Biologically Inspired Anomaly Detection and Security Control Frameworks for Complex Heterogeneous Networks

Fazirulhisyam Hashim, *Student Member, IEEE,* Kumudu S. Munasinghe, *Member, IEEE,* and Abbas Jamalipour, *Fellow, IEEE*

***Abstract*—The demand for *anytime, anywhere, anyhow* communications in future generation networks necessitates a paradigm shift from independent network services into a more harmonized system. This vision can be accomplished by integrating the existing and emerging access networks via a common Internet Protocol (IP) based platform. Nevertheless, owing to the interworked infrastructure, a malicious security threat in such a heterogeneous network is no more confined to its originating network domain, but can easily be propagated to other access networks. To address these security concerns, this paper proposes a biologically inspired security framework that governs the cooperation among network entities to identify security attacks, to perform security updates, and to inhibit attacks propagation in the heterogeneous network. The proposed framework incorporates two principal security components, in the form of anomaly detection framework and security control framework. Several plausible principles from two fields of biology, in particular the human immune system (HIS) and epidemiology have been adopted into the proposed security framework. Performance evaluation demonstrates the efficiency of the proposed biologically inspired security framework in detecting malicious anomalies such as denial-of-service (DoS), distributed DoS (DDoS), and worms, as well as restricting their propagations in the heterogeneous network.**

***Index Terms*—Heterogeneous network security, biologically inspired security, human immune system, danger theory, epidemiology.**

I. Introduction

WITH the ever-increasing demands for seamless high-quality network services, the future generation network is envisaged to offer a boundless communication paradigm, thereby realizing *anytime, anywhere, anyhow* communications for its users. As illustrated in Fig. 1, to achieve these goals, future generation networks require the capability for integration and interoperation with existing and emerging access technologies under an interworked Internet Protocol (IP) based framework [1][2]. Such an interworking infrastructure facilitates the convergence of networks as well as services, thereby addressing the requirement for seamless communications in future generation networks. Owing to the interworking principle, every network entity (or node) in the heterogeneous network infrastructure encounters data transactions over various traffic classes from different networking technologies.

Despite its advantages, the interworking architecture may introduce additional security challenges, which hinder successful future generation networks deployment. In particular, the heterogeneous network is exposed to vulnerabilities stemming from individual access networks. These vulnerabilities can be largely categorized into [3]: (i) network access security (e.g., authentication of new users due to vertical handoffs) and (ii) defending against external attacks. While the former has received much attention from the research community [4] and governing bodies [5], it has not been the case for the latter. Owing to the boundless communication paradigm in heterogenous networks, this paper focuses on two possible external security threats, which are referred as epidemic and pandemic attacks. An epidemic attack denotes a large scale anomaly (e.g., denial-of-service (DoS), distributed DoS (DDoS)) that is targeted at nodes residing in the same network as the adversary. On the other hand, a pandemic attack implies to the migration of security threats across network boundaries, which can occur by attacking nodes at other access networks, as well as due to vertical handovers of infected terminals (e.g., worms attacks). As the heterogeneous network infrastructure interconnects a number of access networks, any attack in the heterogeneous network is no more confined to the respective network (i.e., epidemic) as it can be easily extended into a pandemic type of attack.

In light of these two possible attack scenarios, conventional security mechanisms (i.e., commonly based on independent approach) are no more sufficient in heterogeneous networks. A concerted security effort, which involves cooperation among dissipated networking entities at various levels of the architecture is therefore necessary for securing the heterogeneous network early enough from external attacks [3]. Due to the possibility of experiencing attacks from various sources (i.e., epidemic and pandemic), the heterogeneous network should incorporate a robust detection and mitigation mechanism at the core network of each domain, which would act as a *first line of defence* (i.e., especially against pandemic attacks) for the respective network domains. Detecting and mitigating these external attacks via a cooperative approach will therefore form

Manuscript received November 23, 2009; revised May 21, 2010 and July 6, 2010. The associate editor coordinating the review of this paper and approving it for publication was M. Brunner.

This work is partly supported by the Australian Research Council under the Discovery Project Scheme (DP0771523). F. Hashim is sponsored by the Malaysian Ministry of Higher Education.

The authors are with the School of Electrical and Information Engineering, University of Sydney, NSW 2006, Australia (e-mail: {fhisyam, kumudu}@ee.usyd.edu.au; a.jamalipour@ieee.org).

Digital Object Identifier 10.1109/TNSM.2010.1012.0360

the core of any heterogeneous network's security architecture.

With the aim to accommodate an appropriate security solution (i.e., to govern the cooperative security functions) to the heterogeneous network, this paper draws inspirations from security mechanisms found in other research disciplines. Promising solutions for security exists in the field of biology, in particular, the human immune system (HIS). In principle, the HIS is analogous to the network intrusion detection systems (NIDS) as they perform similar security functions to their respective systems. The HIS identifies malicious microbes via cooperation among various cells (e.g., B cells and T cells). Whenever a malicious microbe is detected inside the human body, the HIS updates surrounding cells/tissues/organs about the event. Another interesting avenue for inspirations exists in the field of epidemiology, specifically on diseases control strategies (e.g., quarantine and social distancing). These strategies are efficient for restricting widespread diseases, especially during the absence of appropriate vaccines. In regards to network security, given the rapid propagation of external attacks (e.g., worms), it is common that the attack solution may not be available at the security database during the time of attack. In such a scenario, the most effective approach is to slow down the attack propagation.

Motivated by these two fields of biology, we propose a biologically inspired security framework to defend heterogeneous networks against three dominant epidemic and pandemic attacks; namely, DoS, DDoS, and worms. The security framework incorporates two key components; an anomaly detection framework and a security control framework. The anomaly detection framework adopts the working principle of the HIS, in particular the danger theory (DT) for governing the detection of malicious adversaries. On the other hand, the security control framework conducts an autonomous mitigation process for retrieving appropriate security solutions from security databases. In the absence of a security solution, the framework initiates an inhibition strategy which is adopted from the field of epidemiology to restrict the propagation of epidemic and pandemic attacks in the network.

The remainder of this paper is organized as follows. Section II provides an overview of existing literature on biologically inspired security. The proposed anomaly detection framework is presented in Section III, while the security control framework is discussed in Section IV. Section V presents the performance evaluation and discussions, followed by some concluding remarks in Section VI.

II. Bio-inspired Security: An Overview

This section highlights several seminal works on biologically inspired security from the following perspectives; anomaly detection and anomaly inhibition.

A. Anomaly Detection

A large and growing body of literature has adopted the detection concept of the HIS into their security systems [6][7][8]. This detection concept follows two distinct theories; namely, negative selection (NS) and danger theory (DT). While the NS is the traditional understanding of anomaly detection in the HIS, the DT is a radical new concept that challenges the main fundamentals of the NS. According to the NS, the HIS detects anomalies by discriminating between *self* and *nonself* markers presented at the cell's surface. In principle, a *self* marker is carried by the body's own cells, whereas a *nonself* marker is carried by foreign cells. Whenever an immune defender (e.g., a T cell) encounters a cell carrying *nonself* marker, it identifies this cell as an invader. On the contrary, the DT identifies anomalies by discriminating the nature of cell distress, i.e., either *apoptosis* or *necrosis*, where the former is a natural process of cell death and the latter is an abnormal process caused by external factors such as infections from bacteria. According to the DT, an anomaly can be detected by reacting to a danger situation, which is caused by necrotic cell distress.

