A Survivability Framework for the NGMN : Inspirations from the Human Immune System

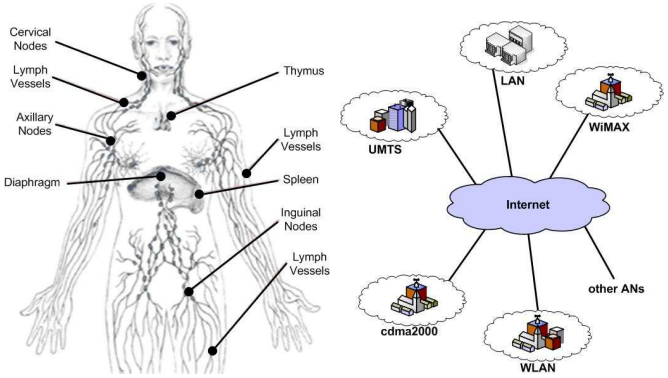
Fazirulhisyam Hashim, Kumudu S. Munasinghe and Abbas Jamalipour
The University of Sydney, NSW 2006, Australia
Email: {fhisyam,kumudu,abbas}@ee.usyd.edu.au

***Abstract*—Motivated by the phenomenal capabilities of the Human Immune System (HIS) in defending the human body against dangerous foreign agents, this paper proposes an HIS-inspired survivability framework to address security threats in Next Generation Mobile Networks (NGMN). In particular, the proposed framework incorporates two key components: namely, the attack detection framework and the security control framework. While the former is used for identifying malicious attacks on the network, the latter offers a competent technique for isolating and recovering from such attacks. Performance evaluation indicates that the proposed survivability framework is efficient in detecting attacks and quarantining the under attacked network segments, thereby increasing the survivability of the NGMN.**

I. Introduction

The Next Generation Mobile Networks (NGMN) [1] has emerged as a promising platform to offer inter-connectivity among disparate access networks. Utilizing the IP-based framework as its communication paradigm, the NGMN aims to offer *anytime, anywhere, anyhow* connectivity by materializing both seamless mobility and guaranteed quality of service (QoS) to its users. The inter-connectivity of heterogeneous networking interfaces, however, has introduced new security challenges to the NGMN. Not only the NGMN is vulnerable to security threats stemming from individual legacy networks, it can also be exposed to more severe attacks due to migration of security threats across network boundaries [2]. While various techniques have been proposed to resolve these security issues (i.e., in the form of firewall architectures and intrusion detection systems (IDS)), unfortunately most of these techniques are inherently designed for a homogeneous network, and thus not viable for a distributed heterogeneous environment like the NGMN.

In the recent years, the exceptional capabilities of the Human Immune System (HIS) in mitigating foreign invaders inside the human body has inspired researchers to adopt this concept into computer and systems security [3]. While this concept has also been extended into network security, particularly for a homogeneous system [4], to the best of our knowledge, there is no such work on an NGMN scenario reported in literature. With the aim of filling in the gap, this paper highlights and discusses the potential of applying the principles of the HIS concept for securing the NGMN. Several important points, in particular the distributed nature of the HIS in handling invaders and its fault tolerance feature (i.e., its ability to operate accordingly even in the event of failure of certain organs of the HIS) have motivated us to apply this concept to the NGMN. Note that the distributed nature of the organs of the HIS in the human body is analogous to various interworked access networks in the NGMN architecture (as illustrated in Fig. 1). On the other hand, the fault tolerance feature is essential for an NGMN scenario. Every attack detected in a sub-network should be locally resolved and not collapse the NGMN structure.



(a) HIS architecture [5]. (b) NGMN architecture [2].

Fig. 1. Distributed nature of the HIS and the NGMN.

