WPMSD: A Malicious Script Detection Method Inspired by the Process of Immunoglobulin Secretion

Zhao hui, Chen wen, Zeng Jie, Shi Yuanquan, Qin Jian
College of computer science, Sichuan University
Chengdu, 610065, China
E-mail: zhaohui@scu.edu.cn

Abstract

Inspired by the process of immunoglobulin secretion in biological body, we present a Web Page Malicious Script Detection Method (WPMSD). In this paper, Firstly, the basic definitions of artificial immune items are given. Secondly, according to the spreading range of malicious script, the immunoglobulin number is changed as the detector clone proliferation is stimulated by malicious scripts. Further more, the nonlinear dynamics of antibody number is discussed. Thirdly, we propose a probability approach to trigger alarms to inform that the detected scripts are harmful. Finally, the WPMSD collects the effective immunoglobulin set based on Hidden Markov Model (HMM) to update the detector gene library. Compared with the traditional immune based detection methods, such as Negative Selection Algorithm (NSA), Dynamic Colonel Selection (DynamiCS), and Variable size Detector (V-detector), the false alarm rate of WPMSD has been reduced by 18.09%, 12.6%, and 7.47% respectively.

Keywords: malicious script detection; false alarm rate; immunoglobulin secretion; artificial immune system.

1. Introduction

In order to promote the interaction between clients and web pages, many types of scripts have been embedded into the web pages. However, many malicious scripts may hide in the web page, which often lead to serious intrusion to the target computers by some web page connections from attackers. Hence, the detection of the hidden malicious scripts in the web pages is critical for the network security.1,14,15,16.

The problems in Biological Immune System (BIS) are similar to the ones in the web page malicious script detection method. In 1994, Forrest et al. 2 proposed Negative Selection Algorithm (NSA) that simulates the new immune cell tolerance process in BIS to avoid mismatching any normal script patterns. In 2002, Kim3 presented Dynamic Colonel Selection (DynamiCS) algorithm in which the malicious scripts can be defined as the changed elements to reduce false detection. In 2009, Zhou Ji et al.4 proposed an algorithm of Variable size Detector (V-detector) that can modify the detection radius of detector according to the changed context of web page scripts.

In order to exactly catch harmful foreign antigens, the immune cells have to go through two stages of immune response: the primary immune response and the secondary immune response.5,17 In the primary immune response stage, once the affinity that an immune cell’s matching antigen comes up to a certain threshold, the immune cell will be activated. In the secondary immune response, with the continuous expansion of antigen invasion, the immune cell clones itself and secretes much immunoglobulin to catch more antigens, which results in a fast increasing of the...
immunoglobulin density. After antigens have been eliminated, the immune cell clone proliferation is suppressed and the immunoglobulin density decreased simultaneously. From then on, the biological body restores into a normal health status.

Inspired by the process of immunoglobulin secretion in BIS, we present a Web Page Malicious Script Detection Method (WPMSD) to reduce the high false alarm rate in traditional web page malicious script detection methods based on immune system.

2. Method Description

The WPMSD is composed of two important parts, the initial component and the immune response component. The initial component is responsible for the detector initialization, such as the new detector generation and the negative selection of new detectors. The task of immune response component is performing the detector execution procedure, such as the detector memorization and the detector clone proliferation. The architecture of WPMSD is shown in Fig. 1.

2.1. Basic Definition

Definition 1. Antigens (Ag) are defined as the web page script patterns.

The web page script patterns represent the n-dimensional vector of script activity features that are gain from web pages. The antigen feature calculation is shown in Fig. 2. Hence, antigen is given by Eq. (1).

\[
\text{Ag} = \{a | a \subset f, f = \{f_1, f_2, \cdots, f_n\}, f_n \in [0,1], f > 0\}.
\]

Fig. 1. The architecture of WPMSD

Fig. 2. The antigen feature calculation

Where f represents the n-dimensional vector of script activity features. The structure of immunoglobulin is the same as the antigen.

Definition 2. Self Antigens (Self) are defined as the normal web page script patterns. It is given by Eq. (2).

\[
\text{Self} = \{<s, rd > | s \subset f, rs \in R\},
\]

(2)

Where f represents the n-dimensional vector of normal script activity features, rs is the self radius, R is the set of real numbers.