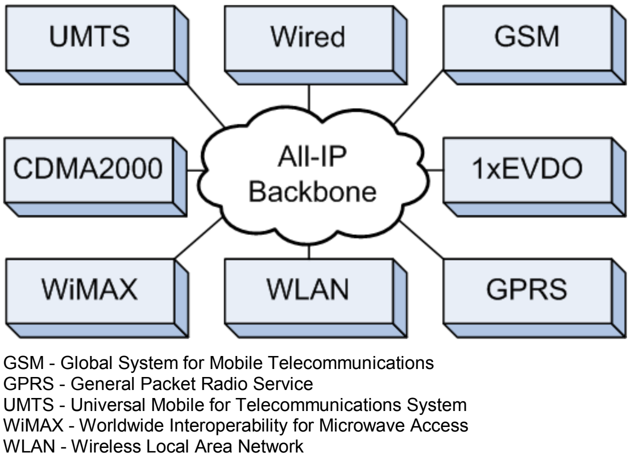

UMTS
Wired
GSM
CDMA2000
All-IP Backbone
1xEVDO
WiMAX
WLAN
GPRS
GSM - Global System for Mobile Telecommunications
GPRS - General Packet Radio Service
UMTS - Universal Mobile for Telecommunications System
WiMAX - Worldwide Interoperability for Microwave Access
WLAN - Wireless Local Area Network

Fig. 1. General interworking framework of heterogeneous networks.

Forrest *et al.* were among the earliest researchers to apply the NS theory for detecting anomalies in a computer system [6][7][8]. Given its remarkable ability to distinguish between legitimate cells (*self*) and anomalous cells (*nonself*), the NS theory has been extensively exploited in solving the computer-virus problem [6]. Most of the existing literature have employed the "learning" mechanisms of the NS theory and created a pattern-matching rule to identify *self-nonself* feature in a computer system [7][8][9][10]. Unfortunately, the NS imposes various theoretical limitations for being implemented in a heterogeneous network: no clear premise on how to distinguish between the *self* and the *nonself* elements, and significant computational overhead for maintaining a set of *self-nonself* elements.

In 1998, Mark Burgess introduced the DT concept for securing computer systems [11]. Several other notable works by Burgess: an entropy-based tool (*Cfengine*) to identify anomalies in Unix-like systems [12] and a machine learning approach to detect anomalies in computer systems [13]. However, the proposed methods are loosely based on the HIS as they haven't applied any principle of the HIS, but rather emphasize the importance of providing an immunity for computer systems. A more well-defined approach is provided in [14] that utilizes a co-stimulation process to reduce the number of false alarms in anomaly detection. While [14] is similar in part to the approach presented in this paper, the method is limited to host intrusion detection system (HIDS), which is not directly applicable to a networking domain.

The ideology of the DT inspired IDS has also been extended into a computer networking paradigm [15]. Several notable works to this effect: detection of SYN scans [16] and Bots [17] based on the working principle of a Dendritic Cell (DC), T cell immunity and tolerance for computer worm detection [18], a double layers detection model for DoS attacks based on the interaction principle between DCs and T cells [19]. Nevertheless, to the best of our knowledge, no such work on a complex heterogeneous scenario exists at present.

B. Anomaly Inhibition

In the field of epidemiology, two inhibition strategies, i.e., social distancing and quarantine, have been proposed for containing the initial emergence of infectious diseases [20]. In general, the social distancing strategy is based on the principle of avoiding contact with people in the community. Meanwhile, the quarantine strategy utilizes the *assume guilty until proven innocent* principle, where an aggressive quarantine action takes place whenever a person exhibits symptoms of a disease.

The idea of adopting these strategies for restricting anomaly propagations in networks is not new. Zou *et al*. [21] investigated a dynamic quarantine scheme using Susceptible-Infectious (SI) epidemic model. Nevertheless, this model considers a *homogeneous mixing* scenario, which is not directly applicable for a heterogeneous networking environment. Subsequent researches have focused on various problems of quarantine strategy in homogeneous environment: the effectiveness of partial quarantine (i.e., which network should be quarantined first) [22] and the impact of limited network capacity on quarantine strategy [23].

On the other hand, traffic rate limiting (i.e., correspond to social distancing) has been proposed as a less aggressive inhibition approach, which enables traffic from suspicious nodes to enter the network but at a slower pace. In [24], the authors suggested that throttling the volume of outbound connections that a host is allowed to initiate to new machines may reduce the attack rate, without significantly hindering normal communications. In [25], the authors argued that throttling both incoming and outgoing traffic are more effective than the outgoing-only approach. Nevertheless, host-based rate control has very little benefit unless they are universally deployed, which may not be viable in real implementation. In regards to heterogeneous networks, controlling the rate of network hosts at the backbone, which accommodate the links among individual networks are relatively more effective.

Besides the above mentioned strategies, another potential avenue for inspirations lies from the concept of homeostasis in biology. In principle, homeostasis is a property of a system to maintain its stability (normal operation). It should be noted that the previously discussed HIS can be perceived as a subset of homeostasis, as it identifies malicious microbes to maintain the stability of human body. One notable work on the homeostasis computing is presented by Somayaji and Forrest [26], where they proposed a response system called pH (process homeostasis), to detect and stop intrusions before the target system is fully compromised. This pH system monitors every executing process in a computer at the system-call level, and subsequently responds to the detected anomalies by either delaying or aborting system calls. The objective of this approach is somewhat similar to our proposed inhibition strategy, although it does so at the system-call (i.e., computer kernel) instead of the network traffic-level (i.e., packets/flows). For this reason, the pH system could be implemented (i.e., in network entity's kernel) in conjunction with our proposed inhibition strategy to further slow down anomaly propagation.

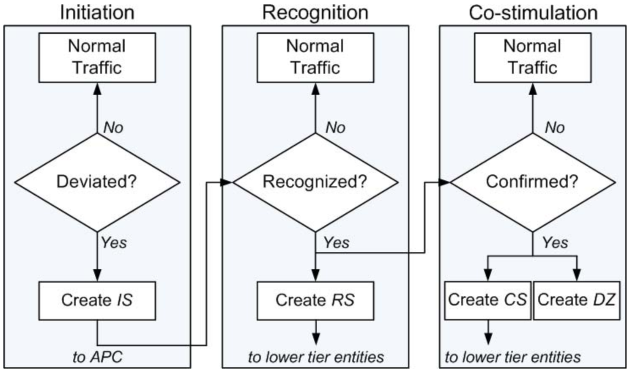


Fig. 2. DT principle of the anomaly detection framework.

III. Anomaly Detection Framework

Our proposed anomaly detection framework adopts the working principle of the DT, which was published by Matzinger in 1994 [27]. According to the DT, the detection of malicious microbes in the human body is handled by three danger signals, which are governed by a framework called *lymphotic laws*.