In general, there are two distinct perspectives about the working principle of the HIS. The first is based on the principle of *self-nonself* discrimination of cells in the human body [5]. Nevertheless, there is no clear premise on how to differentiate between the *self* (legitimate) and the *nonself* (illegitimate) agents since both elements often share common regions. This problem may also lead to the violation of fundamental security principles such as introducing large false positives and false negatives in the detection process. The second concept, the Danger Theory (DT) addresses some of the limitations of its counterpart. Instead of relying on the *self-nonself* criteria, the

This work is partially supported by the Australian Research Council under the Discovery Project Scheme (DP0771523). Fazirulhisyam Hashim {fhisyam@ee.usyd.edu.au} is sponsored by the Malaysian Ministry of Higher Education.

978-1-4244-4388-8/09/$25.00 ©2009 IEEE

central idea of the DT is to react in the event of a danger condition resulted by an invader's malicious behavior. In addition, the DT also proposes an alternative method to resolve invaders within a local region (say, sub-network) called the Danger Zone (DZ). Due to these interesting features, several researchers have utilized the DT concept to address security problems in homogeneous networking environments [6][7]. In this paper, the DT is used to enhance the survivability of a distributed NGMN from malicious network attacks. This so-called survivability framework incorporates two key components: namely, an attack detection framework and a security control framework. The former is responsible for attack identification, while the latter performs a recovery mechanism by isolating the region under the malicious attacks within the NGMN and restricting their propagation to other domains.

The remainder of this paper is organized as follows. Section II presents a brief overview of the DT, while Section III discusses the theoretical framework of adapting the DT in the NGMN. The performance evaluation is presented in Section IV, followed by some concluding remarks.

II. An Overview of Danger Theory (DT)

The Danger Theory (DT) challenges the traditional *self-nonself* principle by forming the basis of legitimate-illegitimate distinction in the HIS. Initiated by Matzinger in 1994 [8], this ideology is based on a so-called *danger signal* rather than differentiating between *self-nonself*. In fact, given its central idea on responding to danger, the DT has also emphasized the notion that not all *nonself* elements (i.e., invaders) are malicious and even *self* elements are not necessarily incapable of causing a danger to the human body. Furthermore, the DT introduces the concept of a Danger Zone (DZ). According to this concept, whenever a cell detects a danger, the distressed cell establishes a DZ around itself. Thus, only the cells that reside within the DZ gets stimulated by the signal, and are involved in the mitigation process. Those cells that are located beyond the DZ are not stimulated. The DZ concept can also be perceived as a control method where the effect of an intruder is localized to a certain spatial degree. This improves the efficiency of the system since only the affected area (i.e., within the DZ) reacts to the warning. While the concept of responding to a danger signal seems to be a more logical explanation to the HIS, similar to its counterpart, the exact nature of a danger signal is unclear [8]. Nevertheless, a three-signal rule framework: namely, *lymphotic laws* has been proposed as the working principle for the DT [8]. According to the *lymphotic laws*, the first signal is merely a signal that initiate the HIS, i.e., *Initiation Signal* (*IS*). The second one is the *Recognition Signal* (*RS*) and the last signal is the *Co-stimulation Signal* (*CS*). While the *RS* is used for antigen detection, the *CS* is utilized for ensuring that the detected antigen is really dangerous. Not only the correlation of these signals guarantee the working principle of the HIS, it also reduces the possibility of having high false alarms (i.e., false negatives and false positives) in the system.

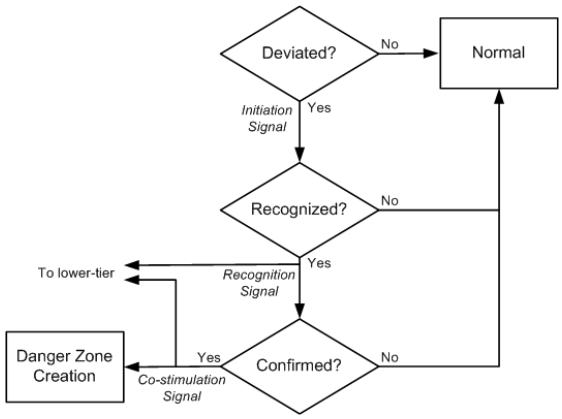


Fig. 2. Danger theory in heterogeneous networks.

