Computing and Informatics, Vol. 34, 2015, 1089–1112

NETWORK PROACTIVE DEFENSE MODEL BASED ON IMMUNE DANGER THEORY

Yu Wang, Zhenxing Wang, Liancheng Zhang, Yazhou Kong

National Digital Switching System Engineering and Technological Research Center
JianXue Str. 9
450000 Zhengzhou, China
e-mail: stonchor@gmail.com

Abstract. Recent investigations into proactive network defense have not produced a systematic methodology and structure; in addition, issues including multi-source information fusion and attacking behavior analysis have not been resolved. Borrowing ideas of danger sensing and immune response from danger theory, a proactive network defense model based on danger theory is proposed. This paper defines the signals and antigens in the network environment as well as attacking behavior analysis algorithm, providing evidence for future proactive defense strategy selection. The results of preliminary simulations demonstrate that this model can sense the onset of varied network attacks and corresponding endangered intensities, which help to understand the attack methods of hackers and assess the security situation of the current network, thus a better proactive defense strategy can be deployed. Moreover, this model possesses good robustness and accuracy.

Keywords: Network security, danger theory, proactive defense model, attacking behavior analysis, real-time awareness

1 INTRODUCTION

Internet security is attracting more and more attention [1, 2]. Traditional defense technologies such as firewall [4], network monitoring and intrusion detection system utilize passive security defense strategies to implement protection. However, a network under this type of asymmetric attack-defense architecture will always be trailing behind varied attack techniques. It will also be lacking essential proactivity

and the ability to initiate effective counter measures, which are especially critical for networks related to national security or warfare.

Recent studies [3, 5, 6, 7] show that network defense systems utilizing proactive technologies are playing a more and more important role in confronting numerous attacks, where "proactive" means to create or control a situation by causing something to happen rather than responding to it after it has happened. Compared to conventional methods, proactive defense technology is able to assist in discovering network vulnerabilities as well as identifying potential threats, to maximally reduce losses [8]. Thus, proactive network defense is a kind of intelligent initiative defense, which aims at capturing and analyzing attack incident in a highly active and timely way, as well as taking measures to improve local network security. Significant research efforts have focused on addressing proactive network defense technology. Typical proactive network defense technologies include honeynet and honeypot traps that are deliberately set to detect, deflect, counteract or in some manner interact with unauthorized access attempts, in order to trace and analyze their activities and assist in protecting the real production system.

Barford et al. [9] explored ways to integrate honeypot data into network security monitoring, with the goal of classifying and summarizing the data to provide ongoing situational awareness. However, this approach has to combine 4 types of methodologies; besides which, more than 18 types of events must be considered to analyze the honeynet events which makes implementation extremely complex. Pham et al. [10] proposed a method to identify and group together traces left on low interaction honeypots. The approach was validated thanks to the data collected with the distributed Leurr.com system. However, this method is time consuming. It generally takes several hundred days, to distinguish the relevant traces, which means a timely response may not be possible. Lee et al. [11] presented a conceptual framework of the Social Honeypot Project to uncover social spammers who target online communities. However, this process can take several months to distinguish between legitimate users and spammers. Although the level of accuracy is acceptable compared to the similar schemes, this approach is far from the real-time requirements of practical proactive defense.

As was mentioned above, issues related to implementation complexity and real-time performances have limited their potential applications of previous proactive network defense systems. Researchers have found the biological immune system with outstanding merits can be used to solve problems in network security, borrowing related ideas from biological immunology, a danger theory [12] based network proactive defense model (DTNPD model) is proposed combining honeynet trapping, attacking behavior analysis and traffic camouflage techniques. Specifically: inspired by immune danger theory, the malicious attacking behavior in and out of an intranet is captured and analyzed through multi-source information fusion, enhancing the ability of proactive defense system to identify danger signals and resist network attacks.

Compared to the previous solutions, DTNPD model utilizes only 4 types of signals as inputs for the attacking behavior analysis algorithm which means it is

much simpler to implement, and the computational complexity of the algorithm is linear. Moreover, the most important characteristic is that the DTNPD model holds good consistency with the real-time attack intensity. An attack attempt can be sensed and evaluated with minutes as the unit of measurement, in contrast to the days and even years sometimes required in previous approaches. Thus DTNPD is superior to most current proactive defense systems, which satisfies the demand of practical proactive network defense. Furthermore, based on 125 simulations in the given experimental environment, the average accuracy achieved in sensing aggressive attacks was 92.37 % which is higher than any of the other previous approaches.

The remainder of this paper is organized as follows: in Section 2, a network proactive defense model based on danger theory is proposed, then Section 3 and Section 4 describe the functioning of Compartment A and Compartment B, two key part of the DTNPD model respectively. Section 5 presents multiple simulations and the corresponding analysis, followed by the conclusions provided in the final section.

2 THE DTNPD MODEL

2.1 Danger Theory and DCA

Matzinger proposed the danger theory [12], which theoretically explained many problems encountered in traditional theory of "self/non-self" immune response pattern. When a cell undergoes necrosis, it will degrade in a chaotic manner and produce various molecules called "danger signals". Antigen Presenting Cells (APCs) are responsible for collecting and identifying these danger signals which are divided into two categories: generated internally (such as by the body itself) and generated by external invasions (such as bacteria). Both types of signals are able to stimulate the APCs and trigger the immune response.

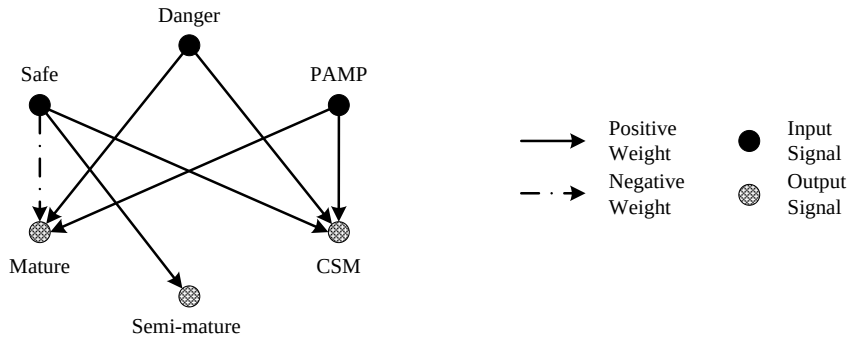


Figure 1. Abstract signal processing model in DCA

The Dendritic Cell (DC) is known as the most powerful APC so far. By modeling the behavior of dendritic cells, Greensmith designed and implemented the

Dendritic Cell Algorithm (DCA) [13]. The algorithm follows the antigen presenting process of immune system, firstly to extract input signals from collected antigens, and then calculate the "antigen expression" as the output signals to sense the "endangered degree" of antigens, through comparison with the preset threshold, to provide an evaluation reference for the next phase of operations.

The input signals for DCA include Danger, Safe, PAMPs (Pathogenic Associated Molecular Patterns) and Inflammation, while the output signals are CSM (Co-stimulation), Semi-mature and Mature. The abstract signal processing model in DCA is shown in Figure 1.