The *lymphotic laws* state that the first danger signal, called initiation signal (*IS*), is triggered whenever a cell senses danger condition. The *IS* is sent to the Antigen Presenting Cell (APC), which is responsible for detecting the cause of the danger. Once the cause of the danger is identified, say a virus, the APC triggers the second danger signal called recognition signal (*RS*) and subsequently transmits several copies of *RS* to nearby cells. In order to confirm that the identified virus is really malicious, the APC performs a cross-examination between the causes of the first two danger signals. Once confirmed, the APC creates the third danger signal called co-stimulation signal (*CS*), and sends them to the nearby cells. The correlation of these danger signals ensures the human body for correctly identifying the cause of cell distress. Moreover, the *lymphotic laws* also enables the human body to localize the impact of cell distress. This localization allows the distressed cell or the APC to establish a spatial area around itself called a Danger Zone (DZ), which stimulates other cells within the DZ coverage to aid in the mitigation process.

The proposed anomaly detection framework utilizes the *lymphotic laws* principles to govern the following three detection processes; (i) the identification of abnormal behavior in network traffic pattern (i.e., handled by Initiation Process), (ii) the detection of malicious anomalies in the traffic (i.e., handled by Recognition Process), and (iii) the confirmation of an attack occurrence (i.e., handled by Co-stimulation Process). Fig. 2 illustrates the working principle of this framework. While the Initiation Process can be performed by any entities in the network, the Recognition and Co-stimulation Processes are handled by the APC of the network, which is the highest entity in the network domain (e.g., gateway for wired networks).

A. Initiation Process

According to the DT, the HIS activates the Initiation Process whenever a body cell is distressed by a possible danger condition. In regards to heterogeneous network security, this initial detection process is triggered whenever an entity in the heterogenous network detects any irregularity in its normal operations. This irregularity can be detected either at the node (or system) level or at the network level. In the former, the detection of abnormal condition can be performed by any appropriate HIDS (e.g., *Cfengine* by Burgess [12]), whereas at the network level (i.e., local network in particular) it can be performed by any suitable NIDS.

Since we are considering the detection of malicious bandwidth attacks (e.g., DoS and DDoS), the deviation of network traffic pattern from its normal profile is used as the indicator of a danger condition. Recent studies have shown that traffic in a high-speed network exhibits self-similar attributes [28]. As the envisioned heterogeneous network is also enjoying such high-speed links (i.e., especially at the backbone), it is feasible to assume that network traffic in this network also shares similar attribute. The underlying pattern of heterogeneous traffic can be represented by a generic expression $X_t = \mu_t + \varepsilon_t$, where μ_t is a time-varying function of the long-trend traffic pattern (i.e., originated by the "stationary" mean μ and seasonal deviation factors, such as days, weeks, and so on). On the other hand, the ε_t represents the short-trend variations from the μ_t, which exhibits Gaussian behavior and can be characterized as an independent identically-distributed (i.i.d) with a zero mean $\varepsilon_t \sim N(0, \sigma^2)$. This self-similar attribute indicates that the network traffic in a heterogeneous environment exhibits a specific pattern over time, and thus it is feasible to assume that the network administrator should have a prior knowledge of the normal traffic profile of the network. Given the dynamic nature of network traffic, the baseline profile should be updated based on a predefined time interval fixed by the administrator. This update process can be carried out by any appropriate machine learning mechanism [13] or time-series analysis.

Two deviation scenarios may occur in the network traffic. In the first scenario, the network traffic exceeds the acceptable normal baseline profile, $X_t > \mathfrak{B}_t$, where $\mathfrak{B}_t = \mu_t(1 + \alpha_t)$ and α_t indicates the percentage of permitted deviation from μ_t. This phenomenon mainly happens due to the occurrence of useless packets/flows from malicious bandwidth attacks (i.e., DoS, DDoS, and worms). The second scenario emerges from the dynamic nature of network conditions, for instance failure of connections, lack of resources, and so on. In this case, the observed network traffic is significantly less than the baseline profile $X_t < \mathfrak{B}_t$. Given the nature of a malicious bandwidth attack on the network, here, we only address the former case, i.e., X_t exceeds the normal baseline profile $\mathfrak{B}_t$. In this situation, the distress entity initiates an alert message, in the form of *IS* which is then submitted to its APC. The procedure of the Initiation Process is summarized in Fig. 2 (labeled as "Initiation").

B. Recognition Process

The Recognition Process is responsible for analyzing the network traffic that causes the distress condition to the network entities. In principle, this process identifies malicious anomalies that reside in the deviated traffic, therefore it shares similar functionality with a conventional NIDS. While effective in legacy networks, conventional NIDS (i.e., commonly utilized packet-level analysis) may no longer be efficient in identifying epidemic and pandemic attacks in heterogeneous networks.

In heterogeneous networks, every network entity encounters data transactions over various traffic classes from different networking technologies. These heterogeneous traffic flows inherit disparate characteristics due to different packet headers, which lead to various packet sizes, traffic criteria, and traffic distributions. Furthermore, each network may have different MAC protocols and topologies. In light of their distinct characteristics, traffic traversing in such an interworked network is considered as heterogeneous in nature. With such disparity in traffic flows, conventional NIDS (i.e., proprietary to specific networks) have been found insufficient in identifying malicious attacks in a heterogeneous networking environment. In fact, it becomes almost impossible for the system to prevent external attacks by monitoring and regulating individual users in a large network like the heterogeneous network. An increase in traffic aggregation at network edges (especially core network) precludes detecting and filtering solely on packet header information, as that could remove legitimate traffic. Furthermore, an increase in traffic volumes will also enable malicious traffic to hide themselves in background traffic, yet still do great harm to the heterogeneous network.

Besides, various challenges exist to the conventional NIDS, in particular, the ability of sophisticated attackers to spoof and forge the packet header information (e.g., IP address), the complexity of packet-level inspection, both attacks (e.g., DoS) and legitimate traffic may exhibit similar statistical properties, and so on. In light of this, a competent anomaly detection approach becomes necessary, which is able to expose the existence of malicious flows in heterogeneous traffic, as well as immune to the above mentioned limitations.

1) Flow-level Spectral Analysis: This paper utilizes an efficient entropy-based detection technique for detecting malicious network anomalies [29]. In order to avoid a complex packet-level inspection, the Recognition Process conducts a flow-level spectral analysis on the heterogeneous network traffic. In [29], we have demonstrated the capability of this spectral analysis method for exposing the exact nature of traffic (i.e., either normal or malicious) in a heterogeneous network environment. This is achieved by exploiting the distinct spectral characteristics properties of traffic in individual access networks. Various types of network traffic have been considered to emulate the underlying traffic distributions of existing networks. The analysis involved the robustness of the proposed spectral analysis method against various dynamic characteristics of heterogeneous networks such as link capacity, link delay, cross-traffic and bottleneck scenarios. It should be noted that this method has various significant advantages over the existing NIDS: ability to circumvent packet-level inspection and encryption, only using packets timing information for detecting anomaly, and insensitive to spoof attack [29].

In principle, the proposed spectral analysis transforms the time-series packet arrivals (X_t) into frequency-series (X_f) data (i.e., in the form of power spectral density (PSD)) by using the Lomb periodogram [30]. Specifically, the spectral analysis method identifies network anomalies by analyzing dominant amplitude bands in the PSD. From our observations, we found that anomalous traffic, in particular DoS and DDoS, possess a very unique pattern of power spectrum distribution that distinguishes them from the normal behavioral traffic [29]. Specifically, the DoS traffic exhibits dominant frequencies at higher frequency points, while for the DDoS traffic, the spectral distribution is dominated by lower frequency components. Given these inherent characteristics, the generated traffic spectrum from this flow-level spectral analysis can be used as the signature for the observed network traffic. Assuming that it belongs to a malicious traffic, this signature is then distributed across the heterogeneous network so that it can be utilized for traffic forensic (e.g., as evidence for capturing the perpetrator of any malicious DoS/DDoS activity) and to avoid possible repetitive attacks on the network.