Definition 3. Nonself Antigens (Nonself) are defined as the malicious web page script patterns. It is given by Eq. (3).

\[
\text{Nonself} = \{ns | ns \subset f\},
\]

(3)

Where f represents the n-dimensional vector of malicious script activity features. And we have:

\[
\text{Self} \cup \text{Nonself} = \text{Ag},
\]

(4)

\[
\text{Self} \cap \text{Nonself} = \emptyset.
\]

(5)

Definition 4. Detectors (De) simulate immune cells in BIS for detecting the web page malicious scripts. It is given by Eq. (6).

\[
\text{De} = \{ab, rd, aff, den, cos, count, age > | ab \in f, \ (rd, aff, den, cos) \in R, (count, age) \in N\},
\]

(6)

where ab represents the n-dimensional vector of scripts activity features, rd is the detection radius of detector, aff is the affinity of detector, den is the density of detector, cos is the costimulation of detector, count is the matched number of a type of scripts activity, age is the age of detector, R is the set of real number, N is the set of natural number. The calculation of detection radius of detector is according to Eq. (7).

\[
xrd = \min \{x_{ab} - y_{rs} | y > rd\}.
\]

(7)
Where $x \in \text{De}$, $y \in \text{Self}$ and $\| \|$ represents the Euclidean Distance. The calculation of affinity of detector is according to Eq. (8).

$$x_{\text{aff}} = 1/[1+\exp(1-x_{\text{rd}})]$$  \hspace{1cm} (8)

The affinity of detector reflects the performance of individual in the detector set. The greater detection radius a detector has, the higher affinity of this detector would have. The density of detector is based on the theory of immune networks\textsuperscript{7}, which is built on the principle that antibodies can match others as well as antigens. The calculation of density of detector is according to Eq. (9).

$$x_{\text{den}} = \sum_{y \in \text{De}} f_{\text{similar}}(x,y)/|\text{De}|.$$  \hspace{1cm} (9)

Where $x \in \text{De}$, the $\sum_{y \in \text{De}} f_{\text{similar}}(x,y)$ represents the similarity between detector $x$ and detector $y$, the calculation of this similarity is according to Eq. (10).

$$f_{\text{similar}}(x,y) = \begin{cases} 1, & \|x.ab - y.ab\| \leq \alpha \\ 0, & \text{otherwise} \end{cases}$$  \hspace{1cm} (10)

Where $\alpha (0 \leq \alpha \leq 1)$ is the similarity threshold. The calculation of costimulation of detector is according to Eq. (11).

$$x_{\text{cos}} = x_{\text{aff}}/\exp(x_{\text{den}}).$$  \hspace{1cm} (11)

A detector with higher affinity and lower density will gain more co-stimulation from the system.

### 2.2. Initial Component

- **New Detector Generation**
  A new detector is generated from the detector gene library. The library contains a lot of useful detector gene sequences for detecting the malicious web page scripts and these detector gene sequences can be used to generate new detectors.

- **Negative Selection**
  In order to avoid matching any normal web page script, the new generated detector must go through the process of negative selection, as is shown in Eq. (12).

$$f_{\text{mature}}(x) = \begin{cases} 1, & x_{\text{age}} > \omega \land \|x.ab - y.s\| > x_{\text{rd}} \\ 0, & \text{otherwise} \end{cases}$$  \hspace{1cm} (12)

Where $x \in \text{De}$, $y \in \text{Self}$ and $\omega$ is the period of self tolerance. If the result of Eq. (12) equals to 1, then the negative selection of the detector is successful.

### 2.3. Immune Response Component

The task of immune response component is to perform the detector execution procedure, including detector activation, the detector memorization, and the detector clone proliferation.