As a firm indicator to inform the innate immune system that an anomalous state is detected by DCs, PAMPs are produced by microorganisms [14]. Specific PAMPs bind to specific pattern recognition receptors on DCs, which causes the production of CSM and Mature signals.

Danger signal is a kind of by-product of cellular degradation which indicates the potential damages to tissue. Receiving danger signals would lead to DCs differentiation to the fully mature state and the release CSM and Mature signals, however, the presence of them may or may not indicate an anomalous situation.

The Safe signal is a result of healthy cell death termed as apoptosis. When DCs receive safe signals, the impact includes:

1. a resulting production of CSM signals;
2. production of Semi-mature signals indicating DCs have collected antigens in a healthy tissue environment;
3. suppression of the production of Mature signals which correspond to Danger and PAMPs inputs.

Inflammation signals not only indicate the presence of inflammatory cytokines but also the increased temperature in the tissue, which results in more cells being recruited into affected tissue. That is, inflammation signals have an amplifying effect on the other signals.

The function of CSM signals, together with other receptors in the natural immune system, is to incur the DCs entering the lymph node for antigen presenting. Semi-mature only responds to the Safe signals; PAMPs and Danger signals will lead to the increase of Mature, while Safe signals will reduce that.

2.2 Architecture of DTNPD Model

Immune system modeling under danger theory has many similarities with the network proactive defense model especially in terms of the structural characteristics and the problems encountered. Firstly, both are complex systems composed of independent but interactive objects. Independent objects of the former are various types of lymphocytes, while for the latter they are the proactive defense nodes. Secondly, both aim to ensure the safe operations of the protected objects in a changing environment. The key functions of the former are to detect and determine the "danger

signals", to recognize and respond to "dangerous" antigens, protecting the living organisms from viruses; while those of the latter are to capture and study threatening behavior through proactive defense nodes, to respond to network attacks in a timely way, protecting the safe operations of a network system.

DTNPD model is composed of five functional components including Signal Collection (SigC), Antigen Collection (AgC), Behavior Analysis (BhA), Data Communication (DatC) and Strategy Control (StrgC), which is denoted as $DTNPD=\{SigC, AgC, BhA, DatC, StrgC\}$.

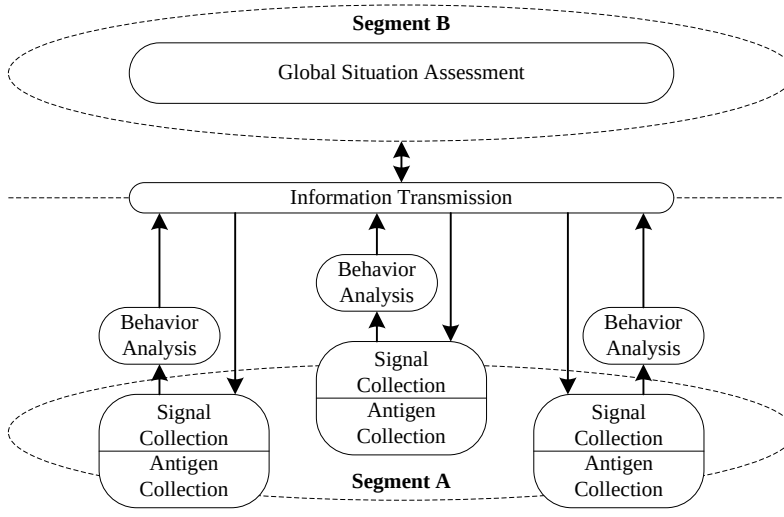


Figure 2. Architecture of DTNPD model

The Signal Collection component is responsible for collecting all types of signals determined by the network environment, operating system, resources and time, be denoted as $SigC: NetEnvn \times OS \times Resrc \times Time \rightarrow \{Danger, Safe, PAMPs, Inflam\}$, in which *Danger*, *Safe*, *PAMPs* and *Inflam* are signal types respectively indicating Danger signals, Safe signals, Pathogenic Associated Molecular Patterns signals and Inflammation signals, which are inspired by and correspond to the signals in the immune system.

The Antigen Collection component collects the antigen information related to signals transforming, in order to assist in examining the cause of transforming signals. The process is denoted as $AgC: OS \times Resrc \times Time \rightarrow Antigen$.

After the collection process, the Behavior Analysis component is used to analyze the signals and antigens with a given behavior analysis algorithm. The process is denoted as $BhA : SigC \times AgC \times Algorithm \rightarrow \{Mature, SemiM, CSM\}$, where a *Mature* signal indicates that a defense node is in the endangered state, a *SemiM* signal indicates the safe state, and *CSM* denotes the costimulatory molecules signal,

which in the immune system is used as a marker of maturation and in the DTNPD model is used to control the attacking behavior analysis cycle.

The Data Communication component is responsible for secure data transmission in the defense model. Since potential intruders may exist inside and outside the intranet, secure transmission utilizes not only encryption technology to prevent deep packet inspection, but also traffic camouflage implementation to combat traffic analysis attack.

The Strategy Control component receives the results of the attacking behavior analysis, based on which, this component then dynamically generates and deploys strategies at the defense nodes to acquire the surrounding endangered degree, which makes DTNPD model more deceptive. At the same time, it has to be on full alert to the intrusion behavior, avoiding some malicious activities launched from the defense model by the intruders.

2.3 Discussion

In a practical implementation, inspired by the immune system where the information flow passes between the lymph nodes and tissue, we define Compartment A as the environment for collecting signals and antigens, and for preliminary analysis, composed of multi-Honey DC. We define Compartment B as the decision making part, composed of a multi-Responder, to respond with appropriate strategies. Figure 3 gives an example of a DTNPD model implementation.

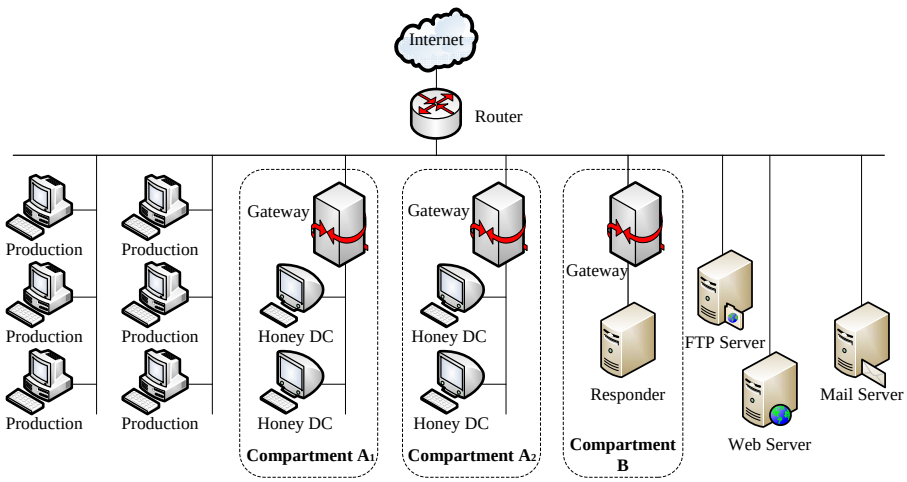


Figure 3. Practical example of DTNPD model

"Honey DC" is the proactive defense node for implementing the functions of SigC, AgC and BhA. We also define "Responder", as the response node to accomplish StrgC. Each Honey DC disguises itself as a normal production host, while

Responder exists in the form of an application server, such as a database server. Between Honey DCs and the Responder, secure communication of data should be strictly considered to prevent deep packet inspection and traffic analysis.