It is worthwhile to highlight that this spectral analysis is also efficient for exposing other types of malicious anomalies (e.g., worms). The spectral analysis may utilize different traffic attributes (e.g., incoming or outgoing packets, packet sizes) for identifying other malicious anomalies. Thus, by carefully examining the "behavior" of a particular anomaly, one may exploit its unique attribute for creating a specific spectral signature using this method.

2) Detecting Malicious Anomaly: A malicious flow can be segregated from a legitimate flow by identifying the existence of the *mirror effect* property in traffic [29]. Since anomalous traffic possesses a very unique pattern of PSD, it can be used as the signature for anomaly in the Recognition Process. Now, let X_f and Y_f depict two distinct frequency spectrums, where the former represents the generated spectrum of the observed traffic and the latter denotes the predefined anomaly signature. Note that the *mirror effect* property indicates the level of similarity of the cross-correlated spectrums R_{xy}, which can be defined as, $R_{xy}(-z) \approx R_{xy}(z), \forall z : -l_{ag} \leq z \leq l_{ag}$, where l_{ag} is the lag generated from the cross-correlation function. Now, let d_m represents the *mirror effect* parameter such that, $d_m = \frac{1}{l_{ag}} \sum (\Delta R_{xy})^2$, where $\Delta R_{xy} = R_{xy}(z) - R_{xy}(-z)$. Recall that the existence of the *mirror effect* property in the cross-correlated signals strongly suggests the presence of particular anomalies (either DoS or DDoS, depending on the signature spectrum Y_f). Therefore, the d_m value is then used to segregate the anomalous and the normal traffic, according to the following conditions:

$$X_t = \begin{cases} \text{anomaly } (\hat{A}) & \text{if } d_m \leq \epsilon \\ \text{normal } (\hat{N}) & \text{if } d_m > \epsilon \end{cases} \quad (1)$$

where, ϵ represents a predefined threshold value for the *mirror effect* property. Interested readers are referred to [29] for a detailed description of the spectral analysis detection method.

In order to reduce the number of false alarms, each of the suspicious traffic flow l ($l \in m$, where m is the number of observed traffic flows that invokes the *IS*) is dedicated a counter C_l. Each counter comprises of k number of sub-counters c, such that $C_l = \{c_j : j = 1, 2, \dots k\}$. Every suspicious traffic flow is divided into k number of equal segments (i.e., sub-counters), where each segment is then transformed into the frequency-series and their d_m are computed using the spectral analysis method. Let us denote by $\hat{A}_j(l)$ the detected anomaly event from the spectral analysis, which is added to the specific jth sub-counter of the flow l. The severity level of the suspicious flow l can be expressed in a probability form:

$$Pr(\hat{A}(l)) = \sum_{j=1}^{k} \frac{x_j}{k} \quad (2)$$

where, x_j represents the detected $\hat{A}_j(l)$ event from the spectral analysis method. In this process, the *RS* is triggered whenever $Pr(\hat{A}(l))$ violates a predefined threshold value, $\mathbf{T}_{\hat{A}}$, which is specified by the network administrator.

Since the severity level of the observed traffic flow is represented in a probability form $Pr(\hat{A}(l))$, the network administrator may fix the $\mathbf{T}_{\hat{A}}$ to any appropriate probability value. Different sets of policies can be authorized for different types of anomalies. For example, considering a DoS attack, the network administrator may define that the APC will initiate the *RS* when the computed severity level $Pr(\hat{A}(l))$ exceeds 0.3. Multiple copies of *RS* are then transmitted to lower tier entities to inform them about the occurrence of possible DoS attacks in the heterogeneous network. The procedure of the Recognition Process is summarized in Fig. 2 (labeled as "Recognition").

C. Co-stimulation Process

The final component of the proposed anomaly detection framework is the Co-stimulation Process. In comparison to existing NIDS, this process imposes an additional security measure, which involves a cross-examination between the previous two detection processes. It provides a mechanism to identify the "significance" of the identified anomaly, as well as to further reject false positives in the detection. In particular, the Co-stimulation process focuses on the following question: "is the suspicious anomaly significant enough to be classified as a genuine attack?", given the previous two detection processes may have falsely accused a legitimate traffic as an attack.

This corroboration task can be performed by using either the likelihood-ratio test or the Bayes' Theorem. For brevity, this paper utilizes the likelihood-ratio test for performing such a task. Let a random variable D represents the occurrence of traffic deviation in the Initiation Process, where $D = 1$ implies to traffic deviations from the normal profile, and $D = 0$ represents no traffic deviation. On the other hand, we denote by $\hat{A}$ the presence of malicious anomalies in the network traffic, which is detected by the Recognition Process. Following the principle of the Co-stimulation Process, the APC (e.g., GGSN) would like to determine whether the suspicious anomaly (identified by the Recognition Process at the APC) is significant enough to create a danger condition at the node (identified by the Initiation Process). It should be noted that these two information (i.e., provided by *IS* and *RS*) are readily available to be used by the APC.

This corroboration can be determined by the traffic deviation likelihood-ratio Λ_D, which is represented by, $\Lambda_D \equiv \frac{P(D=1|\hat{A})}{P(D=0|\hat{A})}$, 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 $\hat{A}$. Thus, if the likelihood ratio is significant enough, this Co-stimulation Process concludes that the traffic deviation (i.e., cause of node distress in Initiation Process) is really originated by the identified anomalies from the Recognition Process.

Since traffic deviation in the Initiation Process can be originated by various traffic flows (i.e., in the case of DDoS attacks), the Co-stimulation Process needs to consider the possibility of an attack from every single flow in the traffic. Note that 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 suspicious attacks in the flow counter C_l (i.e., from the Recognition Process), as previously emphasized in (2). Thus, for a single flow l, the presence of attack events can be represented by its severity level, which is given by $P(D=1|\hat{A}:C_l) = \sum_{j=1}^{k} \frac{x_j}{k}$. By extending this equation, the Co-stimulation Process may compute the conditional probability of traffic deviation for multiple traffic flows, $P(D|\hat{A}:C_1, C_2, \ldots, C_m)$. Given the two traffic deviation conditions (i.e., $D=1$ and $D=0$), their conditional probabilities can be represented as follows:

$$\prod_{l=1}^{m}(1-P(D=1|C_l)) \qquad \text{if } D=0 \tag{3}$$

$$1-\prod_{l=1}^{m}(1-P(D=1|C_l)) \qquad \text{if } D=1 \tag{4}$$

Using both (3) and (4), the likelihood-ratio test Λ_D can be quantified as the following:

$$\Lambda_D \equiv \frac{P(D=1|\hat{A}:C_l)}{P(D=0|\hat{A}:C_l)} \equiv \frac{1-\prod_{l=1}^{m}(1-P(D=1|C_l))}{\prod_{l=1}^{m}(1-P(D=1|C_l))} \tag{5}$$

The occurrence of a malicious bandwidth attack in the deviated traffic can be confirmed whenever $\Lambda_D \geq \gamma$, where γ is the decision threshold value defined by the network administrator. In this process, if the APC corroborates that the detected traffic deviation is really originated by the malicious attack, it triggers multiple copies of *CS* and sends them to the lower tier entities for alerting them about the occurrence of attack in the network. The procedure of the Co-stimulation Process is summarized in Fig. 2 (labeled as “Co-stimulation”).

