and recipient of the IEEE Third Millennium Medal. His research interests include applications of sensor networks in monitoring Parkinson disease patients and neurosis, applications of sensor networks in monitoring fitness of athletes personnel wellness, applications of sensor networks in monitoring firefighters physical condition in action, efficient secured communication in Sensor networks, secured group communication in Vehicular Networks, use of Femto cells in LTE technology and interference issues, heterogeneous wireless networks, and resource allocation and security in mesh networks for 4G technology.