The Gateway is responsible for connecting a proactive defense system and other networks, while controlling all the traffic flowing through. On the data link layer, the transparency of the gateway puts Compartment A and the production hosts in the same network segment so that the logical location and functional representation of Compartment A are entirely consistent with those of the production network.

For camouflage purposes, the communication channels between Compartment A and Compartment B are exposed to the network segment, where some risks do exist. Attackers within or outside of the segment are likely to adopt traffic analysis to identify and determine the traffic between the two compartments, in order to identify the proactive defense system deployed. Therefore, communications between Compartment A and B should use the traffic camouflage method to guarantee data transmission on the basis of identities hidden.

3 COMPARTMENT A

In order to sense the surrounding danger of a local network, each Honey DC in Compartment A is responsible for attacking behavior analysis based on the sampling of signals and antigens, and then presents the results of this preliminary analysis to the Responder. Drawing lessons from the DCA [15], the general analysis process of a single Honey DC is shown in Figure 4.

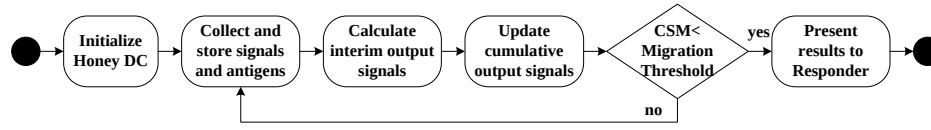


Figure 4. Overview diagram of Honey DC processing

In this process, the input signals are pre-classified as PAMPs, Danger, Safe and Inflammation, and the output signals includes CSM, Semi-mature and Mature, as explained above, indicating different types respectively. Each Honey DC has to collect and store signals and antigens, transforming the input signals into the outputs.

The migration threshold is a random number within a given range, and it is by adjusting this threshold that the life span of the analysis process is controlled. Before the migration occurs, Honey DC calculates the interim values of three output signals, along with the former values, which are added as to form the cumulative output results. This is done in each iteration.

To function perfectly, the mapping of signals and antigens from danger theory to network defense is the first critical factor for DTNPD model. In Sections 3.1 and 3.2,

we will select the signals and antigens by analyzing the nature of each respectively. The attacking behavior analysis performed by single Honey DC is another important factor which will be described in Section 3.3.

3.1 Signals

In vivo, DCs gather all the input signals, through the receptor network, signal transduction and gene regulatory processes, to produce the output signals. Natural DCs are very sensitive to the environment change; similarly, Honey DC nodes in the DTNPD model are also subject to the change of signal matrix values. For proactive network defense system, attacks launched by hackers and the corresponding countermeasures can be divided into three categories:

1. Attacks using the known weaknesses or vulnerabilities which are deliberately reserved in the proactive defense system. In this case, the system can easily detect these attacks.
2. Attacks using undisclosed vulnerabilities of an operating system or application. In this case, the defense system can only determine the malicious intent by attacking behavior mode.
3. For those attacks which are known but are difficult to prevent (e.g. DDoS attacks), the defense system can only determine the attacker's behavior from the real-time status of network.

Signal Type	Signals	Implication
PAMPs	P1: # of errors per second	Buffer overflow. et al.
	P2: # of vulnerability exploits to OS	Seizing OS Administration
	P3: # of vulnerability exploits to applications	Seizing control of applications
Danger	D1: # of received packets per second (100 packets per unit)	DoS Attack
	D2: # of port connections (10 connections per unit)	Port Scan
Safe	S1: Rate of change of sending packets per second	Steady behavior of performance
	S2: Rate of change of receiving packets per second	
Inflammation	Inf: Simultaneous multi-access	Amplify other signals

Table 1. Input signals mapping

Therefore, considering the above cases, when mapping signals for the defense system, 8 signals from the features captured by Honey DCs are selected as the algorithm inputs, whose definitions and descriptions are given in Table 1. We have

selected 23 sorts of behavioral features at the beginning, however, these 8 featured signals have been verified and proved to be the most significant and efficient factors through multiple experiments. By selecting a variety of signals, the robustness of the DTNPD model could be further enhanced in network environment with random fluctuations.

There are three PAMPs signals. P1 represents the number of system errors per second, since frequent system errors quite probably means the system is under attack such as buffer overflow. P2 and P3, respectively denote that the vulnerabilities of operating system and application software have been triggered, which indicates that the privilege of the OS or ordinary applications will be obtained, and ultimately attackers shall gain control of the entire system.

Two Danger signals are defined. D1 denotes the network traffic rate in unit time, where too many packets pouring in may indicate that the host is suffering from DoS attacks. D2 refers to the frequency of port connections suffered by the system, which may indicate probing conducted by hackers before an attack. Both of them could reveal the potential situation of being attacked.

Two Single Safe signals are also defined. S1 and S2 respectively represent the changes in the number of network packets sent or received. A mild rate of change probably means that the current host is running in a relatively stable state which could be aware of the network situation.

A Single Inflammation signal Inf refers to remote multi-logins by many users, and this behavior may act as a multiplier for other signals.

3.2 Antigens

The fusion process of signals can provide adequate information to indicate whether the network environment is in danger of attack, however, it does not result in any information about the potential attackers. It is the antigen that we need to link the evidence of attacking behavior with the network invader.

Referring again to the process in the immune system where convergence of antigens with identical structures are found in the tissue, to select the proper antigen type in the DTNPD model, multiple items with the same structure should be chosen as the antigens. Sampling of a good many antigens is also key to providing robustness against rogue signal processing of small number of Honey DCs.

In addition to collecting various types of signals, each Honey DC also has to collect the antigens and presents them to the Responder. Learning from the detection of botnet and SYN scan proposed by Yousof and Greensmith [16], the PID generated by the system call each time is selected to be the antigen. In fact, the structure of the PID is not important, as it is just used to identify the process in order to determine whether signal changes have been triggered by potentially malicious processes, which provides evidence for the evaluation later.

3.3 Behavior Analysis

All categories of signals for the DTNPD model have been defined in Section 3.1. In order to calculate the output signals, we utilize a weighted sum equation which can bypass any biologically gene regulatory network or signal transduction mechanism, largely reducing any additional calculation cost.

