Journal of Computer and Communications, 2017, 5, 182-197
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

An Immunity-Based IOT Environment Security Situation Awareness Model

Yuanquan Shi[1,2], Tao Li[3], Renfa Li[2], Xiaoning Peng[1], Pengju Tang[1]

[1]College of Computer Science and Engineering, Huaihua University, Huaihua, China
[2]College of Computer Science and Electronic Engineering, Hunan University, Changsha, China
[3]College of Computer Science, Sichuan University, Chengdu, China
Email: syuanquan@163.com

How to cite this paper: Shi, Y.Q., Li, T., Li, R.F., Peng, X.N. and Tang, P.J. (2017) An Immunity-Based IOT Environment Security Situation Awareness Model. *Journal of Computer and Communications*, **5**, 182-197.
https://doi.org/10.4236/jcc.2017.57016

Received: April 20, 2017
Accepted: May 22, 2017
Published: May 25, 2017

Abstract

To effectively perceive network security situation under IOT environment, an Immunity-based IOT Environment Security Situation Awareness (IIESSA) model is proposed. In IIESSA, some formal definitions for self, non-self, antigen and detector are given. According to the relationship between the antibody-concentration of memory detectors and the intensity of network attack activities, the security situation evaluation method under IOT environment based on artificial immune system is presented. And then according to the situation time series obtained by the mentioned evaluation method, the security situation prediction method based on grey prediction theory is presented for forecasting the intensity and security situation of network attack activities that the IOT environment will be suffered in next step. The experimental results show that IIESSA provides a novel and effective model for perceiving security situation of IOT environment.

Keywords

IOT Environment, Security Situation Awareness, Artificial Immune System, Grey Prediction

1. Introduction

Internet of Things (IOT) is a heterogeneous network that consists of the conventional Internet and the edge networks, and it is connected by many different resource constrained devices/nodes using IP protocol [1]. As a part of the future Internet, IOT will comprise billions of "Things" possessing intelligent communication capability [2]. Generally, IOT is defined as a dynamic global network which possesses self-configuring capability based on standards and interoperable communication protocols, and all physical or virtual "things" of IOT hold spe-

cific identities that they can be integrated as an information network by using intelligent interfaces [3] [4]. But the definition of IOT varies because of many advanced technologies involved into IOT [2], such as wireless sensor networks, near field communication, low energy wireless communications, barcodes, intelligent sensing, radio frequency identification, and cloud computing etc. At present, IOT is very important in our society, and it has been widely used in industrial automation, environmental monitoring, healthcare monitoring, daily living monitoring, traffic congestion controlling, library services, smart cities and so forth [1] [2] [5]. The challenges of IOT, however, have been emerged. They mainly include IOT standardization, implementing technologies, innovation in IOT environment, security and privacy protection etc. For IOT, its every physical object, which can provide services for users, should be addressed and labelled, but the interconnections among things of IOT might bring many security problems, such as denial of service attacks, sybil attacks, data attacks, code attacks, local security of sensing nodes and so on [5] [6] [7].

To solve security problems of IOT, many researchers have proposed different security schemes, which involve from security architecture of IOT to security mechanism, introduced for the faced real problems. The security and privacy requirements of IOT mainly include data confidentiality and authentication, access control, privacy and trust among users and things, the enforcement of security and privacy policies [2] [6] [7] [8] [9]. Sun and Wang [6] proposed the security hierarchy structure of IOT, which consists of the sensation layer, the network layer and the application layer. And meanwhile they analyzed different security problems and corresponding security requirements in different layers of IOT. According to the related studies in the architecture and security threats analysis of IOT, Li and Zhou [10] proposed the security architecture of IOT based on security architecture of information system, and the related security problems are analyzed in IOT, such as security services, security domains and network hierarchies etc. Abie [11] proposed adaptive evolving security model (AES) and adaptive trust management model (ATM) used for implementing the automation of message-oriented middleware (MOM), and the proposed models can learn, anticipate, evolve and adapt to the changed environment according to the changing threats. Habib *et al*. [12] classified adaptive security approaches according to the hierarchy architecture of IOT based on the ITU-T reference model and IOT dynamic environment. Yan *et al*. [13] proposed IOT system model based on trust management (TM), and emphasized that TM plays an important role in IOT to enhance user privacy and information security. Raza *et al*. [14] proposed a novel intrusion detection system (*i.e*. SVELTE) for IOT to detect routing attacks such as spoofed or altered information, sinkhole attacks, and selective-forwarding etc.

Known from the above-mentioned literatures, the research about security defense policies of IOT is still scarce, especially the security policies for IPv6 over low-power wireless personal area networks (6LoWPAN) that is to prevent many attacks from conventional Internet passed by the 6LoWPAN border router

(6BR). Firewall provides an effective defense mechanism against network attacks by performing careful gatekeeping over the communication traffic that enter and exit the protected system [14] [15], that is to say, user may deploy security policies by running a gateway-level firewall to prevent hacker attacks from external network. Therefore, a firewall provides a clean interface to control bidirectional access to/from an individual application, an entire device, or a portion of a network [16]. The application of firewall has been used extensively to the conventional Internet, WSNs, and network based embedded systems [15] [16] [17] [18] [19]. In IOT, the resource constrained devices are usually connected to the unreliable and untrusted Internet via IPv6 and 6LoWPAN [14], these devices will face wireless attacks from 6LoWPAN and conventional Internet, even though these devices are secured with encryption and authentication. Some security policies of the conventional Internet, such as Firewall and Intrusion Detection System (IDS), are unsuitable to protect resource constrained devices of IOT because these policies need higher storage space and time cost in devices/nodes of IOT. Therefore, the uncovering requirements and the developing Firewall/IDS under IOT environment are worth investigating. At present, the relevant technologies of firewall/IDS for IOT have been proposed by some researchers in the existed literatures in order to ensure the security of 6LoWPAN network [1] [8] [14] [20] [21] [22] [23].

The security problems under IOT environment are similar to the faced intrusion problems of biological immune system (BIS), and they need keep the systemic stability under a varying environment [24]. Artificial immune system (AIS) inspired by BIS is one of bionic intelligent systems, and is also another new frontier research in artificial intelligence fields after genetic algorithm (GA) and artificial neural network (ANN). AIS can not only distinguish and withstand non-self antigens, which are illegal intrusions, but also possess the evolving learning mechanism of Darwin's evolution theory [25]-[32]. According to the dynamism of IOT environment and the illegal attacks from external and internal 6LoWPAN network, an immunity-based IOT environment security situation awareness model (IIESSA) is proposed to protect the security of resource constrained devices/nodes under IOT environment.