- **Detector Activation**
  The detector activation simulates the primary immune response in BIS. When the matched number of script activity is greater than match threshold, which means the detector has found an anomaly and it will be activated. The process of detector activation is shown in Eq. (13).

$$f_{\text{act}}(x) = \begin{cases} 1, & x_{\text{age}} \leq \xi \land x_{\text{count}} \geq \phi \\ 0, & \text{otherwise} \end{cases}$$  \hspace{1cm} (13)

Where $x \in \text{De}$, $\phi$ is the threshold of detector activation, $\xi$ is the period of detector activation. If the result of Eq. (13) equals to 1, then the activation of the detector is successful. After that, this mature detector get activated.

- **Detector Memorization**
  After detector activation, the activated detectors should be checked by the detector control center. When the costimulation signal from control center is greater than memory threshold, this activated mature detector will evolve into a memory detector. The process of detector memorization is shown in Eq. (14).

$$f_{\text{mem}}(x) = \begin{cases} 1, & x_{\text{age}} \leq \theta \land x_{\text{cos}} \geq \psi \\ 0, & \text{otherwise} \end{cases}$$  \hspace{1cm} (14)

Where $x \in \text{De}$, $\psi$ is the threshold of detector memorization, $\theta$ is the period of detector memorization. If the result of Eq. (14) equals to 1, then the memorization of the detector is successful.

- **Detector Clone Proliferation**
  The detector clone proliferation simulates the secondary immune response in BIS: when the similar or same antigens attack the biological body again, the memory detector can be activated in short time, meanwhile, this activated memory detector starts cloning itself and secretes much immunoglobulin to catch more antigens\textsuperscript{8}.

Published by Atlantis Press

Copyright: the authors

790
2.3.1. Immunoglobulin Number Accumulation

In this paper, we propose the nonlinear dynamic system Eq. (15), to model the accumulation process of antibody:

\[
\begin{align*}
\frac{dD_e}{dt} &= S_{\text{clone}} R_{\text{mem}} D_e + S_{\text{new}}, \\
\frac{dS}{dt} &= -S_{\text{mem}} S_i + S_{\text{max-secret}} S_{\text{new}} R_{\text{mem}}, \\
\frac{dn_{\text{num}}}{dt} &= -S_{\text{den}} n_{\text{num}} + D_e S_i.
\end{align*}
\]

(15)

Where \(D_e\) is the \(i^{th}\) detector subset of a system, \(S_{\text{new}}\) is the rate of generation new \(D_e\) detector in system, \(S_{\text{clone}}\) is the clone rate of memory detectors, \(R_{\text{mem}}\) is the memorization ratio of \(D_e\), \(S_i\) is the rate of antibody secretion, \(S_{\text{max-secret}}\) is the maximum rate of antibody secretion, \(S_{\text{mem}}\) determines the rate of memorization, \(n_{\text{num}}\) is the accumulation of antibody number in detector subset \(D_e\), \(S_{\text{den}}\) is the detector density of detector subset \(D_e\).

The Equilibrium Value of nonlinear dynamic system (15) is shown in Eq. (16).

\[
\begin{align*}
(D^*_e, S^*_i, n_{\text{num}}^*) &= \left(\frac{\frac{S_{\text{mem}}}{S_{\text{clone}} R_{\text{mem}}} S_{\text{max-secret}} R_{\text{mem}}}{\frac{S_{\text{mem}}}{S_{\text{clone}} R_{\text{mem}}}}, \frac{\frac{S_{\text{mem}}}{S_{\text{clone}} R_{\text{mem}}} S_{\text{max-secret}} R_{\text{mem}}}{\frac{S_{\text{mem}}}{S_{\text{clone}} S_{\text{den}}}}, \frac{S_{\text{clone}} R_{\text{mem}} S_{\text{new}}}{\frac{S_{\text{clone}} R_{\text{mem}} S_{\text{new}}}{S_{\text{mem}}} e^{S_i S_{\text{max-secret}}}} \right).
\end{align*}
\]

(16)

From the result of Equilibrium Value of this nonlinear dynamic system, we can know that the antibody is keeping the emancipation status. However, both of the scale of detector and the number of antibody are apparently representing the tendency of decrement at the same time.