	PAMPs	Danger	Safe
CSM	2	1	3
Semi-mature	0	0	1
Mature	2	1	−3

Table 2. Weight matrix for behavior analysis

Before illustrating the behavior analysis based on the given weighted sum equation, the weight matrix must first be assigned. According to the interactive influence between PAMPs, Danger and Safe during signal processing, the weight matrix for signals in the DTNPD model is given in Table 2, these weights are derived from the immunological data which are empirically obtained in the lab [17].

The general behavior analysis equation is shown in Equation (1) which is used to calculate the outputs signals. In Equation (1), Pw, Dw and Sw represent the weights of PAMPs, Danger and Safe respectively; Pn, Dn and Sn denote values of the three input signals; I refers to the Inflammation signal. The output signals including CSM, Semi-mature and Mature can be obtained using the summation equation in three times respectively.

$$Output = \left(\sum(P_n * P_w) + \sum(D_n * D_w) + \sum(S_n * S_w)\right) * (1 + I) \tag{1}$$

For example, the calculation of CSM signal is carried out as follows. As we have defined in Section 3.1, there are two PAMPs input signals, namely the number of errors per second and the vulnerability exploits to the OS or an application. If the values captured for these two signals are 4 and 3 respectively, according to the PAMPs weight defined in Table 2 for CSM is 2, thus, $\sum(P_n * P_w) = 4 * 2 + 3 * 2 = 14$; And for the Danger signals defined in Section 3.1, there are two Danger signals, namely the number of packets received (100 packets as one unit) and port connections per second (10 connections as one unit), if the values are 0.8 and 1.3 respectively, according to the Danger weight defined in Table 2 for CSM is 1, thus, $\sum(D_n * D_w) = 0.8 * 1 + 1.3 * 1 = 2.1$; There is only one Safe signal defined in Section 3.1, if the value is 1.2, considering the Safe weight for CSM is 3, thus $\sum(S_n * S_w) = 1.2 * 3 = 3.6$. In the case that the value for I signal is 4, the value of CSM is calculated as follows.

$$\begin{aligned} CSM &= \left(\sum(P_n * P_w) + \sum(D_n * D_w) + \sum(S_n * S_w)\right) * (1 + I) \\ &= (14 + 2.1 + 3.6) * 5 = 98.5 \end{aligned}$$

The calculation processes of Semi-mature and Mature signals are similar to the above based on Equation (1), furthermore, the weights of the two signals have to refer to the second and third rows of Table 2. Utilizing the given weight matrix and weighted sum equation, the captured signals and antigens implicating potential attacking behavior can be analyzed, and the information provided to the Responder in order to determine the endangered degree of Compartment A in the proactive defense system.

4 COMPARTMENT B

The attacking behavior analysis process is a population-based process; Honey DCs do not perform their functions in isolation but as a group in Compartment A. Each of them has to sample antigens and signals, and then multiple Honey DCs present multiple copies of the same antigen type to the Responder. The latter is responsible for adjusting current proactive defense strategies based on the presented information.

$$ODE = \frac{\varepsilon_1}{\varepsilon_1 + \varepsilon_2} \tag{2}$$

Let ε_1 and ε_2 denote the number of Mature signals and Semi-mature signals, and the Overall Degree of Endangerment (ODE) can be calculated using Equation (2), which indicates the "maturity" of the environment where the signals and antigens were captured.

It is worth noting that the term "danger" is sentimental, as it does not necessarily denote a "dangerous" incident. This is because some danger signals may be either positive (providing some useful information), or may be negative (certain attacks are committed).

Once the ODE value is obtained, the Responder immediately examines the current condition of the local networks, and then determine the appropriate defense strategy for the next phase, the basic strategies include:

1. When attackers are trying to probe the proactive defense system, current configurations should be maintained to observe the status of attack; if the attackers are not effectively trapped, enticing techniques should be increased appropriately (too many vulnerabilities will make attackers question the authenticity, whereas too strict protection will make attackers stay away).
2. When an attacker has started to utilize the Honey DC, connections with attacker should be cut off in any situations in which enough information about the hackers has been collected or the Honey DC is about to be used in a malicious way. When necessary, counter-attack measures should be launched.

The multiplicity of Honey DCs deployment is a significant feature of the DTNPD model and is one of the benefits of basing the model on biological immune system concepts, an important result being that a few misclassifications determined by several Honey DCs will not be enough to invoke a false positive error, enhancing the robustness of determinations made by the Responder.

5 SIMULATION

5.1 Experimental Networks

A prototype system of DTNPD was implemented mainly including the Cap module to capture characteristics of network behavior and system calls and Analyzer module to analyze attacking behaviors. To verify the validity of the DTNPD model, more than 100 hosts and servers were used to establish the experimental networks as shown in Figure 5, with reference to the Cisco's security enhanced network design.

The experimental network is divided into five administrative domains including Production A, Production B, Compartment A1, Compartment A2 and Compartment B, where IDS is responsible for monitoring the attack incidents in each administrative domain. This environment is mainly used for analyzing attacking behavior, and to verify the sensing ability of the model.

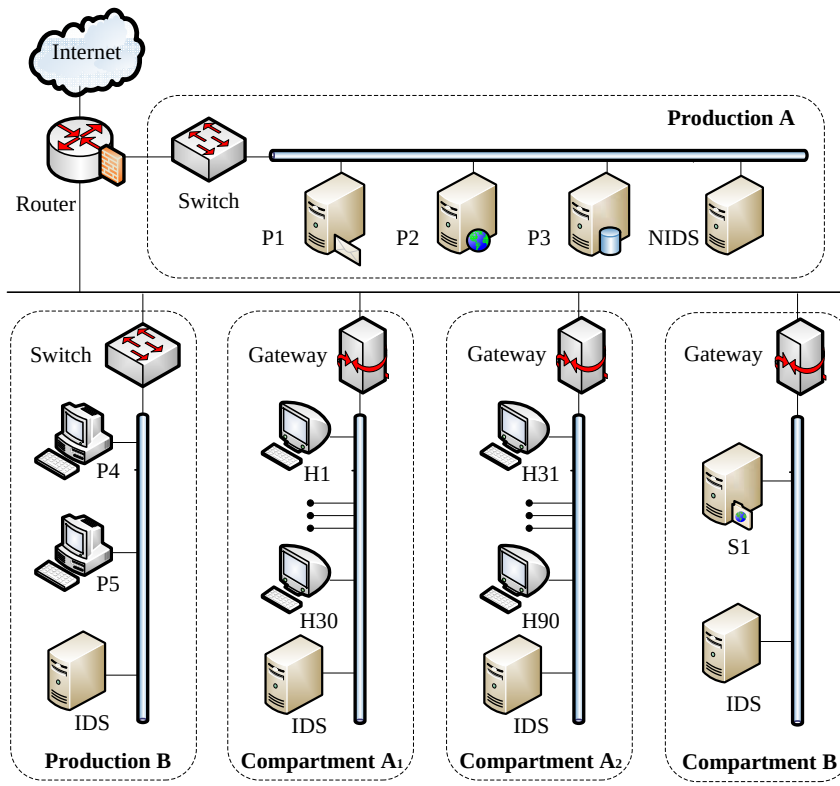


Figure 5. Topology of DTNPD simulation

Production A and B are both normal production networks. The other three administrative domains comprise the DTNPD prototype, camouflaged as the other production networks. There are 30 Honey DC hosts in Compartment A1 and 60 Honey DC hosts in A2 respectively; S1 is the Responder disguised as a Web server, located in Compartment B, which is responsible for adjusting current proactive defense strategies based on the presented antigens and signals.