2. The Proposed IIESSA Model

An Immunity-based IOT Environment Security Situation Awareness (IIESSA) model is shown in **Figure 1**. In IIESSA, the 6LoWPAN of IOT connects directly to the conventional Internet by 6LoWPAN router (6LBR). The 6LoWPAN is comprised of router (RT), security awareness center (SAC) and security sensor (SS), where SS represents all kinds of resource constrained devices (RCDs) based on Contiki that is the embedded operation system, and SSs communicate with other devices/nodes of IOT by 6LBR or RT. IIESSA adopts SAC and SS to monitor intelligently the security of 6LoWPAN environment. SS is viewed as an immunity-based security sensor under IOT environment, and its function modules mainly include extracting security elements, evaluating security situation and

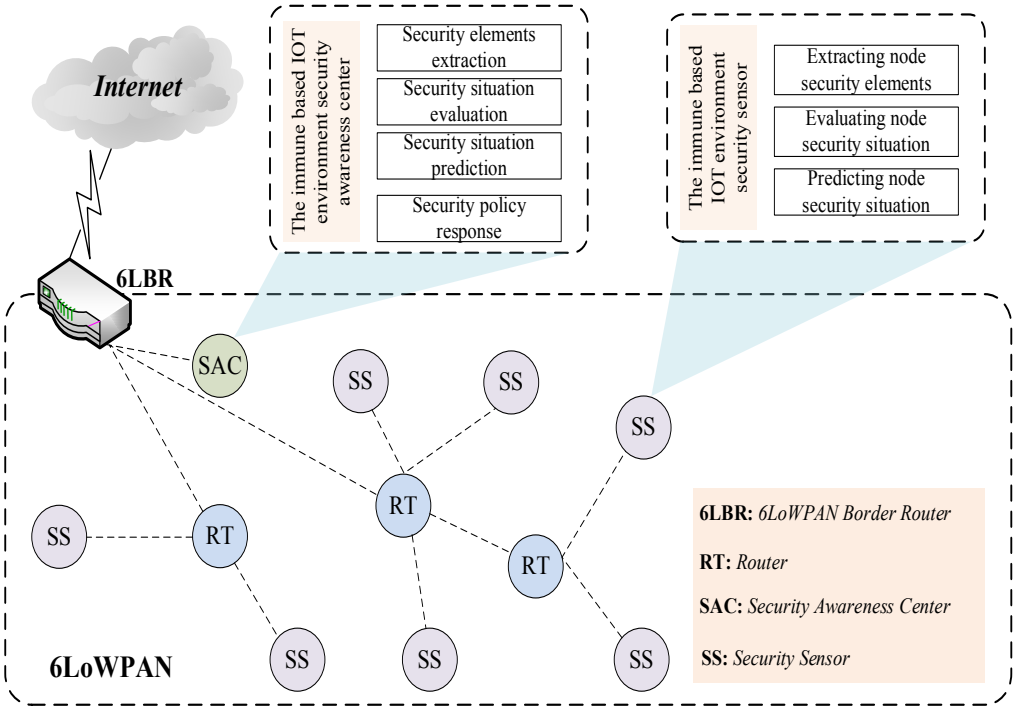

Figure 1. An immunity-based IOT environment security situation awareness model.

predicting security situation, where the former two modules adopt artificial immune mechanism to detect network intrusions and evaluate network security situation according to arbitrary kind of network attacks that resource constrained devices faced, and the last modules is used for predicting the security situations of devices/nodes of IOT by grey prediction method. For SAC, it is viewed as security awareness center based on artificial immune mechanism, and the tasks of SAC mainly include intrusion detection, security situation evaluation, security situation prediction and security policy response. Inspired by immune vaccine mechanism, SAC and SS can distribute new feature strings (detectors), which are extracted from network attack activities, to other devices/nodes of IOT by vaccine distribution mechanism so that the security of devices/nodes can be protected and enhanced timely. And meanwhile network attacks and results of network security situation that SSs faced will be sent to SAC so that SAC can manage timely 6LoWPAN environment security situation and execute corresponding security policy response.

To perceive effectively IOT environment security situation, the key problems that need be solved by IIESSA is how to evaluate and predict security situation which result from all kinds of network attack activities of 6LoWPAN under IOT environment. In this paper, IIESSA adopts artificial immune mechanism to evaluate quantitatively security situation of 6LoWPAN in SAC and SS, and use grey prediction method to predict security situation of 6LoWPAN. As a result, IIESSA can obtain effectively network attack activities from massive network information, and then can dynamic intelligent perceive and supervise IOT environment security situation.

2.1. Immunity-Based IOT Environment Security Situation Evaluation Method

Inspired by artificial immune system, this paper firstly presents the relevant concepts and formal definitions for self, non-self, antigen and detector to solve security situation evaluation problems under IOT environment. In IOT environment, all antigens are detected by the mature/memory detectors that have experienced self-tolerance, clonal selection and immune mutation. The more network attacks, the more detector clones. The antibody-concentration of memory detectors reflects quantitatively and real-timely the attack intensity and security situation that IOT faced.

Definition 1 Antigen set $Ag = \{ad \mid ad \subset S\}$ represents original IP packets under IOT environment, where antigenic determinant *ad* represents a *l*-bit binary feature string obtained by antigen-presenting of IP packet, it includes source/destination IP address, source/destination port number, protocol type, feature code and so on, shape-space $S = \{0,1\}^l$ represents all network activities, and *l* is a nature number (constant).

Definition 2 Self set $Self \subset Ag$ represents all normal network activities, non-self set $Nonself \subset Ag$ represents all illegal network activities, so that $Self \cup Nonself = Ag$ and $Self \cap Nonself = \phi$.

Definition 3 Immune detector set $D = \{\langle ab, p, t, age, cnt\rangle \mid ab \in S, p \in R, t, age, cnt \in N\}$, where *ab* represents antibody, *p* represents antibody-concentration, *t* represents tolerance value of immature detector, *age* represents the age of mature/memory detector, *cnt* represents the number of antigen matched by antibody, *R* represents the set of real numbers, and *N* represents the set of nature numbers.

Definition 4 Memory detector set $M_d = \{d \mid d \in D, d.cnt > \beta\}$, mature detector set $T_d = \{d \mid d \in D, d.age < \lambda, d.cnt < \beta\}$, immature detector set $I_d = \{d \mid d \in D, d.t < \alpha\}$, where $D = M_d \cup T_d \cup I_d$, α represents the tolerance threshold of immature detector, λ and β represents the lifecycle and activated threshold of mature detector respectively.