Therefore, we get the Jacobian Matrix \(9\) of nonlinear dynamic system. Eq. (15) is shown as following:

\[
\begin{align*}
L(D_e, S_i, n_{\text{num}}) &= D_e^2 + S_i^2 + n_{\text{num}}^2.
\end{align*}
\]

(18)

Hence,
According to Ref. 6, the arguments in Eq. (24), including \( S_{\text{clone}} \), \( S_{\text{mem}} \), \( S_{\text{abr}} \), and \( \text{deni} \) are shown in Eq. (25)-(28), where \( S_{\text{al}} \) is the intensity of script attacks and \( |M_{\text{al}}| \) is the number of mature detectors:

\[
S_{\text{clone}} \approx e^{-\frac{S_{\text{al}}(S_{\text{al}}+1)|M_{\text{mem}}|}{2|M_{\text{al}}|}} S_{\text{al}}. \quad (25)
\]

\[
S_{\text{mem}} \approx \left[ 1 - e^{-\frac{|M_{\text{al}}|}{n^2} (1-p_{\text{al}})} \right] S_{\text{al}}. \quad (26)
\]

The effect of \( S_{\text{al}} \) on \( S_{\text{clone}, \text{mem}} \) are shown in Fig 3 and Fig 4, respectively. From Fig 3 we can see that as the increase of \( |M_{\text{clone}}|/|M_{\text{al}}| \), the clone rate of memory detectors \( S_{\text{clone}} \) is decreasing, meanwhile the higher the intensity of network attack is, the higher the value of \( S_{\text{clone}} \) is, which means the clone rate of memory detectors can reflects the attacking situation.

From Fig 4 we knowns that the attacking intensity \( S_{\text{al}} \) can linearly increase with the memorization rate of detectors \( S_{\text{mem}} \) when the number of mature detectors \( |M_{\text{al}}| \) is less than 300. \( S_{\text{mem}} \) could also reflects the attacking situation of malicious script. The analyzed result is in consistent with Ref.6.

The arguments of Eq. (24) are replaced by Eq. (25), (26), (27), and Ref.6 shows that when \( t=1, S_{\text{clone}}, S_{\text{al}} = 1:3 \), therefore, the number of antibody in every time point is calculated as Eq. (29).

\[
\text{num} = \frac{S_{\text{max, secrete}} e^{\frac{1}{3} S_{\text{al}} R_{\text{new}}}}{9 S_{\text{al}}^2 R_{\text{new}} + \frac{1}{3n} \ln \left( \frac{1 + \frac{n}{e} - \left[ 1 - e^{-\frac{|M_{\text{al}}|}{n^2} (1-p_{\text{al}})} \right] S_{\text{al}}^2 \text{den}_i }{S_{\text{al}}^2 \text{R}_{\text{mem}}} \right)} - \frac{\ln \left( \frac{1 + \frac{n}{e} - \left[ 1 - e^{-\frac{|M_{\text{al}}|}{n^2} (1-p_{\text{al}})} \right] S_{\text{al}}^2 \text{den}_i }{S_{\text{al}}^2 \text{R}_{\text{new}}} \right)}{A + B \cdot R_{\text{new}} - \frac{S_{\text{max, secrete}} S_{\text{new}}}{B}}. \quad (29)
\]

Where

\[
A = S_{\text{al}} R_{\text{mem}} \left[ \frac{1}{3} S_{\text{al}} R_{\text{mem}} - \left( 1 - e^{-\frac{|M_{\text{al}}|}{n^2} (1-p_{\text{al}})} \right) S_{\text{al}} \right] \) and \n\]

\[
B = \ln \left( \frac{1 + \frac{n}{e} - \left[ 1 - e^{-\frac{|M_{\text{al}}|}{n^2} (1-p_{\text{al}})} \right] S_{\text{al}}^2 \text{den}_i }{S_{\text{al}}^2 \text{R}_{\text{new}}} \right) \]
Hence, we simplify Eq. (29) and get the calculation of the number of antibody as follow:

\[ \text{num}_t \rightarrow \omega \times e^{\frac{k_t}{2}}, \quad \text{where} \quad \omega \in (0.0, 1.0). \]  

(30)

From Eq. (30), we know that the number of antibody can keep the 0.0 to 1.0 times relationship with the intensity of network attacks.