The network administrator may determine the threshold γ by bounding the performance of the Λ_D according to the probability of true positives, P_D (i.e., traffic that invokes the Initiation Process is really an attack), and the probability of false positives P_F (i.e., wrongfully accused as an attack). Since these two are unknown parameters, we may use maximum achievable values for both P_D and P_F, say 0.99 and 0.01, respectively. The network administrator may define theoretical performance achievements for both P_D and P_F, which can be bounded by two requirement parameters η_0 and η_1 such that $\eta_0 \geq P_F$ and $\eta_1 \leq P_D$. Using these relations, the decision threshold parameter γ can be expressed in terms of both P_D and P_F, where $\gamma \leq \frac{P_D}{P_F}$ [31]. Given the requirement parameters η_0 and η_1, it can be deduced that the decision threshold γ can be assigned a specific value subject to the following relation, $\gamma \leftarrow \frac{\eta_1}{\eta_0}$.

In addition, the *CS* also incorporates the traffic signature (i.e., extracted from the spectral analysis) of the newly encountered attack. Upon receiving the *CS* from the APC, the lower tier entities may initiate their own DT mechanism by establishing a Danger Zone (DZ) around themselves, and update their lower tier entities about the attack. Note that once an adversary is detected, the under attacked domain creates a set of graylist addresses from the Access Control List (ACL). The attacker’s ID (e.g., IP address for wired networks, IMSI (International Mobile Subscriber Identity) for cellular) is then inserted into the graylist and remains in the graylist for a T_g period. This graylist is used during the mitigation process, in particular for thwarting the propagation of malicious anomalies in the network, which will be discussed in the next section.

IV. Security Control Framework

Our proposed security control framework incorporates two key processes; namely, security update process and attack recovery process. In general, this framework governs the following security functions; (i) to update the under attacked network about the adversary, and (ii) to restrict anomaly propagations (i.e., in the absence of security solutions).

A. Security Update Process

As various access networks are interworked together in a heterogeneous network, our proposed method addresses the following two update scenarios, i.e., intra-network and inter-network updates. Note that the update process is subject to the spatial coverage defined by the Danger Zone (DZ).

In this paper, the DZ is defined according to the computed Λ_D in the Co-stimulation Process. Whenever the APC determines that the observed traffic flow is highly likely to be an attack traffic, a larger DZ coverage is imposed on the network. For instance, when the Co-stimulation Process reports a small Λ_D value of DoS attack on the SGSN, an update is sent to other SGSNs in the same network domain. However, if the Λ_D is relatively larger, the SGSN may also consider updating not only its peer SGSNs but also other lower tier nodes in the domain. The appropriate DZ coverage for a specific Λ_D is predefined using a full histogram. Hence, the APC may perform a lookup operation to find an appropriate solution for the DZ. This information is inserted into the *CS* before being disseminated in the network. Note that the network may also consider the types of threats for defining the DZ. As the decision for this coverage may vary among the heterogeneous networking domains, the decision should be kept as a proprietary parameter.

1) Intra-network Update: The principal idea of the intra-network update is to alert other networking entities in the network domain about the detected attack. Referring to Fig. 3, let us consider a scenario where a malicious DoS attack scenario has been detected in a UMTS domain and the APC (i.e., in this case, the GGSN) has decided to update all other entities in its domain. Upon receiving the *RS* from its APC, the lower tier entity (i.e., SGSN) acknowledges the occurrence of a suspicious attack in its domain. The SGSN then forwards the *RS* to its lower tier entity (i.e., RNC), and so on. According to the *lymphotic laws*, the DZ can only be established when the entity receives the *CS* from its upper tier. Nevertheless, if an entity has not received the *CS* after waiting for a t_w interval, the entity is then deactivated. This scenario occurs when the APC hesitates to create the *CS* as the suspicious traffic have falsely been accused as malicious during the Initiation Process. As the entity has not received the *CS*, all its lower tier entities will be deactivated, thereby stopping the distribution of the *CS* to other areas of the network. The proposed strategy ensures that the network only reacts to confirmed malicious traffic (i.e., notified by the *CS*), thus reducing the number of false alarms. Owing to its local containment process, this method enables a very strategic and effective control mechanism by isolating the attack within a particular domain, and eases the process of alerting the network about the attack.

2) Inter-network Update: Given the inter-connectivity of various access networks in heterogeneous networks, a malicious attack will no more be confined to a single network. Thus, it is necessary to provide a global security updates for heterogeneous networks. Unfortunately, the DZ concept alone is not capable for performing such a task, i.e., informing other interworked network domains about the attack, as the security update is confined within the under attacked domain. To achieve this goal, the inter-network update adopts another concept from the HIS; namely, the *clonal expansion* (*CE*). In HIS, the *CE* is a process of good lymphocytes to divide themselves (via mitosis) into multiple clones with similar capabilities [32]. Unlike the DZ where signal distribution is restricted to a certain spatial degree, in the *CE*, the clones are distributed via blood vessels, thereby providing immunity to the entire body. In regards to heterogeneous networks, this procedure is handled by the APC of the under attacked domain, where it updates its peer APC nodes at other access networks. For example, in Fig. 3, upon confirming the occurrence of an attack, the GGSN distributes the *CS* to the PDSN in the CDMA2000 network. Upon receiving the *CS*, the PDSN may decide whether to alert its local domain about the attack (i.e., initiating its own DZ mechanism).

B. Attack Recovery Process

This process regulates an autonomous anomaly mitigation procedure and restricts attack propagations in the network.

1) Autonomous Mitigation Process: Extending the concept from our security update process, the proposed attack mitigation process is handled locally within the DZ area. This autonomous process is administered by the APC, which performs the task of the security manager for the domain. Each APC of the heterogeneous network is equipped with a security server, which acts as a global security database for its domain. Meanwhile, every individual network may have their own security database, which is coordinated with the global security database. Assuming that an appropriate solution is available in the server, whenever an adversary is detected, the APC fetches this solution from its security database and subsequently distributes the solution to other network nodes within the predefined DZ coverage. In the case that the solution is not available, the APC may request the solution from its peer APCs in other domains. Nevertheless, if the adversary is a newly detected attack and the solution (e.g., patch) is not available in the global security server, human intervention becomes inevitable.