2.1.1. Detector Evolution

In the course of detector evolution, immature detectors can turn into mature detectors when immature detectors are successful during self-tolerance phase. When the matching times between a mature detector in its lifecycle and antigens are up to the activated threshold β, the mature detector clones itself and then evolves into memory detector, and when antigens are identified by a memory detector, the detectors cloned from this mature detector will be merged to mature/immature detector set. To ensure effectively identify antigens and make the diversity of antibody of detector so as to may handle known or unknown network attacks, three immune operators are introduced during evolving detector, namely affinity evaluation, clonal selection and immune mutation.

1) Affinity evaluation In this section, Hamming distance based matching algorithm [24] is adopted used for calculating affinity between detector and detector/antigen. Take the self-tolerance of detector as an example, the immature

detector's tolerance is successful if immature detector never match all elements of *Self* at α, conversely, it's dead. Suppose self $s \in Self$, immature detector $id \in I_d$, Equation (1) represents how to identify immature detector *id* by *s*, where 1/0 represents whether *id* match with *s* or not, l_d is the length of detector *id*, f_{affinity} is used for calculating affinity between *s* and *id*, $\gamma(0 \le \gamma \le 1)$ represents the threshold of affinity. Equation (2) is used for executing self-tolerance of immature detector *id*, and Equation (3) is used for accumulating the times of self-tolerance for *id* when the result of Equation (2) returns 1, and if $t \ge \alpha$, immature detector *id* evolves into mature detector.

$$f_{\text{match}}(s, id) = \begin{cases} 1, & f_{\text{affinity}} / l_d > \gamma \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

$$f_{\text{tolerance}}(s, id) = \begin{cases} 0, & \exists s \in Self, f_{\text{match}}(s, id) = 1 \\ 1, & \text{otherwise} \end{cases} \tag{2}$$

$$\begin{cases} T_d = T_d \cup id, \ I_d = I_d - id, & \text{iff } id \in I_d, id.t \ge \alpha \\ id.t = id.t + 1, & \text{iff } id \cdot t < \alpha \wedge f_{\text{tolerance}}(s, id) = 1 \end{cases} \tag{3}$$

2) Clonal selection Clonal selection operator is used for executing cell clonal operation of the mature detectors and memory detectors. Equation (4) is used for cloning detectors, where $\xi(>0)$ is a clonal constant, $N_d = T_d \cup M_d$ represents all mature detectors and memory detectors, n_d represents the sum of detectors which possess similarity antibody with detector $d(\in N_d)$. For Equation (5), T_{cln} and M_{cln} represent the clonal selection sets of the mature detectors and that of the memory detectors, respectively. After running clonal selection in one generation, the cloned detectors are added to the mature detector set, and the same detectors $d_t(\in T_d)$ existing in the clonal selection set T_{cln} and M_{cln} will be deleted.

$$C_{num}(d) = \lceil \xi \cdot (1 - n_d / N_d) \rceil \tag{4}$$

$$T_d = T_d \cup T_{cln} \cup M_{cln} - \{d_t \mid d_t \in T_{cln} \vee d_t \in M_{cln}\} \tag{5}$$

3) Immune mutation The purpose of immune mutation operator is to improve the diversity of detectors by mutating the gene of antibody of the corresponding detectors in order to enhance the identifying ability for antigens. Taking $(l_d - f_{\text{affinity}}(d, ag))$ bits from detector $d(\in N_d)$ matched by antigen $ag(\in Ag)$, and these bits are instead randomly by 1/0, where l_d represents the length of *d*. The mutated detector is regarded as immature detector that is renewed tolerance by self set.

2.1.2. Antigen Surveillance

During antigen surveillance, all antigens are detected by the mature and memory detectors. Firstly, the memory detector surveils antigens, antigens will be deleted from antigen set A_g if non-self antigens identified by this detector are successful, reversely, and this detector is deleted from memory detector set M_d if self antigen identified by this detector is successful. Secondly, the mature detector surveils antigen, the antigen will be deleted from antigen set A_g if non-self antigen

identified by this detector is successful, and this detector will be turned into memory detector if the accumulating times of mature detector matching antigens are up to the activated threshold β in its lifecycle λ. Reversely, the mature detector is deleted from mature detector set T_d if antibody identified by self antigen is successful or mature detector is not activated in its lifecycle. Lastly, to sustain the dynamic update of self set *Self*, the remainders of antigens are merged into *Self*, and then immature detector in I_d is matched by *Self* in order to keep detectors evolution dynamically.

Definition 5 Suppose η_1 (>0, constant) is the initial value of antibody-concentration of memory detector, η_2 (>0, constant) simulates the award factor of antibody of memory detector, θ (>0, constant) is the maintaining period of antibody-concentration of memory detector.

For mature detector, if its matching time is up to the activated threshold β, it is stimulated and cloned via Equation (4), and then merged into the memory detector set via Equation (6). Suppose *t* represents the order number of detector which can match antigen, memory detector will be cloned via Equation (7) when memory detector can successful match antigen, and meanwhile the antibody-concentration of memory detector will be increased via Equation (7). If memory detector isn't cloned again in the maintaining period θ, the antibody-concentration of memory detector will be decreased to zero via Equation (8), and it shows that the corresponding kind of antigen has been eliminated in IOT environment.

$$M_d = M_d \cup \{d \mid d \in T_d, d.p = \eta_1, d.age = 0\} \tag{6}$$

$$M_d = \{d \mid d \in M_d, d.p(t) = \eta_1 + \eta_2 \cdot d.p(t-1), d.age = 0\} \tag{7}$$

$$d.p = \begin{cases} d.p\left(1 - \dfrac{1}{\theta - d.age}\right), & d.age++ < \theta \\ 0, & d.age++ \geq \theta \end{cases} \tag{8}$$

2.1.3. Situation Evaluation

For evaluating quantitatively network security situation under IOT environment, the fatalness that IOT and its resource constrained devices undergo all kinds of attacks must be considered. To effectively classify for the illegal network attacks, the consanguinity method [33] is adopted used for classifying detectors in this paper. The significance for different resource constrained devices and different services must be considered under IOT environment. Let $St(t)\left(0 \leq St(t) \leq 1\right)$ denotes the security situation that IOT and its resource constrained devices faced at time *t*, where $St(t) = 1$ indicates extreme danger for the current system, $St(t) = 0$ indicates no danger. Consequently, $St(t)$ exactly reflects the variety of network security attacks that the current system has faced. Let $\varphi_j\left(0 \leq \varphi_j \leq 1\right)$ denotes the fatalness coefficient of the *j*th kind of the attack Att_j, $\mu_j\left(0 \leq \mu_j \leq 1\right)$ denotes the weightiness coefficient of the corresponding service, and $\omega_i\left(0 \leq \omega_i \leq 1\right)$ represents the weightiness coefficient of the *i*th device/node.