III. The Danger Theory (DT) in NGMN

In this section, we present the key components of our proposed survivability framework for the NGMN.

A. Attack Detection Framework

The attack detection framework incorporates three distinct processes where each of them is responsible for initiating the previously mentioned three danger signals (i.e., *IS, RS,* and *CS*) from the *lymphotic laws*. Fig. 2 illustrates the working principle of this framework.

1) Initiation Process: This process is triggered whenever any node in the network detects any irregularity from its normal operation. While the abnormal characteristic can be defined by appropriate parameters (e.g., number of packet loss, jitter, delay, etc.), in this work we consider the deviation of network traffic pattern from its normal baseline profile. Therefore, in this work network traffic, in particular the traffic pattern is considered as the antigen. Since we are considering a malicious bandwidth attack such as denial-of-service (DoS) or a distributed DoS (DDoS), the deviation of network traffic typically involves an excessive number of packets/flows, thereby causing the observed traffic (X_t) to go beyond the normal baseline profile ($\mathfrak{B}_t$). This profile is defined according to the traffic envelope concept, proposed in [9]. Upon detecting any abnormality in the traffic, the under attacked node triggers the *IS* (i.e., a report message) and sends it to the Antigen Presenting Cell (APC), which is responsible for performing the identification and confirmation of attacks. In this work, the highest entity in the domain is considered as the APC (e.g., gateway for a wired domain, Gateway GPRS Support Node (GGSN) for a Universal Mobile Telecommunications System (UMTS) domain). For instances, consider an attack scenario in a UMTS domain where an abnormal behavior is detected at the Serving GPRS Support Node (SGSN). In this case, the SGSN sends the *IS* to its GGSN. The GGSN then initiates the DT mechanism within the network.

2) Recognition Process: In this process, the APC (i.e., the GGSN) examines the severity level of the observed traffic (i.e., indicated by the *IS*). If it detects any anomalous observations in

the traffic, it will send the *RS* (i.e., act as a triggering or report message) to its lower tier entities (i.e., the SGSNs) to notify about the occurrence of malicious behavior in the network.

Let m be the number of observed traffic flows that invokes the *IS* (i.e., $X_t > \mathfrak{B}_t$). Each flow is dedicated a counter C_l ($l = 1, 2, \ldots, m$), which comprises of k number of subcounters c such that $C_l = \{c_j : j = 1, 2, \ldots k\}$. Given the scenario where $\hat{A}_j(l)$ represents the detected attack event added to the specific jth subcounter of the flow l, the severity level of the flow can be expressed as follows,

$$Pr(\hat{A}(l)) = \sum_{j=1}^{k} \frac{x_j}{k} \tag{1}$$

where x_j represents the detected $\hat{A}_j(l)$ event. In [10], we have established the idea of identifying and classifying anomaly behavior by utilizing the distinct spectral characteristics properties of network traffic. This method employs the Lomb periodogram [11] to transform the time-series data into the frequency-series. The analysis involves the evaluation of the packet arrival at different angular frequencies, which leads to the identification of possible anomalies in the spectrum representation. From our discreet observations, we found that anomalous traffic, in particular DoS and DDoS, possess a very unique pattern of spectral power distribution that distinguish them from the normal behavior traffic (as illustrated in 3(a)). In general, the DoS traffic exhibits dominant frequencies at higher frequency points, while for the DDoS traffic, the spectral distribution is dominated by lower frequency components. Fig. 3(b) shows the spectrum distribution of DoS and DDoS attacks from our performance evaluation.