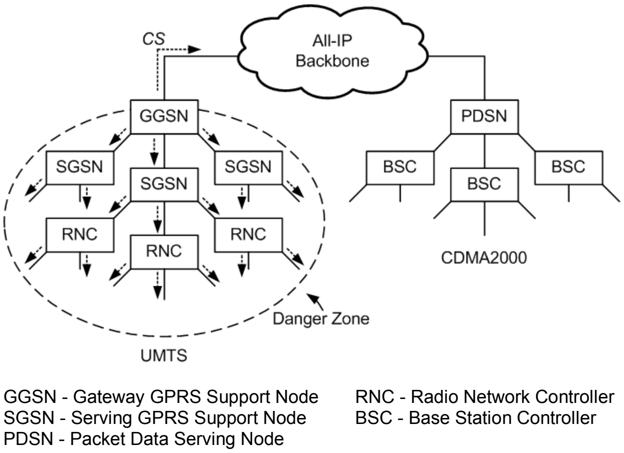

CS
All-IP Backbone
GGSN
SGSN
SGSN
SGSN
RNC
RNC
RNC
PDSN
BSC
BSC
BSC
CDMA2000
Danger Zone
UMTS
GGSN - Gateway GPRS Support Node
SGSN - Serving GPRS Support Node
PDSN - Packet Data Serving Node
RNC - Radio Network Controller
BSC - Base Station Controller

Fig. 3. Danger Zone creation and *CS* disseminations in the network.

2) Inhibiting Anomaly Propagation: Given the possibility that the required solution is not available in the security server, an alternative option is to prolong the time for the security personnel to respond to the attack. Motivated by the disease outbreak control procedures of the real world, our proposed inhibition strategy utilizes two competent methods; namely, node quarantine and traffic rate limiting. In principle, node quarantine is more efficient than traffic rate limiting for restricting attack propagations. Nevertheless, rate limiting may benefit a falsely accused node as its traffic may still enter the network but at a slower pace.

Owing to their advantages, we incorporate both methods into our inhibition strategy, and exploit two types of attack identifiers; namely, the attack signature and the attacker ID, as illustrated by the algorithm in Fig. 4. Let us consider the propagation of attacks, either epidemic or pandemic, in an access network i. Their propagations can be modeled using the Community of Household (CoH) model [33], which is an extension of the classical epidemic Susceptible-Infectious (SI) family. The macroscopic representation of anomaly propagations between individual access networks can be expressed by the following equation:

$$\frac{dI_i}{dt} = \beta_i I_i (N_i - I_i) + \sum_{j \neq i} \beta_{ji} I_j (N_i - I_i) \tag{6}$$

where, β_i is the infection parameter in network i (i.e., epidemic) whereas β_{ji} is the infection parameter from network j to network i (i.e., pandemic), I_i is the number of infected nodes in network i, and the total population of network i (N_i) is assumed to be constant such that $\forall t, S_i + I_i = N_i$, where S_i is the number of susceptible nodes. As the inhibition strategy is dependent on the anomaly detection capabilities, it has also

```
if (signature is matched) then
    update signature and ID logs
    fetch appropriate solution
    update security personnel
    while $t < T_q$ do
        quarantine the node
    end while
    release node from quarantine
    traffic rate limiting
end if
if (ID is in graylist) then
    traffic rate limiting
end if
```

Fig. 4. Algorithm of the attack recovery process.

introduced true positive and false positive to the inhibition performance. In this context, the true positive implies to the inhibition of infectious entities by the proposed strategy. On the contrary, the false positive depicts the inhibition of non-infectious entities.

Let us denote by $I_i(t)$ the number of infectious nodes at any given time t in network i, the proposed inhibition strategy may quarantine $R_i(t)$ nodes and subsequently rate limit the traffic of $r_i(t)$ nodes, such that $r_i(t) \subset R_i(t) \subset I_i(t)$. At the same time, the network may also quarantine $Q_i(t)$ nodes and rate limit the traffic of $q_i(t)$ nodes, out of susceptible nodes $S_i(t)$, where $q_i(t) \subset Q_i(t) \subset S_i(t)$. Thus, the dynamics of infectious nodes in the network i can be formulated as follows:

$$\frac{dI_i(t)}{dt} = \beta_i[I_i(t)_\Delta][S_i(t)_\Delta] \tag{7}$$

where, $I_i(t)_\Delta = I_i(t) - R_i(t) - r_i(t)$ and $S_i(t)_\Delta = S_i(t) - Q_i(t) - q_i(t)$.

Referring to Fig. 4, if an attack possesses a known signature with the ones in the database, the adversary is then quarantined for a T_q time. Unlike the quarantine strategy in epidemiology where the person is released after passing a latent period without displaying any symptoms of the disease, our quarantine method releases the node as the T_q counter expires, regardless of the rectification results. Note that this strategy may benefit the falsely detected nodes as they are quarantined only for a limited period of time. Thus, at a given time t the number of quarantined nodes from the infectious and the susceptible states can be approximated by:

$$R_i(t) = \int_{t-T_q}^{t} [I_i(\tau) - R_i(\tau)]\lambda_R d\tau \tag{8}$$

$$Q_i(t) = \int_{t-T_q}^{t} [S_i(\tau) - Q_i(\tau)]\lambda_Q d\tau \tag{9}$$

where, λ_R and λ_Q are the quarantine rates for true positive and false positive scenarios, respectively. These quarantine rates represent the time taken by the anomaly detection framework to infer the severity of a node (i.e., attack detection time).

Assuming that T_q is a significantly small number (i.e., compared to N_i, $R_i(t)$, and $Q_i(t)$), an average quarantine rate can be used for each entities in the network, subject to their respective scenarios (i.e., either true positive or false positive). Thus, for a small time interval $d\tau$, the $R_i(t)$ and $Q_i(t)$ can be derived as follows:

$$R_i(t) = [I_i(t) - R_i(t)]\lambda_R T_q \tag{10}$$

$$Q_i(t) = [S_i(t) - Q_i(t)]\lambda_Q T_q \tag{11}$$

and can be further simplified as:

$$R_i(t) = \left(\frac{\lambda_R T_q}{1 + \lambda_R T_q}\right) I_i(t) = \theta_R I_i(t) \tag{12}$$

$$Q_i(t) = \left(\frac{\lambda_Q T_q}{1 + \lambda_Q T_q}\right) S_i(t) = \theta_Q S_i(t) \tag{13}$$

where, $\theta_R = \frac{\lambda_R T_q}{1+\lambda_R T_q}$ and $\theta_Q = \frac{\lambda_Q T_q}{1+\lambda_Q T_q}$.

According to Fig. 4, as the quarantine time expires, the traffic from the adversary is then inserted into a rate limiting queue for restricting its access to the network. Instead of targeting the entire traffic of the malicious entity, this strategy regulates the propagation of malicious traffic in the network, where traffic from the malicious entity is permitted to enter the network but at a slower pace [24]. Every packet that is released by the quarantined is then transferred into the rate limiting queue, say at a rate of r_q.

In the queuing system, each packet is released into the network based on a time-out mechanism, which can be performed by any classical scheduling mechanism. Thus, for every time-out period, say d seconds, one packet is discharged from the queue to enter the network. Following the concept in [24], at any given time t, the queue size can be approximated as $l_r(t) \equiv \frac{r_q}{d}(d-1)t, (d > 1)$. Theoretically, as a packet is released from the queue per timeout, the queuing delay generated by this strategy can be computed as $T_d = dl_r t_0$, where t_0 is the time when the malicious packet was inserted into the rate limiting queue. As the T_d increases, this strategy slows down the release of malicious packets into the network, subject to the following relation, rate of release $= \frac{1}{T_d}$. In this strategy, a gigantic anomalous traffic is imposed a lower transmission rate when entering the network. As the size of the queue is significantly large (i.e., occupied by massive number of malicious packets), the T_d increases, thereby slowing down the propagation of anomalous traffic into the network.