For the *i*th device/node, Equation (9) is applied to calculate the index value of

security situation of the jth kind of attack Att_j at time t, Equation (10) is used for calculating the index value of security situation of all kinds of attacks in the ith device/node.

$$St_{DNode_{ij}}(t) = 1 - \frac{1}{1 + \ln\left(\varphi_j \cdot \sum_{b \in Att_j(t)} d.p + 1\right)} \tag{9}$$

$$St_{DNode_i}(t) = 1 - \frac{1}{1 + \ln\left(\sum_j \left(\mu_j \cdot \varphi_j \cdot \sum_{d \in Att_j(t)} d.p\right) + 1\right)} \tag{10}$$

Under IOT environment, Equation (11) is applied to calculate the index value of security situation of the jth kind of attack Att_j at time t, Equation (12) is applied to calculate the index value of the all kinds of attacks.

$$St_{Net_j}(t) = 1 - \frac{1}{1 + \ln\left(\mu_j \cdot \varphi_j \cdot \sum_i \left(\omega_i \cdot \sum_{d \in Att_j(t)} d.p\right) + 1\right)} \tag{11}$$

$$St_{Net}(t) = 1 - \frac{1}{1 + \ln\left(\sum_i \left(\omega_i \cdot \sum_j \left(\mu_j \cdot \varphi_j \cdot \sum_{d \in Att_j(t)} d.p\right)\right) + 1\right)} \tag{12}$$

2.2. IOT Environment Security Situation Prediction Method

The variation of security situation under IOT environment is affected by many existed uncertain factors, so the prediction results of network security situation actually possess uncertainty. The grey prediction theory is the most key part of grey theory because of its merits in the short period, such as a few data samples, facility operation, and high prediction precision [28]. At present, the grey prediction theory is usually applied to predict in industry, agriculture, military affairs and science technology etc. The grey prediction theory is adopted to predict the time series of security situation obtained by the evaluation method of network security situation based on immune mechanism. GM(1,1) model can predict precisely for the data sequence that possesses the characteristics of exponential curve, but it doesn't effective for the random data sequence [34]. Therefore, the weaken operator D [35] is introduced to be used for decreasing the randomcity of the original data sequence in order to improve the prediction precision of GM(1,1) model in this paper.

Definition 6 Suppose the original data sequence of network security situation under IOT environment $X^{(0)} = \left\{x^{(0)}(k) \mid k = 1, 2, \cdots, n\right\}$, if $x^{(0)}(i) > x^{(0)}(i+1)$, then $d(i+1) = d(i) + 2\left(x^{(0)}(i) - x^{(0)}(i+1)\right)$, and if $x^{(0)}(i) < x^{(0)}(i+1)$, then $d(i+1) = d(i)$, where $i = 1, 2, \cdots, n-1$, $d(1) = 0$, so $D = \left\{d(k) \mid k = 1, 2, \cdots, n\right\}$ is regarded as a weaken operator.

The 1-AGO sequence $X^{(1)} = \left\{x^{(1)}(k) \mid x^{(1)}(k) = \sum_{i=1}^{k}\left(x^{(0)}(i) + d(i)\right)\right\}$ is generated by $X^{(0)}$ and D, where $k = 1, 2, \cdots, n$. The neighbor datum mean generation sequence of $x^{(1)}$ is $Z^{(1)} = \left\{z^{(1)}(k) \mid k = 1, 2, \cdots, n\right\}$, where

$z^{(1)}(k)=\sigma x^{(1)}(k-1)+(1-\sigma)x^{(1)}(k)$, $\sigma=0.5$, $k=1,2,\cdots,n$. Equation (13) represents the whitenization equation of GM(1,1) model, where *a* is the development coefficient, its size and sign reflect the development situation of $x^{(0)}$, while *b* is the input of the system and its value denotes some kinds of grey information.

$$\frac{\mathrm{d}x^{(1)}}{\mathrm{d}t}=-ax^{(1)}+b \tag{13}$$

The coefficients, *a* and *b*, can be calculated by the equation $\hat{\omega}=(a,b)^{\mathrm{T}}=\left(B^{\mathrm{T}}B\right)^{-1}B^{\mathrm{T}}Y$, where Y is listed in Equation (14).

$$Y=\begin{bmatrix}x^{(0)}(2)+d(2)\\ x^{(0)}(3)+d(3)\\ \vdots\\ x^{(0)}(n)+d(n)\end{bmatrix},\quad B=\begin{bmatrix}-z^{(1)}(2) & 1\\ -z^{(1)}(3) & 1\\ \vdots & \vdots\\ -z^{(1)}(n) & 1\end{bmatrix} \tag{14}$$

Consequently, the simulation values of $x^{(1)}(k+1)$ and $x^{(0)}(k+1)$ can be obtained by Equation (15) and Equation (16) respectively, where $k=1,2,\cdots,n$.

$$\hat{x}^{(1)}(k+1)=\left(x^{(0)}(1)-b/a\right)e^{ak}+b/a \tag{15}$$

$$\hat{x}^{(0)}(k+1)=\hat{x}^{(1)}(k+1)-\hat{x}^{(1)}(k)-d(k+1) \tag{16}$$

Known from $X^{(0)}$ and *D*, $d(k+1)$ is regarded as an uncertain data if $k=n$. Therefore, some simple fitting methods, such as the residual error identification and the linear regression, may be introduced to be used for calculating $d(k+1)$ by fitting *D* in GM(1,1) model.

3. Simulation Experiment

To demonstrate the effectiveness of the proposed methods, which are network security situation evaluation method and network security situation prediction method, in this paper, we consider evaluating and predicting network security situations that IOT environment is suffering respectively a specific attack and overall attacks. The experimental platform is mainly related to network simulator Cooja based on Contiki, PCs, Laptops and resource constrained devices (*i.e.* TI MSP430x/wismote, Atmel AVR/micaz). The simulating experimental attacks mainly include some typical network attacks, such as Spoof, Sinkhole and Sybil etc. And the provided network services under IOT environment mainly relate to WWW, FTP and E-mail. For the length of antigen and antibody, a 288-bit binary string is considered that it consists of source/destination IP address, source/destination port, protocol type and so on.