Now, given two distinct frequency spectrums X_f and Y_f, where the former represents a predefined signature (based on the spectrum distribution) and the latter implies the observed traffic, the irregularities can be identified from the deviation of the cross-correlation of the two signals (R_{xy}). A *mirror effect* property is used to indicate the similarity level of the two cross-correlated spectrums, i.e., $R_{xy}(-z) \approx R_{xy}(z), \forall z : -lag \leq z \leq lag$, where lag is the lag generated from the cross-correlation function. Hence, the existence of this feature in the cross-correlated signals strongly suggests the presence of particular anomalies (either DoS or DDoS, depending on the signature spectrum X_f). The *mirror effect* parameter Dv_1 is computed as $Dv_1 = \frac{1}{z}\sum(\Delta R_{xy})^2$, where $\Delta R_{xy} = R_{xy}(z) - R_{xy}(-z)$. The Dv_1 value is then used to segregate the malicious and the normal traffic, according to the following conditions,

$$x(l) = \begin{cases} \text{anomaly } (\hat{A}) & \text{if } Dv_1 \leq \epsilon \\ \text{normal } (\hat{N}) & \text{if } Dv_1 > \epsilon \end{cases}$$

where ϵ represents a predefined threshold value for the *mirror effect* property. The result from the *mirror effect* analysis is used to compute the severity level in (1). In this process, the *RS* is triggered whenever it violates a predefined threshold value (i.e., specified by network administrator).

3) Co-stimulation Process: In this process, the APC (i.e., the GGSN) corroborates whether the detected traffic deviation (i.e., from the *Initiation Process*) is originated by the DoS/DDoS traffic (i.e., from the *Recognition Process*). In such a case, the GGSN reacts by sending the *CS* to its lower tier entities, thereby alerting the SGSNs on the occurrence of attack in the network. In addition, the *CS* also incorporates the signature (i.e., extracted from the spectral analysis) of the newly encountered attack.

Let a random variable D represent the traffic deviation, where $D = 1$ implies possible deviations from the normal envelope and $D = 0$ if otherwise, and $\hat{A}$ as the presence of malicious attack. Thus, the traffic deviation likelihood ratio Λ_D is modeled as $\Lambda_D = \frac{P(D=1|\hat{A})}{P(D=0|\hat{A})}$, where $P(D = 1|\hat{A})$ is the conditional probability of traffic deviation occurrence given the possible attack events $\hat{A}$, and $P(D = 0|\hat{A})$ represents no occurrence of traffic deviation given the possible attack events $\hat{A}$. From the *Recognition Process*, the presence of attack events in a single flow l (i.e., $P(D = 1|\hat{A} : C_l)$) can be represented in a probability form according to the occurrence of possible attacks in the flow counter C_l, as previously emphasized in (1). Thus, given the attack event $\hat{A}$, the Λ_D can be calculated according to the ratio between the probability that $\hat{A}$ in m flows will cause the deviation over the probability that $\hat{A}$ will not cause traffic deviation,

$$\begin{aligned} \Lambda_D &= \frac{P(D = 1|\hat{A} : C_1, C_2, \ldots, C_m)}{P(D = 0|\hat{A} : C_1, C_2, \ldots, C_m)} \\ &= \frac{1 - \prod_{i=1}^{m}(1 - P(D = 1|C_i))}{\prod_{i=1}^{m}(1 - P(D = 1|C_i))} \end{aligned} \tag{2}$$

Using this convention, we can infer the occurrence of attacks in traffic deviation whenever $\Lambda_D \geq T$, where T is the decision threshold value. Upon receiving the *CS* from the GGSN, the SGSNs can initiate its own DT mechanism. This includes the generation of the DZ and update their lower tier entities about the attack (to be discussed in the next section).

B. Security Control Framework

1) Attack Localization Process: In order to restrain the propagation of attacks in the network, we incorporate the foundation of the previously explained *lymphotic laws* [8] and clonal expansion [5] in the HIS. While the former principle ensures the attack propagation can be restricted and resolved within the network domain (i.e., restricting epidemic attack), the latter principle (i.e., to be discussed in the subsequent section) avoids the attack from affecting other network domains in the NGMN (i.e., restricting pandemic attack).

a) Epidemic Attack - Intra-domain Isolation: This strategy utilizes the DZ concept in the DT. Here, the DZ is defined as a spatial region, which spans from where the attack is detected to the respective lower tier network entity L_1. In conformation to the *lymphotic laws*, to update the whole

domain about the attack, both *RS* and *CS* need to be distributed among the L_i ($i \in N$, where N is a real number).