Using a similar derivative approach as in the case of quarantine strategy, the number of nodes in the traffic rate limiting can be approximated as:

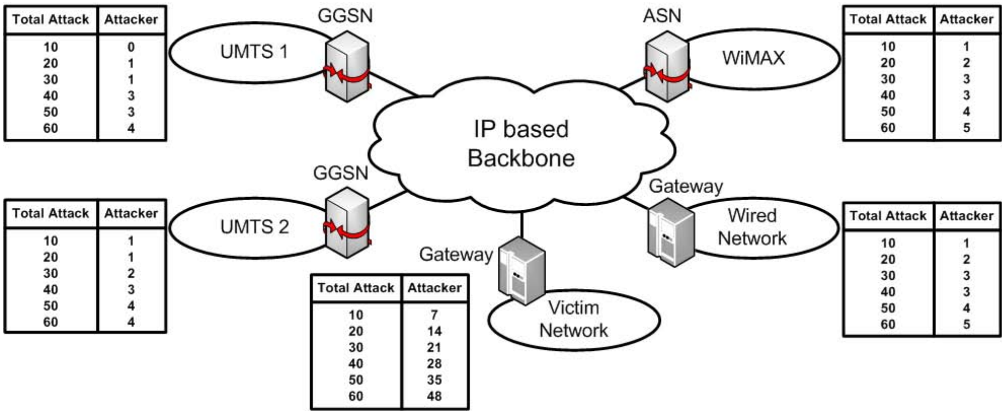
$$r_i(t) = \int_{t-T_q}^{t} [I_i(\tau) - R_i(\tau)]\lambda_R d\tau + \int_{t-T_d}^{t} [R_i(\tau) - r_i(\tau)]\lambda_r d\tau$$

$$q_i(t) = \int_{t-T_q}^{t} [S_i(\tau) - Q_i(\tau)]\lambda_Q d\tau + \int_{t-T_d}^{t} [Q_i(\tau) - q_i(\tau)]\lambda_q d\tau$$

which can be simplified as the following:

$$\begin{aligned} r_i(t) &= [I_i(t) - R_i(t)]\lambda_R T_q + [R_i(t) - r_i(t)]\lambda_r T_d \\ &= \left(\frac{(1-\theta_R)(\lambda_R T_q) + \theta_R \lambda_R T_d}{1 + \lambda_r T_d}\right) I_i(t) = \theta_r I_i(t) \\ q_i(t) &= [S_i(t) - Q_i(t)]\lambda_Q T_q + [Q_i(t) - q_i(t)]\lambda_q T_d \\ &= \left(\frac{(1-\theta_Q)(\lambda_Q T_q) + \theta_Q \lambda_Q T_d}{1 + \lambda_q T_d}\right) S_i(t) = \theta_q S_i(t) \end{aligned}$$

where, $\theta_r = \frac{(1-\theta_R)(\lambda_R T_q)+\theta_R\lambda_R T_d}{1+\lambda_r T_d}$ and $\theta_q = \frac{(1-\theta_Q)(\lambda_Q T_q)+\theta_Q\lambda_Q T_d}{1+\lambda_q T_d}$, where λ_r and λ_q are the queuing rates



Total Attack	Attacker
10	0
20	1
30	1
40	3
50	3
60	4

Total Attack	Attacker
10	1
20	2
30	3
40	3
50	4
60	5

Total Attack	Attacker
10	1
20	1
30	2
40	3
50	4
60	4

Total Attack	Attacker
10	1
20	2
30	3
40	3
50	4
60	5

Total Attack	Attacker
10	7
20	14
30	21
40	28
50	35
60	48

Fig. 5. Simulation environment.

of the infectious and susceptible entities, respectively. In this paper, the queuing rate is defined as the time taken by the network to insert the released malicious packet (i.e., from the quarantine) into the rate limiting queue.

Substituting all the derived formulations into (7), the dynamics of attacks in the network i under the proposed inhibition strategy can be formulated as:

$$\begin{aligned}\frac{dI_i(t)}{dt} &= \beta_i(I_i(t)_\Delta)(S_i(t)_\Delta)\\ &= \beta_i I_i(t) S_i(t)(1-\theta_R-\rho_r)(1-\theta_Q-\theta_q)\\ &= \beta^b I_i(t) S_i(t) \qquad (14)\end{aligned}$$

where, $\beta^b = (1-\theta_R-\theta_r)(1-\theta_Q-\theta_q)\beta_i$. It can be observed that the proposed inhibition strategy reduces the original infection parameter by a factor of β^b. Note that the aforementioned derivations consider the implementation of the proposed inhibition strategy at a single entity in the network i. Considering the hierarchical architecture in existing networks (e.g., UMTS and CDMA200), it is feasible to assume that several entities within the hierarchical architecture are capable of performing such a task. For instance, for UMTS network, this strategy can be implemented at several entities such as GGSNs, SGSNs, and RNCs. Assuming that these entities represent 10% of the total nodes, the infection parameter can be further reduced by a factor of 0.1.

Furthermore, if an attack is launched from the same ID for a p number of times (i.e., repeated attacks), the node's ID (currently in graylist) is then transferred to the blacklist. In this case the node is permanently quarantined by the network and can only be released by the security personnel. Meanwhile, if a node is previously an adversary (ID is still in the graylist) but does not display any malicious behavior, its traffic is rate limited by the network, as shown in Fig. 4.

V. Evaluation and Discussion

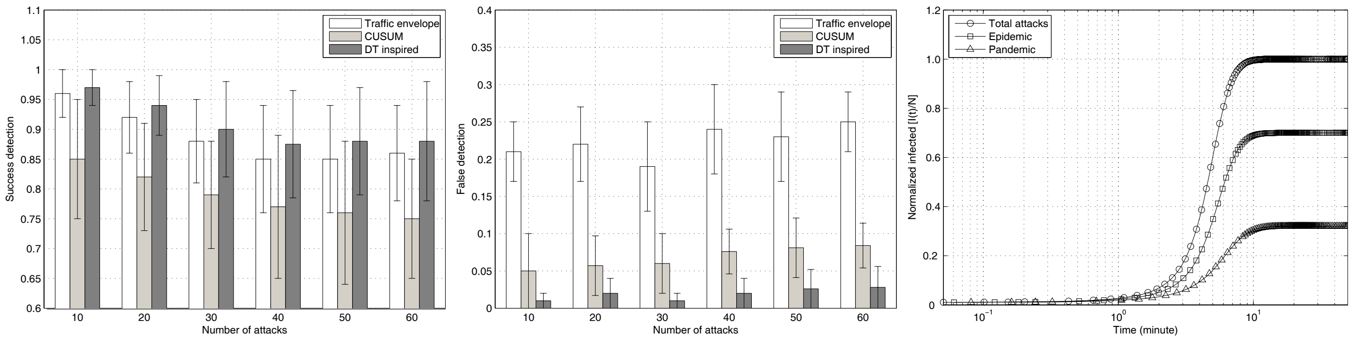
The proposed biologically inspired security framework is analyzed according to the following two simulation scenarios. In the first scenario, we examine the capability of the DT inspired anomaly detection framework for detecting epidemic and pandemic attacks. The detection of two malicious bandwidth attacks, i.e., DoS and DDoS are considered for this simulation. Meanwhile, the second scenario analyzes the capability of the inhibition strategy for restricting anomaly propagations (i.e., worm attacks) in heterogeneous networks.