5.2 Test of DTNPD Sensing Ability

In this section, we mainly test the sensing ability of the DTNPD model. Typically, the attacking process launched by hackers utilizes the information gained from port scanning and packets interception, and then conducts specific attacks against vulnerabilities in the target OS and applications. Therefore, we introduce a three-stage simulation experiment to verify the sensing ability of DTNPD.

In the prototype system, half of the Honey DC hosts in Compartment A1 are well configured with more comprehensive security measures, with no known vulnerabilities remaining; while for the other half, the IE buffer overflow vulnerability – Aurora (CVE-2010-0249) is deliberately kept in the host configuration for the purpose of decoying the attackers to exploit the vulnerability. In addtion, hosts in Compartment A2 are configured the same as A1, that is, half in order and half with flaws.

Stage 1: This stage is used to test the sensing ability of DTNPD to the scan activity. Nmap 5.0 is utilized to scan both Compartment A1 and Compartment A2, over a wide range of scan intensities (we define scan intensity as the number of scans per second), with different migration thresholds, to simulate benign scan activities as well as malicious probing behavior. Figure 6 and Figure 7 show the ODE values under the scanning, respectively for Compartment A1 and Compartment A2. Each curve represents the ODE value fluctuation under different scan intensities within a particular threshold.

We first discuss the relationship between the scan intensity and ODE value. Both Figure 6 and Figure 7 indicate that the ODE values are increasing when the scanning intensity is strengthened. Take the curve of Th=40 in Figure 6 as an example, with the intensity ranges from 20 to 160 times per second, ODE rises from 0.116 to 0.287. This is not surprising since the frequent connections to Honey DC will result in significant Danger signals, consequently, the ODE value will increase.

Then, one can observe both from Figure 6 and 7 that curves with threshold ranging from 80 to 160 are closer to each other, than the curves with threshold 40 and 200. As mentioned above, the migration threshold can be used to control the signal collection cycle, and indirectly influence the generation of Mature signals and Semi-mature signals, as well as, the calculation of the ODE value. Hence, we consider the threshold ranging from 80 to 160 as the optimal configuration for this DTNPD prototype.

From Figure 6, we note that there are several sharp spikes especially within the curves of threshold 40, 200 and 160. For instance, where Th=120, ODE value

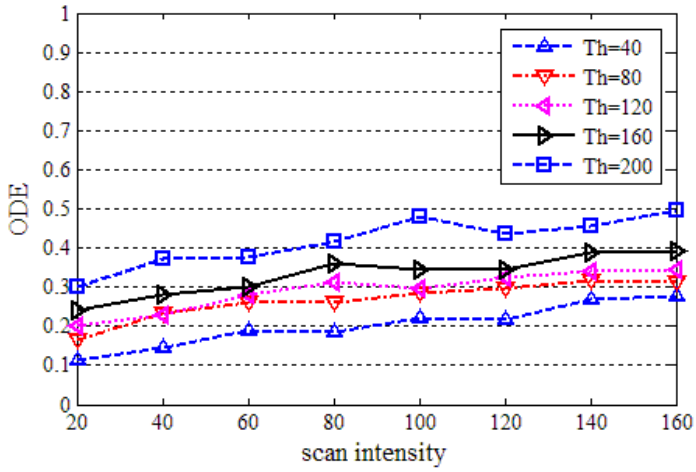


Figure 6. Scanning impact on Compartment A1

is strikingly increased to 0.491 at the intensity of 100, even higher than that of 120 intensity. However, in terms of Figure 7, only tiny spikes are revealed for almost every curve. As the attacking behavior analysis process is a population-based process, the behavior difference in that case can be explained in that there are many more Honey DC hosts in Compartment A2 than the hosts in Compartment A1, where the analysis for presented signals and antigens will yields more steady and correct ODE values.

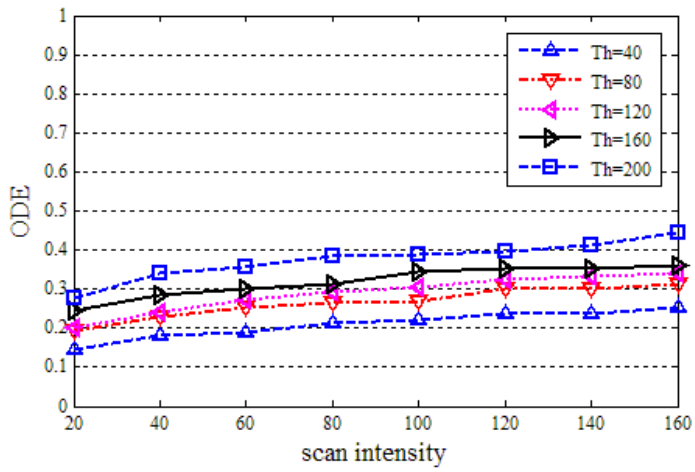


Figure 7. Scanning impact on Compartment A2

Stage 1 concludes that:

1. DTNPD is able to sense the threat of scanning, and ODE value will increase when the scan intensity is strengthened.
2. Threshold ranging from 80 to 160 is the optimal configuration for this DTNPD prototype.
3. Compartment with more Honey DCs possessed more steady and correct sensing ability than that of less Honey DCs.

Stage 2: This stage is used to test the sensing ability of DTNPD to the combo attacks. During this stage, the combo attacks, which combine Nmap scanning and vulnerability exploit, are simulated against both Compartment A1 and Compartment A2. Figure 8 and Figure 9 illustrate the overall degree of endangered values under the combo attacks, respectively for Compartment A1 and Compartment A2. Each curve represents the ODE value fluctuation under different combo attack intensities within a particular threshold.

In Table 3, we use the form of X+Y to define the combo attack intensity, which denotes that the given combo attack comprises X scan repetitions per second and Y exploits attempts to Aurora vulnerability.

Intensity	1	2	3	4	5	6	7	8
Attack	$40+1$	$40+2$	$60+2$	$80+2$	$100+2$	$120+2$	$120+3$	$120+4$

Table 3. Definitions of combo attack intensities

As shown in Figure 8 and 9, some key conclusions emerge from the simulation. ODE values are increasing as the combo attack intensity escalates during the simulation process. As we expected, ODE values are much higher than those in Figure 6 and 7. For instance, in terms of Th=40, the ODE reaches 0.287 under the most violent scan attack, accordingly the ODE gets to 0.702 under the most fierce combo attack. This could be explained by the fact that Aurora vulnerability exploit results in a severe PAMPs signal, which heavily influences the generation of Mature signals, and as a result, the ODE value.