3.1. Experimental Parameter Settings

According to the proposed methods, the experimental parameter settings mainly include two aspects, namely the immune identifying parameters and the situation evaluation parameters. In the immunity-based IOT environment security situation evaluation method, its immune identifying parameters firstly are listed

in Table 1. γ is used for identifying illegal network activities by calculating the affinity between antibody and antigens. To obtain the higher detection rate (TP, True Positive) and lower false alarm rate (FP, False Positive) from security situation evaluation method. α, β and λ are three key parameters that immature detectors are evolved as memory detectors. For memory detectors, the values for parameters θ, η_1 and η_2 [28] are used for maintaining and calculating the antibody-concentration of memory detectors in order to reflect real- timely network security situation under IOT environment.

For the situation evaluation parameters, according to the significance for the resource constrained devices/nodes and the provided services, and the fatalness of specific network attacks under IOT environment, the weightiness coefficients of network services WWW, FTP and E-mail (Identified by protocol port number) are set to 0.8, 0.7 and 0.8, respectively. The biggest value selected from among the importance of all services of a resource constrained device/node is viewed as the weightiness coefficient of the corresponding device/node. The fatalness coefficients of network attacks, which Spoof, Sinkhole and Sybil, are set to 0.8, 0.9 and 0.7, respectively.

3.2. Experimental Results

In simulating experiments, we obtained three actual network attack intensities that IOT environment suffered in 120 seconds in Figure 2, namely Spoof attack intensity for WWW service of device/node, Sinkhole attack intensity for FTP service of device/node, and the overall attack intensity that IOT environment suffered. Take WWW service as an example, the values of actual network attack intensity in Figure 2(a) indicate that the WWW service of device/node is suffering the total amount of network attack packets per second, and the attack frequency at each second that WWW service suffered is from 9000 packets to 33,900 packets. To evaluate and predict network security situation of different network attack intensities given by Figure 2, Figure 3 shows the curves of attack intensity, situation evaluation and situation prediction for Spoof attacks that WWW service of device/node suffered, respectively. Figure 4 shows the curves of attack intensity, situation evaluation and situation prediction for Sinkhole attacks that FTP service of device/node suffered. For the overall attacks that

Table 1. The immune identifying parameters of security situation evaluation.

Parameter	Value
Affinity threshold γ	0.9
Tolerance period of immature detector α	1
Activated threshold of mature detector β	10
Lifecycle of mature detector λ	90
Maintaining period of antibody-concentration θ	1
Initial value of antibody-concentration η_1	0.0010
Award factor of antibody η_2	0.9998

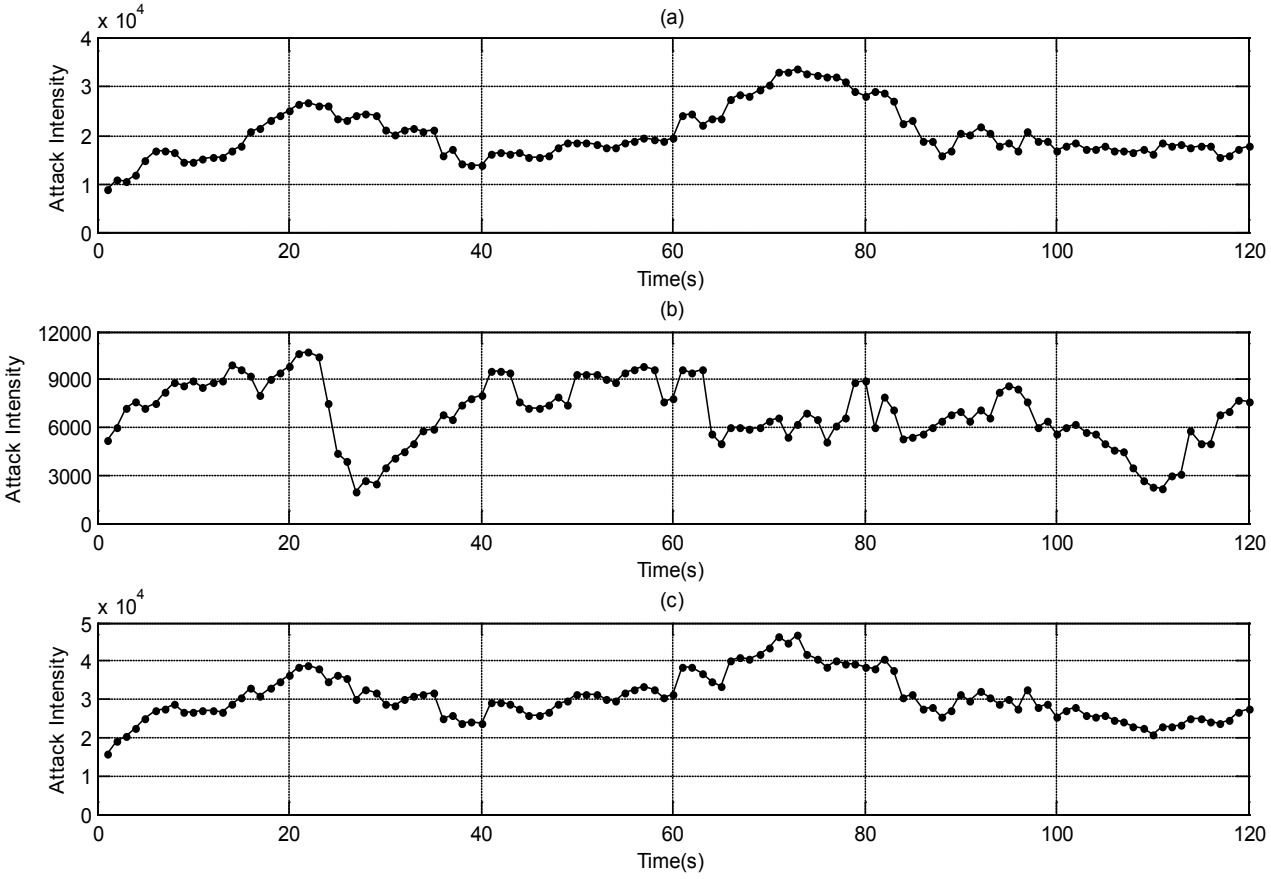

Figure 2. (a) Spoof attack intensity for the WWW service of device/node, (b) Sinkhole attack intensity for the FTP service of device/node, (c) Overall attack intensity that the IOT suffered.