Upon receiving the *RS* from its upper tier, the L_1 (e.g., SGSN) recognizes the occurrence of suspicious attack in the network. The L_1 then forwards the *RS* to its lower tier entities L_2 (e.g., Radio Network Controller (RNC)), and L_2 will forward the *RS* to its lower tier L_3 (e.g., Node B), and so on. Note that according to the *lymphotic laws*, to be fully activated (i.e., to establish the DZ), each network entity has to wait for the *CS*. When the L_1 receives the *CS* from its respective upper tier, it initiates the local DZ and subsequently forwards the *CS* to its lower tier entities. In the case that the network entity L_i has not received the *CS* within a predefined interval t_w[1], the L_i is then deactivated. Since the L_i has not received the *CS*, its entire lower tier entities will be deactivated, thereby stopping the distribution of the *CS* to certain area of the network. Note that the proposed strategy ensures the network to react only to the confirmed malicious traffic (i.e., notified by the *CS*), thus reducing the number of false alarms. Besides, owing to its local containment process, the intra-domain isolation enables a very strategic and effective control mechanism by isolating the attack within a particular domain, and eases the process of alerting the whole network domain about the attack.

b) Pandemic Attack - Inter-domain Isolation: Due to the spatial restriction of the DZ coverage, we employ one of the HIS processes: namely, the clonal expansion (CE) to provide a global security control to the NGMN. The CE is a process analogous to the task of good lymphocytes (or cells, typically B-cells) to divide themselves into multiple clones with similar capabilities [5]. These clones are transferred and distributed via human blood vessels, thereby providing immunity to the entire body.

Owing to the inter-connectivity of various heterogeneous access networks of the NGMN, it can be perceived that any malicious attack is no more proprietary to a particular network. In fact, there is a huge possibility of encountering an attack, which is initiated from different network. With the vision of restricting a pandemic attack on the NGMN, we utilize the CE process to notify other domains of the NGMN about the attack. Similar to the DT, the CE process should be handled by the APC or the highest network entity in the domain. Following the convention of the CE process, the selected APC is responsible to update its peer entities at other network domains. Nevertheless, instead of distributing both *RS* and *CS*, these signals are aggregated into *RCS* before being distributed to the peer network entities. Once receiving the *RCS*, that particular domain (i.e., the recipient) may decide whether to alert its local domain about the attack and to initiate the DZ mechanism.

2) Attack Recovery Process: The DoS/DDoS attack mitigation requires reactive and prompt responses from the network. While some of the attacks' unique identifier is in the source IP address, other types of attacks can be detected based on the payload, the signature, and so on. Hence, network administrators may use any appropriate method that suits their security requirement. For brevity, in this work we implement a simple yet effective filtering method to recover from the malicious DoS/DDoS attack. Using the IP address as the identifier, the attacked domain creates a set of blacklist address from the Access Control List (ACL). In addition, as the attack detection framework utilizes spectral analysis to determine attack signature, a system log containing this information is kept for traffic forensic which can be used to determine the occurrence of repeated attack.

[1]This scenario may happen when the APC cannot guarantee or confirm about the status of the attack, thereby refusing to initiate the *CS*.