Like the trends in Figure 6 and 7, curves in Figure 8 and 9 with threshold ranging from 80 to 160 are closer to each other, than the other curves. In addition, there are still several sharp spikes within the curves when we perform combo attacks to Compartment A1. However, in the case of Compartment A2, the same combo attack only leads to placid fluctuations. The simulation results acquired from Stage 1 and 2 showed good consistency with real attack intensity, accurately reflecting the danger degree when the system suffered from port scan and vulnerability exploit, which indicates DTNPD model has the ability to sense dangerous behavior in the network.

Stage 2 concludes that:

1. DTNPD could sense the threat of combo attacks, and ODE values will increase when the attack intensity escalates.

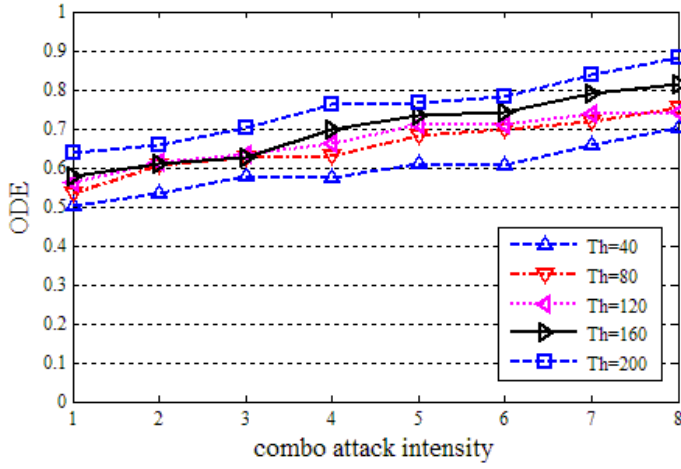


Figure 8. Combo attacks impact on Compartment A1

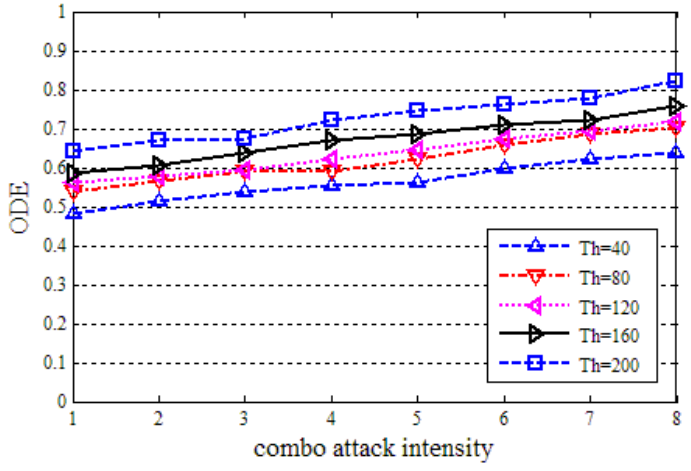


Figure 9. Combo attacks impact on Compartment A2

2. Threshold ranging from 80 to 160 is the optimal configuration.
3. In addtion, compared to Stage 1, ODE values under combo attacks are larger than the former, as the combo attacks are more violent than single scanning.

Stage 3: This stage is used to test the real-time sensing ability of DTNPD. The simulation implemented against Compartment A2 is divided into eight episodes with different time intervals, and in each episode different attack modes are used, with different network traffic rates as well.

The attack modes adopted by the simulation in this stage are given in Table 4, which include Nmap scan, vulnerability exploit and multiple DoS attacks, combined with different attack intensities (the range of traffic rate is 6 K to 24 K packets per second). The result of danger sensing in Compartment A2 is shown in Figure 10.

Episode	Interval (min)	Rate (Packets/s)	Attack
E1	0–5	6 K	Scan with Nmap
E2	5–10	12 K	Scan with Nmap
E3	10–15	12 K	Scan with Nmap; CVE-2010-0249
E4	15–20	24 K	Scan with Nmap; CVE-2010-0249
E5	20–25	6 K	UDP Flood
E6	25–30	12 K	UDP Flood
E7	30–35	12 K	UDP Flood; Smurf; teardrop
E8	35–40	24 K	UDP Flood; Smurf; teardrop

Table 4. Attack modes in different intervals

It can be seen in Figure 10, that after the attack occurred, with the increase of attack intensity, the degree of danger sensed by DTNPD increased synchronously. When the attacking intensity reduced, degree of danger sensed correspondingly reduced. However, the slope of the decline was relatively small especially as the attack intensity firstly began to decline, which indicated that in a real network environment, the proactive defense system could still maintain a high degree of alertness in face of the potential of a recurrence of similar attacks a short time after initial attack.

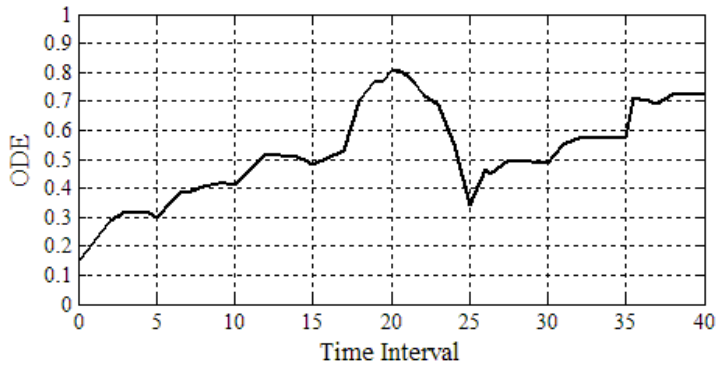


Figure 10. ODE sensed by DTNPD under different attack modes

For example, during interval 20-25, the attack intensity imposed on the network had reduced, but the degree of danger sensed by system declined at a relatively moderate rate, which showed that the system continued to maintain a high vigilance, especially in the initial period following the attack, namely from 20 to 22. From the

moment 25, when a strong attack reoccurred, the degree of danger rose rapidly. Within less than one minute, the ODE had reached 0.483 from 0.347. During interval 30-35, when other attacks were added to the existing UDP Flood DoS with unchanged traffic rate, the degree of danger sensed by the system appeared to be steadily increased, and then ODE remained at the level of 0.579 from time 32 to 35. In the last interval, when the traffic rate was raised markedly, the system could respond quickly to improve the degree of danger from 0.579 to 0.708, which was consistent with the situation in the real network environment. Experimental results showed that the degree of danger sensed by the DTNPD model hold good consistency with the intensity of real-time network attacks, which demonstrated that the model is capable of reflecting actual changes in the current network danger level.

Stage 3 concludes that:

1. DTNPD could correctly sense the threat of multiple attacks in realtime.
2. DTNPD could maintain a high degree of alertness when the network threat is slightly going down, which provides a sound protection to prevent short-time recurrence.