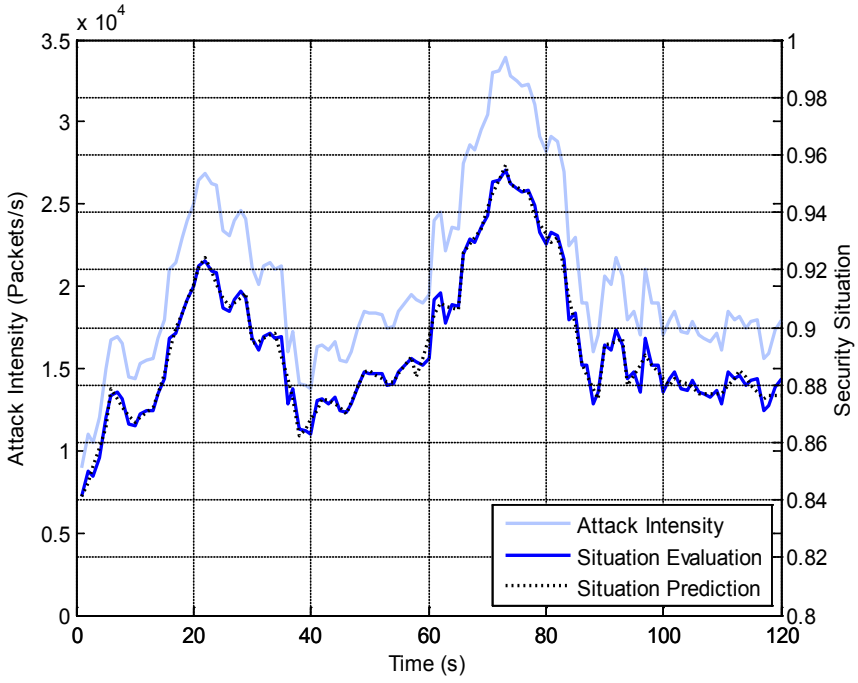

Figure 3. Security situation curves for Spoof attacks that WWW service of device/node suffered.

IOT environment suffered, the curves of the corresponding attack intensity, situation evaluation and situation prediction are given in Figure 5.

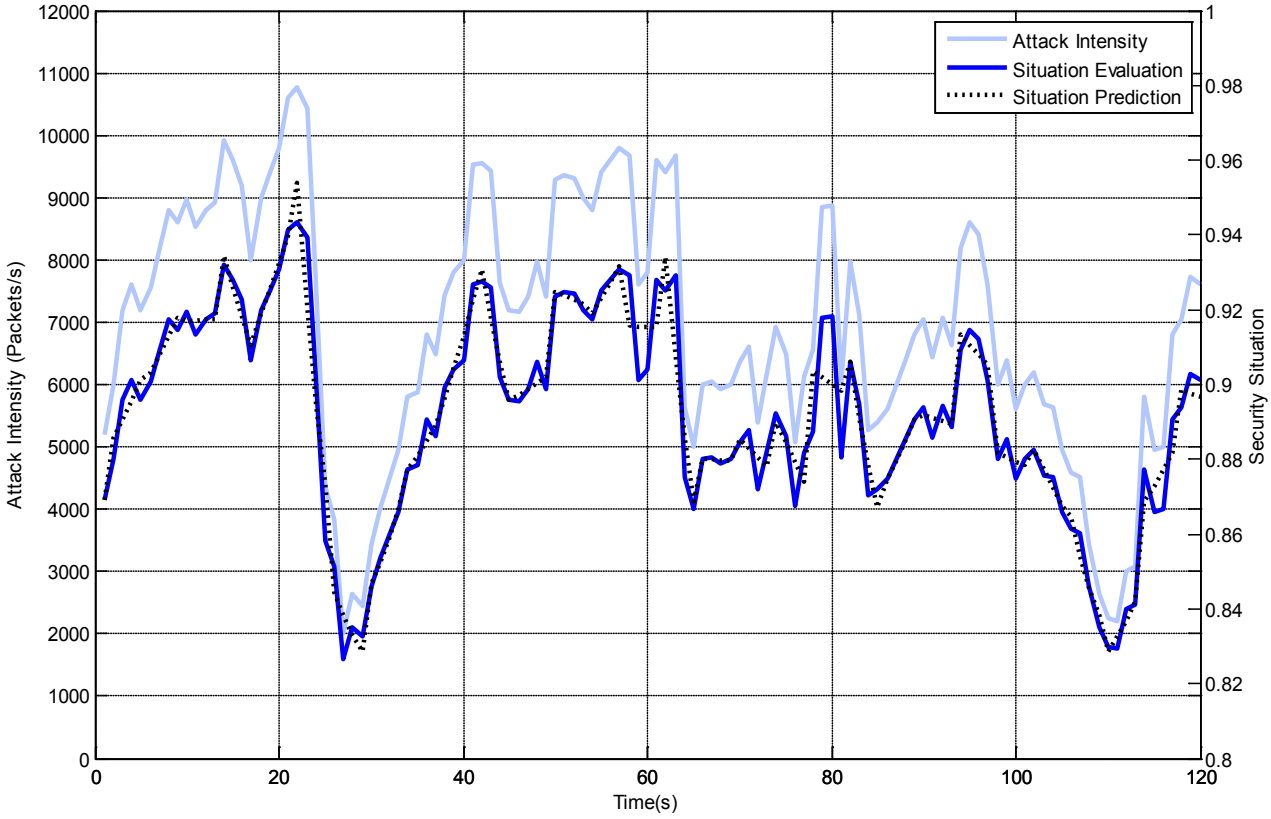

Figure 4. Security situation curves for Sinkhole attacks that FTP service of device/node suffered.