TABLE I
ANOMALY DETECTION PERFORMANCE

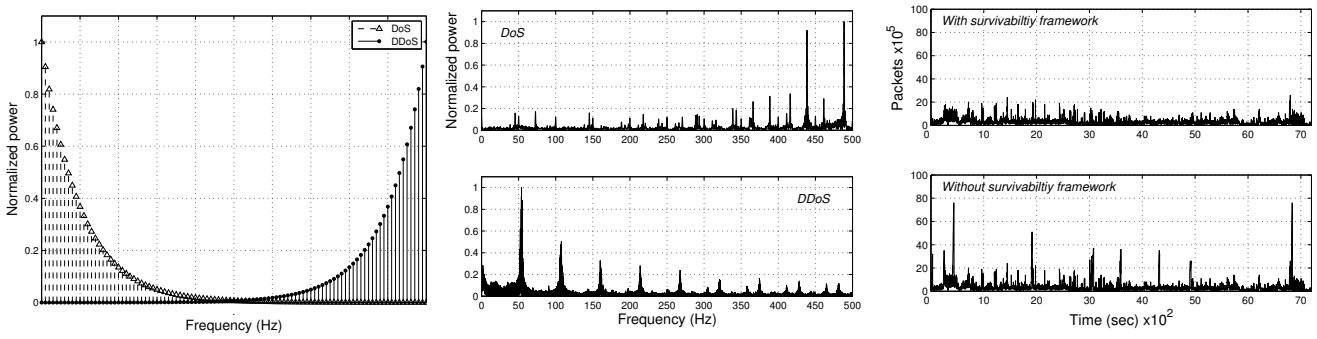
Detection Method	Trace A		
	True Positives	False Negatives	False Positives
Traffic Envelope	10	0	4
CUSUM	8	2	0
Proposed Method	10	0	0
Detection Method	**Trace B**		
	True Positives	False Negatives	False Positives
Traffic Envelope	10	0	3
CUSUM	8	2	0
Proposed Method	10	0	0

IV. PERFORMANCE EVALUATION

We perform an empirical evaluation on two independent trace files: namely, Trace A and Trace B [12]. Ten random DoS/DDoS attacks are initiated and injected into both traces. In addition, we have also created 20 sets of additional traffic flows and injected them to both traces to emulate flash crowd event (FCE) scenarios. The inclusion of malicious DoS/DDoS attacks and FCE in the traffic is essential to examine the capability of the proposed framework in discriminating between malicious (i.e., DoS/DDoS) and non-malicious (i.e., FCE) activities in the network. For comparison purposes, we have considered two additional detection methods,

1) Traffic envelope [9] - Detecting anomalies based on deviation from normal traffic profile.
2) Cumulative Sum (CUSUM) [13] - An abrupt changes detection in traffic statistics using sequential analysis.

The selection of the aforementioned methods are due to their capabilities of offering low false alarm rate, and have proven to be optimal in terms of detection accuracy [9][13]. The performance of these detection methods (i.e., including the proposed attack detection framework) in detecting anomalies is summarized in Table I. Our analysis involves several security parameters such as true positive, false negative and false positive. Here, the true positive indicates the successfully detected malicious attacks, the true negative implies the undetected malicious attacks, and the false positive reflects the criteria of wrongfully detects innocent traffic as malicious ones. From the table, it is apparent that the proposed attack detection framework offers the best performance in terms of anomaly detection. While the traffic envelope is capable of detecting traffic deviation, unfortunately, this method does not consider



(a) (b) (c)

Fig. 3. (a) Unique spectral pattern of DoS and DDoS. (b) DoS and DDoS spectral pattern from network traffic. (c) Impact of the survivability framework.

the cause of the deviation. This explains the large number of false positives of the detection method where it concludes several normal traffic flows (i.e., FCE) as malicious ones. The same explanation applies to the CUSUM technique. However, as the CUSUM technique utilizes heuristic and sequential analysis, it tends to smoothen the effect of the FCE, thus it only detects instantaneous spikes generated by malicious attacks. Nevertheless, if the attack pattern behaves like the FCE (as in the case of our simulation), it may introduces false negative to the system due its incapability of detecting such well-crafted anomalies. Among the three, the proposed detection framework provides the best detection accuracy. This is mainly due to the fact that it uses three levels of detection steps, in particular the *Initiation Process*, the *Recognition Process*, and the *Co-stimulation Process*.