2.3.2. Immunoglobulin Number Decrement

The immunoglobulin number synchronously reduces with the suppressed process of detector clone proliferation. The process of immunoglobulin number decrement is shown in Eq. (31).

\[ \text{num}(\text{age}) = \left(1 - \frac{\lambda}{\text{age}}\right) \times \text{num}(\text{age} - 1). \]  

(31)

Where \( \lambda \) is the immunoglobulin number maintain period, \( \text{age} \) is the age of detector.

**Theorem 1.** Suppose immunoglobulin number is \( \text{num}(i) \) in period \( i \), and since then, the detector fails to match any anomaly, \( \text{num}(i) \) will decrease to zero gradually.

**Proof.** As the detectors failed to match any anomaly, there will be no detector activation and proliferation. According to Eq. (16), the immunoglobulin number is decreased as Eq. (31) shows, when detector age equals to \( \lambda \) the immunoglobulin number will be zero. \( \Box \)

From Fig. 5 we can see that as the increase of detector age, the immunoglobulin number decreases simultaneously. Further more, we find that greater \( \lambda \) could result in longer period for the depression of immunoglobulin number. So we can set large value of \( \lambda \) to maintain enough number of immunoglobulin when there are high-frequency script attacking.

2.4. Web Page Malicious Script Alarm Production

At time \( t \), the probability of malicious script alarm production is shown in Eq. (32).

\[ P_{\text{alarm}}(t) = \min \{1 : \eta \times \text{con}(t) \times \text{allcount}(t)\}. \]  

(32)

Where \( \eta \) is the adjusted argument for malicious script alarm production, \( \text{con}(t) \) is the immunoglobulin concentration at time \( t \), \( \text{allcount}(t) \) is the spreading range of all web page malicious scripts at time \( t \). The function of \( \text{con}(t) \) is given by Eq. (33).

\[ \text{con}(t) = 1 - \frac{1}{1 + \ln \left(\sum_{i=1}^{n} u_i \times \text{exp}(t_i)\right)} . \]  

(33)

where \( \mu \) is the adjusted argument, \( u_i \) is the weight of the \( i \)th web page importance, \( q_i \) is the weight of the \( i \)th type of malicious script destruction. The function of \( \text{con}(t) \) is given by Eq. (34).

\[ \text{allcount}(t) = \sum_{j=1}^{n} u_j \sum_{x \in D_j} x \times \text{count}(t). \]  

(34)

2.5. Detector Gene Library Update

According to Hidden Markov Model (HMM) \(^1\), we calculate the effective immunoglobulin set and update this immunoglobulin set into the detector gene library. The calculation of the effective immunoglobulin set is shown in Eq. (35).

\[ P(G | A) = \frac{P(A | G)P(G)}{P(A)}. \]  

(35)

Where \( A = A_1, A_2, \ldots, A_n \) is a malicious script alarm sequence that is composed of the \( n \) time points. At time \( t \), \( A = A_1, A_2, \ldots, A_n \). \( G = G, G, \ldots, G \) present a set of effective detector gene sequence which calculated the maximum result by the Eq. (36).

\[ G = \arg \max_G \left[P(A | G)P(G)\right]. \]  

\[ = \arg \max_G \left[P(A_1, A_2, \ldots, A_n | G_1, G_2, \ldots, G_n)P(G_1, G_2, \ldots, G_n)\right] \]  

\[ = \arg \max_G \left[\prod_{i=1}^{m} P(A_i | G_i)P(G_i | G_{i-1})\right]. \]  

(36)

Considering the entire detector gene sequences are independent from each other. Hence:

Fig. 5. The effect of \( \lambda \) on \( \text{num}(0)=100 \).
\[ G' \approx \arg \max_{G} \left[ \prod_{i=1}^{n} P(A_1, A_2, \cdots, A_m | G) \right]. \quad (37) \]

### 3. Experiment

In order to test the performance of WPMSD, we use web page malicious scripts to test our model and compare it with the traditional immune based detection methods, including NSA\(^2\), DynamiCS\(^3\), V-detector\(^4\). There are three web pages for the performance test, which could be downloaded from Ref. 13.