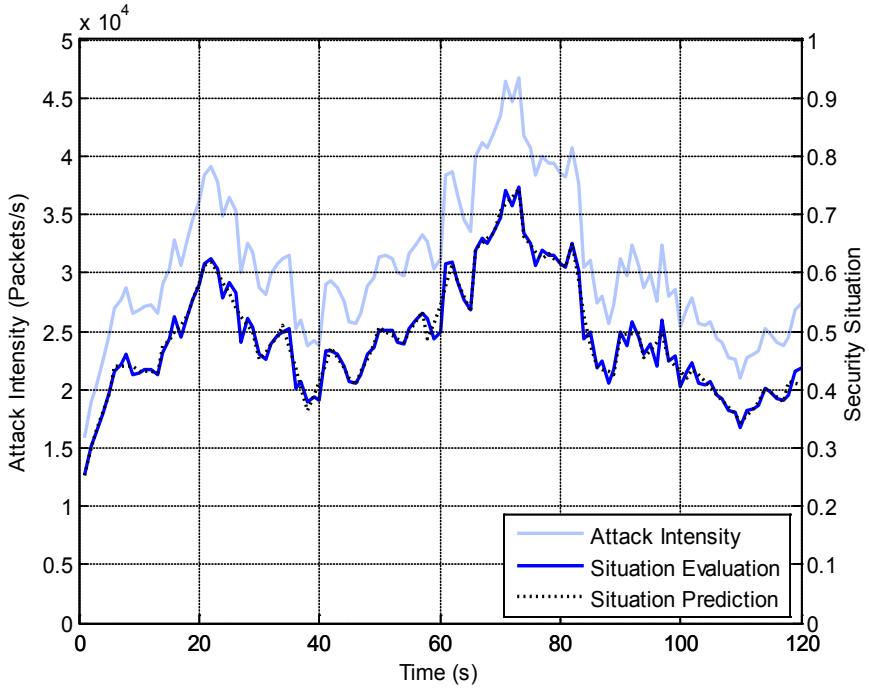

Figure 5. Security situation curves for the overall attacks that IOT environment suffered.

Known from Figures 3-5, the evaluation results of network security situation can be calculated reasonably by the proposed immune-based network security situation evaluation method. When network attack intensity increases, antibody-concentration of memory detector increases correspondingly, conversely, it decreases. That is to say, the situation evaluation curves are accordant with the corresponding attack intensity curves. Therefore, the evaluation results of network security situation can reflect real-timely the situation changes of network attacks under IOT environment, and meanwhile the proposed method can keep the higher alert level when the same attacks happened again according to the antibody-concentration phenomenon of BIS.

In the process of situation prediction, the sliding window mechanism and the grey prediction method are adopted. For the original data sequence that is used for predicting network security situation, it is obtained in turn by using the proposed situation evaluation method in terms of equal interval time (sec.). When we need to predict the element value of original data sequence at time $T+1$, we firstly take $N(=10)$ data of this data sequence before time $T+1$. The situation prediction curves in Figures 3-5 show that the grey prediction method can predict precisely network security situation of IOT. However, the evaluation curve of network security situation isn't regular because of the randomicity of network attacks. In other words, the precision of security situation prediction in Figures 3-5 will be more affected when the taken N situation values possess more randomicity. To ensure the precision of the prediction results, the grey prediction method need to check the errors between the evaluation results and the prediction results of network security situation. The residual series of grey prediction theory can be adopted to improve the prediction results that haven't met the precision requirements, and the general strategy of error detection is the relative error detection [34].

The experimental results show that IIESSA can evaluate and predict network security situation for both the specific attack and the overall attacks that IOT and its resource constrained devices/nodes suffered. Simultaneously, the evaluation and prediction results of network security situation can reflect really network attack activities under IOT environment.

4. Conclusions

Inspired by BIS, an immunity-based IOT environment security situation awareness model (IIESSA) is proposed in this paper. The merit of IIESSA is that many network security problems can be mapped to the corresponding biological immune problems, and its corresponding immune mechanisms are adopted to solve security problems of IOT environment. Compared with conventional models, IIESSA possesses many advantages, such as self-learning, robust, adaptability and real-time etc. Security situation evaluation method in IIESSA can surveil dynamically network security activities of IOT by using immune mechanism so that network security administrator can perceive timely current network security situation. And meanwhile security situation prediction method

in IIESSA is used for estimating and handling the specific network attacks that IOT will be suffered in the next step. Therefore, IIESSA is helpful for network security administrators to judge and handle network anomaly activities in order to improve the security of IOT environment. Although the proposed model has got some very impressive results, it is still under development. We will further improve this model to calculate exactly the results of evaluation and prediction of network security situation in future work.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant Nos. 61173159, 61572334, 61173036, China Postdoctoral Science Foundation under Grant No. 2014M562102, Hunan Provincial Natural Science Foundation of China under Grant Nos. 2015JJ2112, the Scientific Research Fund of Hunan Provincial Education Department of China under Grant No. 12B099, the Scientific Research Foundation of Huaihua University under Grant No. HHUY2015-08.

References

[1] Wallgren, L., Raza, S. and Voigt, T. (2013) Routing Attacks and Countermeasures in the RPL-Based Internet of Things. *International Journal of Distributed Sensor Networks*, 1-11. https://doi.org/10.1155/2013/794326

[2] Li, S.C., Xu, L.D. and Zhao, S.S. (2015) The Internet of Things: A Survey. *Information Systems Frontiers*, **17**, 243-259.

[3] IERC (2013) Coordinating and Building a Broadly Based Consensus on the Ways to Realize the Internet of Things in Europe. www.internet-of-things-research.eu/pdf/Poster_IERC_A0_V01.pdf

[4] Kirtsis, D. (2011) Closed-Loop PLM for Intelligent Products in the Era of the Internet of Things. *Computer-Aided Design*, **43**, 479-501.

[5] Bi, Z.M., Xu, L.D. and Wang, C.G. (2014) Internet of Things for Enterprise Systems of Modern Manufacturing. *IEEE Transactions on Industrial Informatics*, **10**, 1537-1546.

[6] Sun, X.Y. and Wang, C.G. (2011) The Research of Security Technology in the Internet of Things. In: Jin, D. and Lin, S., Eds., *Advances in Computer Science, Intelligent System and Environment*, Vol. 105, Springer, Berlin, Heidelberg, 113-119. https://doi.org/10.1007/978-3-642-23756-0_19

[7] Whitmore, A., Agarwal, A. and Xu, L.D. (2015) The Internet of Things—A Survey of Topics and Trends. *Information Systems Frontiers*, **17**, 261-274.

[8] Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015) Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks*, **76**, 146-164.

[9] Javanmardi, S., Shojafar, M., Shariatmadari, S. and Ahrabi, S.S. (2014) FR Trust: A Fuzzy Reputation-Based Model for Trust Management in Semantic P2P Grids. *International Journal of Grid and Utility Computing*, **6**, 57-66. https://doi.org/10.1504/IJGUC.2015.066397

[10] Li, H. and Zhou, X. (2011) Study on Security Architecture for Internet of Things. In: Zeng, D., Eds., *Applied Informatics and Communication. ICAIC* 2011. *Communications in Computer and Information Science*, Vol. 224, Springer, Berlin, Heidel-

berg, 404-411. https://doi.org/10.1007/978-3-642-23214-5_53

[11] Abie, H. (2009) Adaptive Security and Trust Management for Autonomic Message-Oriented Middleware. *Proceedings of IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, Macau, 12-15 October 2009, 810-817.