In addition, as proof of our concept, we present the effect of the proposed survivability framework for Trace A (as illustrated in Fig. 3(c)). Note that the top and the bottom figures represent the traffic condition in NGMN with and without the survivability framework, respectively. While both scenarios are affected by malicious attacks (i.e., represented by visible spikes in both figures), it can be observed that the one with the proposed framework is capable of isolating and restricting the propagation of the attack. Note that a similar scenario has been observed in the Trace B simulation. This proves the efficiency of the DT, the DZ, and the CE mechanisms in detecting and isolating the malicious traffic, thereby securing the NGMN from an attack.

V. Conclusion and Future Work

In this paper, we proposed a survivability framework for the NGMN that incorporates two key components: namely, an attack detection framework and a security control framework. Inspired from the HIS, the proposed framework adopted the DT concept, in particular the *lymphotic laws* paradigm to identify malicious attacks to the NGMN. On the other hand, the security control framework utilizes the DZ and the CE concepts to mitigate the propagation of epidemic and pandemic attacks, respectively. The simulation results have demonstrated the capability of the proposed framework in detecting and isolating the threats in a timely manner. With such promising results, we intend to explore the HIS capabilities in recuperating injuries of human body and extend the concept into the security control framework in particular the attack recovery process.

References

[1] M. R. Kibria and A. Jamalipour, "On designing issues of the next generation mobile network," IEEE Network, vol. 21, no. 1, pp. 6-13, Jan. 2007.

[2] F. Hashim, M. R. Kibria, and A. Jamalipour, "Securing the next generation mobile network," Wiley Journal of Security and Communication Networks, vol. 1, no. 1, pp. 25-43, Feb. 2008.

[3] P. K. Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont, "An artificial immune system architecture for computer security applications," IEEE Transactions on Evolutionary Computation, vol. 6, no. 3, pp. 252-280, Jun. 2002.

[4] F. Dressler, "Bio-inspired promoters and inhibitors for self-organized network security facilities," in Proc. ACM Conference on Bio- inspired Models of Network, Information and Computing Systems, vol. 275, Cavalese, Italy, Dec. 2006.

[5] P. J. Delves, S. J. Martin, D. R. Button, and I. M. Roitt, *Essential Immunology*, 11th ed., Blackwell Publishing, 2006.

[6] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod, "Danger theory: The link between AIS and IDS?," in Proc. Conference on AIS (ICARIS), pp. 147-155, Edinburgh, UK, Jul. 2003.

[7] A. Secker, A. A. Freitas, and J. Timmis, "A danger theory inspired approach to web mining," in Proc. Conference on AIS (ICARIS), pp. 156-167, Edinburgh, UK, Jul. 2003.

[8] P. Matzinger, "Tolerance, danger and the extended family," Annual Review of Immunology, vol. 12, pp. 991-1045, 1994.

[9] F. Feather, D. Siewiorek, and R. Maxion, "Fault detection in an ethernet network using anomaly signature matching," in Proc. ACM SIGCOMM, pp. 279-288, California, USA, Sep. 1993.

[10] F. Hashim, M. R. Kibria, and A. Jamalipour, "Detection of DoS and DDoS attacks in NGMN using frequency domain analysis," in Proc. Asia-Pacific Conference on Communications (APCC), pp. 1-5, Tokyo, Japan, Oct. 2008.

[11] N. R. Lomb, "Least-squares frequency analysis of unequally spaced data," Astrophysics and Space Science, vol. 39, pp. 447-462, Feb. 1976.

[12] CAIDA, the Cooperative Association for Internet Data Analysis, available at http://www.caida.org/home/, 2009.

[13] H. Wang, D. Zhang, and K. G. Shin, "Change-point monitoring for the detection of DoS attacks," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 4, pp. 193-208, Oct. 2004.