Firstly, we set weights of the web pages: 0.6, 0.1, and 0.3 for Web Page1, Web Page2 and Web Page3 respectively. Meanwhile, we set weights of the malicious script destructions: 0.6, 0.2 and 0.1 for Applet, malicious JavaScript, and malicious VBScript respectively. Then we utilize the malicious Applet, malicious JavaScript, and malicious VBScript to attack the web pages. The experiment results are shown in Fig. 6 – Fig. 8.

From the above experimental results, we know that as the web page malicious script spreading range increases, the corresponding immunoglobulin concentration increases synchronously. Meanwhile, when the web page malicious script spreading range decreases, the corresponding immunoglobulin concentration also decreases synchronously. According to Eq. (32), we set the alarm threshold to be 0.5 and the probability of malicious script alarm production is shown in Fig. 9 to Fig. 11. From these figures we can see that higher threshold could greatly reduce the false alarm rate, while increase the rate of fail report. So the alarm threshold is an important adjustment for the detection performance.
Zhao hui, Chen wen

To compare the performance of WPMSD with NSA\textsuperscript{2}, DynamiCS\textsuperscript{3}, and V-Detector\textsuperscript{4}, the comparative experiment was also conducted on the same data set. According to Ref. 4, 11, 12 the parameters setting are shown in table 1.

The detection result is shown in table 2. As table 2, we can see that the detection performance of V-detector is better than NSA and DynamiCS, because V-detector sets the detection radius according to the changed context of web page script, which avoids the Boundary dilemma problems\textsuperscript{3} and improves the detection rate. However, the false alarm rate of WPMSD is lower than V-detector while the detection rate of WPMSD is comparable to V-detector, further more the standard deviation of WPMSD is far less than other methods, which means its performance is more stable.

### Table 1. The parameters set.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm threshold</td>
<td>0.7</td>
<td>The alarm threshold of WPMSD</td>
</tr>
<tr>
<td>$l$</td>
<td>49</td>
<td>The length of antigen and detectors in NSA</td>
</tr>
<tr>
<td>$R$</td>
<td>25</td>
<td>The match threshold of r-continu method in NSA</td>
</tr>
<tr>
<td>significant level</td>
<td>95%</td>
<td>The maximum probability to accept Type I Error of V-detector</td>
</tr>
<tr>
<td>Self radius</td>
<td>0.05</td>
<td>The variation range of self antigen</td>
</tr>
</tbody>
</table>

### Table 2. The result of comparative experiment

<table>
<thead>
<tr>
<th>Method</th>
<th>Detection Rate</th>
<th>False Alarm Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPMSD</td>
<td>95.27% ± 1.16%</td>
<td>3.06% ± 2.5%</td>
</tr>
<tr>
<td>NSA</td>
<td>72.63% ± 6.52%</td>
<td>21.15% ± 7.6%</td>
</tr>
<tr>
<td>DynamiCS</td>
<td>89.29% ± 3.91%</td>
<td>15.66% ± 5.49%</td>
</tr>
<tr>
<td>V-detector</td>
<td>97.51% ± 1.77%</td>
<td>10.53% ± 2.63%</td>
</tr>
</tbody>
</table>

4. Conclusion
This paper proposed a Web Page Malicious Script Detection Method inspired by the process of immunoglobulin secretion (WPMSD) to reduce the high false alarm rate in immune-based web page malicious script detection methods. We proved the relationships between antibody number and the script attacking intensity. The nonlinear dynamics of antibody number is discussed and the calculation method of antibody number is given. Compared with traditional immune-based web page malicious script detection methods, such as Negative Selection Algorithm (NSA), Dynamic Colonel Selection (DynamiCS), and Variable size Detector (V-detector), the false alarm rate of WPMSD has been reduced dramatically, while the high detection rate is maintained.

Acknowledgements
This work is sponsored by National Natural Science Foundation of China (No. 60873246) and the National Research Foundation for Doctoral Program of Higher Education of China (No. 20070610032)

References


18. Lingxi Peng, Tao Li, Xiaojie Liu, Caiming Liu, Jinquan Zeng, Jian Zhang. An Artificial Immune Network Based Algorithm for Diabetes Diagnosis, Protein and Peptide Letters