5.3 Verification of DTNPD Validity

For now we have just implemented this prototype system for DTNPD, and probably these input signals selected are not enough to produce totally correct results. Therefore in Section 5.3, we focus on the verification of DTNPD validity, that is, the results of DTNPD will be verified whether they are reasonable conclusions compared with the actual situation.

As we mentioned above, Compartment A is responsible for analyzing and judging the state of HoneyDC to be Mature or Semi-mature, which indicates that the host is endangered or safe. Then, the final ODE value can be directly calculated from the results of Compartment A, which implies that the validity of DTNPD model is strictly determined by Compartment A. Therefore, we verify the results of Compartment A by comparing them with the true states of Honey DCs.

We launched combo attacks composed of port scan, UDP flood and vulnerability exploits to verify the validity of Compartment A. Within the whole process, 125 simulations were performed on the experimental networks from April 14, 2011 to September 25, 2012, in which the scale of honey DCs ranged from 40 to 90, and $\mathrm{Th} = 120$ was chosen as the threshold configuration.

As each Honey DC is continually running and camouflaged as normal production host, they may have distinct performances and probably behave different security states under the same attack. We define four basic metrics as the raw outputs of this experiment, including:

- True Positives (TPs). The number of Honey DCs correctly classified by Compartment A as Mature state in face of attacks.

- True Negatives (TNs). The number of Honey DCs correctly classified by Compartment A as Semi-mature state in face of attacks.
- False Positives (FPs). The number of Honey DCs incorrectly classified by Compartment A as Mature state in face of attacks.
- False Negatives (FNs). The number of Honey DCs incorrectly classified by Compartment A as Semi-mature state in face of attacks.

For each scale of Honey DCs, we performed more than 30 times of simulations, and the average results of TPs, TNs, FPs and FNs are shown in Table 5. Take the last row of Table 5 for example, 90 Honey DCs are selected to form the environmental network on which we performed 32 times of combo attacks. By comparing the result of Compartment A with the actual state of each Honey DC, the average TPs, TNs, FPs and FNs are respectively 81, 4, 2 and 3.

Scale	# of simulations	TPs	TNs	FPs	FNs
40	31	30	2	3	5
60	31	47	3	4	6
80	31	67	2	5	6
90	32	81	4	2	3

Table 5. Basic metrics obtained for different scales of Honey DCs

Then, based on the basic metrics, we are able to define four senior metrics including Precision, Recall, F1 Measure and Accuracy, which can help us to verify the validity of Compartment A from multiple angles.

Precision (P, also called Positive Predictive) indicates the proportion of positive classification results that are true positives, where Precision = TPs/(TPs + FPs).

Recall (R, also called Sensitivity) indicates the ability of Compartment A to identify positive results from the true Mature part, where Recall = TPs/(TPs + FNs).

F1 Measure (also called F-score) is defined as a measure of the Compartment A classifications accuracy, which can be interpreted as a weighted average of the Precision and Recall, where F1 Measure = $2 * P * R/(P + R)$.

Accuracy indicates the proportion of true results in all, as a statistical measure of how well Compartment A correctly identifies an Honey DC as endangered or safe, where Accuracy = (TPs + TNs)/(TPs + TNs + FNs + FPs).

Therefore the senior metrics can be calculated based on the Table 5 records of TPs, TNs, FNs and FPs, the corresponding results are given in Table 6.

Among the four senior metrics, we recognize Accuracy as the most important metric to verify the validity of Compartment A, as well as the DTNPD. As we know, TPs and TNs respectively refers to the amount of correct classifications for Mature and Semi-mature state of Honey DC, so Accuracy directly illustrate the ratio of true classifications to the total, which reflects the effectiveness and performance of Compartment A under the potential network attacks.

Scale	# of simulations	Precision	Recall	F1 measure	Accuracy
40	31	0.909	0.857	0.882	87.5 %
60	31	0.922	0.886	0.903	88.33 %
80	31	0.931	0.917	0.923	91.25 %
90	32	0.976	0.964	0.969	93.33 %

Table 6. Senior metrics derived from different scales of Honey DCs

From Table 6, we can observe that (1) when the scale expands, all metrics including Precision, Recall, F1 Measure and Accuracy will increase. (2) Specifically, the Accuracy ranges from 87.5 % to 93.3 %, which indicates that the Accuracy of Compartment A is quite correlated with the scale of Honey DCs, when the population of Honey DC becomes larger, Accuracy will get higher. (3) In our opinion, Accuracy of 93.3 % with the scale of 90 Honey DCs reaches an acceptable degree of our expectation and these results provide strong evidence that DTNPD is capable of identifying the true state of Honey DCs, which verify the validity of DTNPD.

5.4 Comparisons

In this section, DTNPD model will be compared with previous proactive defense approaches. Unfortunately, all of the previous works used private dataset and these datasets are not available for objective reasons. In this situation, we decided to implement these approaches based on our dataset, and Table 7 summarizes important features of these different solutions.

Scheme	Measures	Implement complexity	event types	events	Computing complexity	Accuracy	Real-time
NSA	4	High	18	203	Low	78.86 %	Yes
HTP	2	Medium	3	46–78	Low	76.05 %	No
SHP	1	Medium	4	> 11	High	84.67 %	No
DTNPD	1	Medium	4	8	Low	93.33 %	Yes

Table 7. Comparison of different approaches for network proactive defense

The method presented by Barford et al. [9] for Network Situational Awareness (NSA) which employs 4 methodologies like the MannKendall trend test and χ^2 test to analyze the botnet events, 203 malicious scan events are assorted into 18 types. Although the computational complexity of every algorithm is linear, the staggered implementation cost is obviously higher than the other approaches. Using our dataset, the prototype system detects the scanning events which last for 12 minutes to 4 days, and the average detection accuracy achieves 78.86 %, which is a bit lower than 81.32 % given by the authors.

In the Honeypot trace forensics (HTF) [10] scheme, only 2 distinct observation viewpoints respectively from country and platform are taken as two main methodologies in order to group the attack traces to identify the botnet. Distributed Leurr.com

system is used to collect botnet events whose amount ranges from 46 to 78, divided into 3 types. Though simple statistical method leads to a quite low computational complexity, within our dataset, we observed that 23 days were needed to figure out the zombie army which meant it could not be used in a real-time application.

The Social Honeypot Project (SHP) [11] is a framework deployed for harvesting deceptive spam profiles in which spam classifiers are created to filter out the spammers. More than 11 spam events divided into 4 types including user demographics, user-contributed content, user activity features and user connections are considered to perform the classification. During our experiment, the process took almost 1 month to distinguish between legitimate users and spammers. Although the accuracy rate of 84.67 % was the highest amongst these three schemes, SHP is not well suited to real-time network defense.

For our prototype system of DTNPD model, the Cap and Analyzer modules were installed in every Honey DC, and all the results of behavior analysis based on danger theory were presented to the Responder. The major advantages include:

1. Only 8 typical events are selected and classified into 4 types of signals as the inputs of DCA, and the complexity of DCA is linear.
2. Moreover, based on the 125 simulations that were run, we obtained the Accuracy rate up to 93.33 %, which is higher than the other previous methods in spite of the slightly different threatening objects, and gives quite a good account of the DTNPD model.
3. Last but not least, our model holds good consistency with real-time attack intensity.