[12] Habib, K. and Leister, W. (2013) Adaptive Security for the Internet of Things Reference Model. *Proceedings of Norwegian Information Security Conference*, NISK, Stavanger, 13-24.

[13] Yan, Z., Zhang, P. and Vasilakos, A.V. (2014) A Survey on Trust Management for Internet of Things. *Journal of Network and Computer Applications*, **42**, 120-134.

[14] Raza, S., Wallgren, L. and Voigt, T. (2013) SVELTE: Real-Time Intrusion Detection in the Internet of Things. *Ad Hoc Networks*, **11**, 2661-2674.

[15] Hossain, M.S. and Raghunathan, V. (2010) AEGIS: A Lightweight Firewall for Wireless Sensor Networks. In: Rajaraman, R., Moscibroda, T., Dunkels, A. and Scaglione, A., Eds., *Distributed Computing in Sensor Systems. DCOSS* 2010. *Lecture Notes in Computer Science*, Vol. 6131, Springer, Berlin, Heidelberg, 258-272. https://doi.org/10.1007/978-3-642-13651-1_19

[16] Macfarlane, R., Buchanan, W., Ekonomou, E., Uthmani, O., Fan, L. and Lo, O. (2012) Formal Security Policy Implementations in Network Firewalls. *Computers & Security*, **31**, 253-270.

[17] Hu, H.X., Ahn, G.J. and Kulkarni, K. (2012) Detecting and Resolving Firewall Policy Anomalies. *IEEE Transactions on Dependable and Secure Computing*, **9**, 318-331. https://doi.org/10.1109/TDSC.2012.20

[18] Wilhelm, M., Martinovic, I., Schmitt, J.B. and Lenders, V. (2013) Air Dominance in Sensor Networks: Guarding Sensor Motes Using Selective Interference. 1-16. arXiv preprint arXiv:1305. 4038

[19] Xiao, Q., Qin, Y. C., Xu, C. and Li, K.L. (2013) Lightweight Detecting and Resolving Algorithm for Firewall Policy Conflict. *Proceedings of the 5th International Conference on Ubiquitous and Future Networks*, Da Nang, 2-5 July 2013, 234-239.

[20] Kubler, S., Främling, K. and Buda, A. (2014) A Standardized Approach to Deal with Firewall and Mobility Policies in the IoT. *Pervasive and Mobile Computing*, **20**, 100-114.

[21] Wang, L.H., Teng, H.K. and Yu, G.H. (2014) Sensors Access Scheme Design Based on Internet of Things Gateways. *Proceedings of the 5th International Conference on Intelligent Systems Design and Engineering Application*, Hunan, 15-16 June 2014, 901-904.

[22] Zhu, Q., Wang, R.C., Chen, Q., Liu, Y. and Qin, W.J. (2010) IoT Gateway: Bridging Wireless Sensor Networks into Internet of Things. *Proceedings of IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Co*mputing, Hong Kong, 11-13 December 2010, 347-352.

[23] Schrickte, L.F., Montez, C., De Oliveira, R. and Pinto, A.R. (2013) Integration of Wireless Sensor Networks to the Internet of Things Using a 6LoWPAN Gateway. *Proceedings of the 3rd Brazilian Symposium on Computing Systems Engineering*, Niteroi, 4-8 December 2013, 119-124. https://doi.org/10.1109/sbesc.2013.37

[24] Forrest, S., Perelson, A.S., Allen, L. and Cherukuri, R. (1004) Self-Nonself Discrimination in a Computer. *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, 16-18 May 1994, 202-202.

[25] Timmis, J., Hone, A., Stibor, T. and Clark, E. (2008) Theoretical Advances in Artificial Immune Systems. *Theoretical Computer Science*, **403**, 11-32.

[26] Shi, Y.Q., Li, R.F., Peng, X.N. and Yue, G.X. (2016) Network Security Situation Pre-

diction Approach Based on Clonal Selection and SCGM(1, 1)c Model. *Journal of Internet Technology*, **17**, 421-429.

[27] Shi, Y.Q., Li, R.F., Zhang, Y. and Peng, X.N. (2015) An Immunity-Based Time Series Prediction Approach and Its Application for Network Security Situation. *Intelligent Service Robotics*, **8**, 1-22. https://doi.org/10.1007/s11370-014-0160-z

[28] Shi, Y.Q., Li, T., Chen, W. and Zhang, R.R. (2009) A Quantitative Model for Network Security Situation Awareness Based on Immunity And Grey Theory. *Proceedings of the* 2009 *ISECS International Colloquium on Computing, Communication, Control, and Management*, Sanya, 8-9 August 2009, 14-18. https://doi.org/10.1109/CCCM.2009.5267847

[29] Shamshirband, S., Anuar, N.B., Laiha, M., Kiah, M., Rohani, V.A., Petković, D., Misra, S. and Khan, A.N. (2014) Co-FAIS: Cooperative Fuzzy Artificial Immune System for Detecting Intrusion in Wireless Sensor Networks. *Journal of Network and Computer Applications*, **42**, 102-117.

[30] Mostafaei, H. and Shojafar, M. (2015) A New Meta-Heuristic Algorithm for Maximizing Lifetime of Wireless Sensor Networks. *Wireless Personal Communications*, **82**, 723-742. https://doi.org/10.1007/s11277-014-2249-2

[31] Naranjo, P.G.V., Shojafar, M., Mostafaei, H., Pooranian, Z. and Baccarelli, E. (2017) P-SEP: A Prolong Stable Election Routing Algorithm for Energy-Limited Heterogeneous Fog-Supported Wireless Sensor Networks. *The Journal of Supercomputing*, **73**, 733-755.

[32] Saybani, M.R., Shamshirband, S., Hormozi, S.G., Wah, T.Y., Aghabozorgi, S., Pourhoseingholi, M.A. and Olariu, T. (2015) Diagnosing Tuberculosis with a Novel Support Vector Machine-Based Artificial Immune Recognition System. *Iranian Red Crescent Medical Journal*, **17**, e24557. https://doi.org/10.5812/ircmj.17(4)2015.24557

[33] Li, T. (2005) An Immunity Based Network Security Risk Estimation. *Science in China Series F. Information Sciences*, **48**, 557-578.

[34] Deng, J.L. (2002) Grey System Theory. Publishing House of Huazhong University of Science and Technology, Wuhan.

[35] Wei, B.G., Zhang, W.Z. and Guo, Z.S. (2000) Method of BX Data Producing for Grey Forecast and Its Application for Environmental Forecast. *Journal of Qiqihar University*, **16**, 59-61.