Simulations from Stage 3 of Section 5.2 indicated that attacking attempts can be sensed and evaluated with minutes as the unit of measurement which satisfies the demands of practical proactive network defense.

6 CONCLUSION

In this paper, a danger theory based network proactive defense (DTNPD) model is presented. On the basis of current Honeynet technology, this model is constructed borrowing the idea of danger theory which stands for a novel response pattern of the immune system. Considering the merits of DCA including strong information fusion capabilities and reasonable practicability, the algorithm is improved and redesigned for the proactive network defense.

According to the architecture of the DTNPD model, we first describe Compartment A including the definitions of signals and antigens in the network environment, as well as the behavior analysis algorithm of single Honey DC. Then Compartment B is illustrated to perform the calculation of ODE value which indicates the endangered degree of network environment, to prepare for further defense strategy control. The simulation demonstrated that the DTNPD model could correctly determine the

degree of danger from malicious attacks in the network environment, and the quantitative danger assessment in real-time could provide direct technical references for the strategy adjustment in proactive defense system. In the future, we will conduct more simulations with more Honey DCs and novel network threats, and explore a better way to determine the threshold under distinct network environments.

REFERENCES

[1] Chen, R. M.—Hsieh, K. T.: Effective Allied Network Security System Based on Designed Scheme with Conditional Legitimate Probability Against Distributed Network Attacks and Intrusions. International Journal of Communication Systems, Vol. 25, 2012, No. 5, pp. 672–688.

[2] Guo, Y.—Wang, Z.—Luo, S.—Wang, Y.: A Cascading Failure Model for Interdomain Routing System. International Journal of Communication Systems, Vol. 25, 2012, No. 8, pp. 1068–1076.

[3] Nguyen, H.—Choi, Y.: Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework. International Journal of Electrical, Computer and Systems Engineering, Vol. 4, 2010, No. 4, pp. 247–252.

[4] Valentín, K.—Malý, M.: Network Firewall Using Artificial Neural Networks. Computing and Informatics, Vol. 32, 2013, No. 6, pp. 1312–1327.

[5] Chou, J.—Lin, B.—Sen, S.—Spatscheck, O.: Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks. IEEE/ACM Transactions on Networking, Vol. 17, 2009, No. 6, pp. 1711–1723.

[6] Xie, B.—Yu, S.: Application Layer Real-Time Proactive Defense System Based on Application Layer Protocol Analysis. Chinese Journal of Computers, Vol. 34, 2011, No. 3, pp. 452–463.

[7] Marchese, M.—Surlinelli, R.—Zappatore, S.: Monitoring Unauthorized Internet Accesses Through a 'Honeypot' System. International Journal of Communication Systems, Vol. 24, 2011, No. 1, pp. 75–93.

[8] Lin, W.—Wang, H.—Liu, J.—Deng, L.—Li, A.—Wu, Q.—Jia, Y.: Research on Active Defense Technology in Network Security Based on Non-Cooperative Dynamic Game Theory. Journal of Computer Research and Development, Vol. 48, 2011, No. 2, pp. 306–316.

[9] Barford, P.—Chen, Y.—Goyal, A.—Li, Z.—Paxson, V.—Yegneswaran, V.: Employing Honeynets For Network Situational Awareness. In: Sushil, J., Peng, L., Vipin, S., Cliff, W. (Eds.): Cyber Situational Awareness, Proceedings of International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO '10), Guimaraes, April 2010, pp. 71–102.

[10] Pham, V. H.—Dacier, M.: Honeypot Trace Forensics: The Observation Viewpoint Matters. Future Generation Computer Systems, Vol. 27, 2011, No. 5, pp. 539–546.

[11] Lee, K.—Caverlee, J.—Webb, S.: The Social Honeypot Project: Protecting Online Communities from Spammers. Proceedings of the 19th International Conference on World Wide Web (WWW '10), Raleigh NC, April 2010, pp. 1139–1140.

[12] Matzinger, P.: The Danger Model: A Renewed Sense of Self. Science, Vol. 296, 2002, No. 12, pp. 301–305.

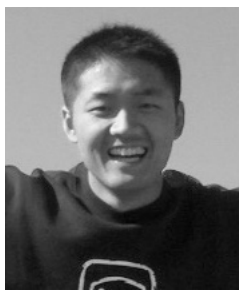
[13] Greensmith, J.—Aickelin, U.—Cayzer, S.: Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection. In: Jacob, C., Pilat, M. L., Bentley, P. J., Timmis, J. I. (Eds.): Proceedings of 4th International Conference on Artificial Immune Systems (ICARIS 2005), Alberta, Canada, August 2005, pp. 153–167.

[14] Hongwei, M.—Xingquan, Z.: Artificial Immune System. Beijing. Science Press, 2009, pp. 29–33.

[15] Greensmith, J.: The Dendritic Cell Algorithm. Ph.D. Thesis. University of Nottingham, Nottingham, UK, 2007.

[16] Greensmith, J.—Aickelin, U.: Dendritic Cells for SYN Scan Detection. Proceedings of the 9th Annual Conference on Genetic and Evolutionary Computation (GECCO '07), London, England, August 2007, pp. 49–56.

[17] Williams, C. A.—Harry, R. A.—Mcleod, J. D.: Apoptotic Cells Induce Dendritic Cell-Mediated Suppression via Interferon-Y-Induced IDO. Immunology, Vol. 124, 2008, No. 1, pp. 89–101.



Yu Wang received the B.Sc. and M.Sc. degrees in computer science and technology from National Digital Switching System Engineering and Technological Research Center (NDSC), Zhengzhou, China, in 2006 and 2009, respectively. Currently he is a doctoral candidate. His current research interests include inter-domain routing system security and network proactive defense, as well as trust computing. He has experience in designing and implementing of database systems and embedded systems.

Zhenxing Wang is Professor of Network Engineering at National Digital Switching System Engineering and Technological Research Center (NDSC), Zhengzhou, China. He received his M.Sc. degree from Xi'an Jiaotong University, Xi'an, China and Ph.D. degree from Nanjing University of Science and Technology, Nanjing, China. His current research interests include network security, traffic analysis, as well as the Next Generation Internet. He has published more than 80 papers and served as a member of editorial boards of several journals.

Liancheng Zhang received his M.Sc. and Ph.D. degree both from National Digital Switching System Engineering and Technological Research Center (NDSC) in 2007 and 2011, respectively. Now he is a lecturer of NDSC. His main research interests include internet routing, traffic camouflage, and network proactive defense.

Yazhou Kong received his B.Sc. degree from National Digital Switching System Engineering and Technological Research Center (NDSC) in 2011. Now he is a graduate of NDSC. His main research interests include network security and traffic analysis.