A. Simulation Settings

We consider an interworked architecture, which consists of 5 access networks, as shown in Fig. 5. For the sake of maintaining consistency, throughout this paper, the proportions of epidemic-pandemic attacks are fixed at 70%-30% of the total number of attacks.

1) DoS/DDoS Simulation: This simulation is performed using discrete-event simulator where the number of entities in every individual network is fixed at $N_i = 100, \forall i$, and runs for 2 hours simulation time. Various number of DoS/DDoS attacks, from 10 to 60 attacks, are generated for this simulation scenario. The distribution of epidemic and pandemic attackers in this simulation is tabulated in Fig. 5. This simulation considers DoS/DDoS attacks on a single node in the victim network. Thus, we assume the danger condition (i.e detected by Initiation Process) due to epidemic attack is handled by a local IDS, whereas for the pandemic attack it is handled by the gateway, which also acts as the APC of this network. Further, various sets of additional traffic flows were created as background traffic as well as flash crowd traffic (i.e., to emulate flash crowd event (FCE) scenarios). The inclusion of both DoS/DDoS attacks and FCE into this simulation is essential to examine the capability of the proposed framework in discriminating between malicious and non-malicious activities in the network. For brevity, both DoS/DDoS attacks are modeled based on the typical bandwidth attack, i.e., sending useless TCP SYN packets to the targeted victim.

2) Worm Simulation: In this simulation scenario, we utilize discrete-time simulation where the number of entities is fixed at $N_i = 10000, \forall i$. Following the 70%-30% rule, this simulation assumes 30% of nodes in the victim network i have the immunity over pandemic attacks but vulnerable to epidemic attacks. Here, a worm attack is modeled based on the random scanning worm, which emulates the real world Slammer outbreaks. To ensure our simulation conforms to the 70%-30% rule, the network should be able to detect the source of the worm, i.e., either epidemic or pandemic. Thus, we define two breeds of Slammer worm, Slam$_{epi}$ and Slam$_{pan}$, which represent an epidemic worm and a pandemic worm,



(a)

(b)

(c)

Fig. 6. (a) *Success detection* performance. (b) *False detection* performance. (c) Worm propagations dynamic in network i.

TABLE I
ANOMALY DETECTION PERFORMANCE CONSIDERING ATTACKS FROM INDIVIDUAL NETWORKS.

Attacker	UMTS 1		UMTS 2		WiMAX		Wired Network		Victim Network	
	Success Detection	False Detection	Success Detection	False Detection	Success Detection	False Detection	Success Detection	False Detection	Success Detection	False Detection
10	0	0	0.95	0	0.95	0	0.95	0.05	0.96	0.01
20	0.95	0	0.90	0	0.93	0.05	0.95	0.05	0.95	0.01
30	0.90	0	0.88	0	0.90	0.03	0.92	0.03	0.91	0.01
40	0.85	0.02	0.87	0.02	0.87	0.02	0.88	0.03	0.87	0.02
50	0.85	0.02	0.84	0.03	0.84	0.04	0.88	0.04	0.87	0.02
60	0.85	0.01	0.85	0.03	0.86	0.04	0.88	0.04	0.86	0.03

respectively. Throughout this simulation, we fix the quarantine time T_q at 20 seconds, and the queuing interval is fixed at $d = 2$ seconds. At $t = 0$, each network is assumed to have one infected Slam$_{epi}$ node and one infected Slam$_{pan}$ node. The simulation stops whenever all nodes in the heterogeneous network is infected by these malicious worms.

B. Simulation Results

1) DoS/DDoS Simulation: Two fundamental security performance metrics; namely, *success detection* and *false detection* are considered in this simulation. These metrics correspond to normalized true positives and normalized false positives of the anomaly detection, respectively. For comparison purposes, the following three anomaly detection methods are considered in our simulation; (i) traffic envelope [34], (ii) cumulative sum (CUSUM) [35], and (iii) the proposed DT inspired anomaly detection framework. In principle, the traffic envelope method detects malicious anomalies based on the deviation of network traffic from its normal pattern profile. Meanwhile, the CUSUM is a nonparametric detection method, which monitors an abrupt change detection in traffic statistics using a sequential analysis approach. The selection of these methods are due to their applicability in existing NIDS, and have been proven for being optimal in terms of detection accuracy [34][35].

Fig. 6(a) and Fig. 6(b) illustrate the *success detection* and the *false detection* of the aforementioned anomaly detection methods. Note that the error bars depict the lower bounds and the upper bounds for 20 independent simulation runs. It can be observed that the proposed DT inspired anomaly detection framework is superior to the other two methods in detecting anomalies in the heterogeneous network. In most of the cases, the proposed framework is capable of detecting over 87% of the DoS/DDoS attacks, while at the same time generates significantly small number of false alarms (less than 5%). As a proof of concept, it is worthwhile to highlight the anomaly detection performance of the proposed framework in detecting both epidemic and pandemic attacks, as tabulated in Table I. Owing to the correlation of its three anomaly detection processes, in particular the Initiation Process, the Recognition Process, and the Co-stimulation Process, it is apparent that the DT inspired framework is efficient in detecting both epidemic and pandemic attacks in the heterogeneous network.

Nevertheless, from Fig. 6(a) it is also apparent that the *success detection* performance of the traffic envelope is somewhat comparable to our proposed detection framework. As mentioned earlier, the traffic envelope identifies anomalies whenever it experiences traffic deviation in the heterogeneous network. Thus, any deviation is regarded as potential anomalous event, which justifies its competency in detecting malicious traffic. However, a main drawback of this method is that it does not consider the cause of the traffic deviation. From our analysis, we observe that this method identifies a significant number of normal flows (i.e., FCE) as malicious traffic. This contributes to the large number of false positives in the simulation results, as shown in Fig. 6(b).

On the other hand, the *false detection* performance of the CUSUM is comparable to our proposed DT detection framework. Unlike the traffic envelope, the CUSUM is initiated whenever the mean of network traffic exceeds a certain percentage value of the baseline profile. When this happens, a change point is registered and the level of change is then accumulated. An anomaly is detected whenever the accumulated change points become greater than an alarm threshold. As the CUSUM method utilizes a nonparametric sequential analysis, it tends to smoothen the effect of the FCE, and thus detecting instantaneous spikes, which are mainly generated by malicious anomalies. Despite its resilience to the FCE, in the case where the attack pattern exhibits similar features like the ones in FCE (as in the case of our simulation), it may introduce false negatives to the system due its incapability of detecting such well-crafted anomalies. Furthermore, from our analysis, the CUSUM method is also incapable of detecting small scale DoS/DDoS attacks. While these attacks produce several significant spikes in the traffic pattern, they have not altered the mean value of the traffic, and thus in some cases the CUSUM is not even initiated.

2) Worm Simulation: For comparison purposes, we have incorporated the following three inhibition strategies; (i) node quarantine, (ii) rate limiting, and (iii) the proposed inhibition method, into the security control framework. The performances of these inhibition strategies are evaluated according to their attack propagation time, in particular on how much time is needed by epidemic and pandemic worms to infect the entire entities in the heterogeneous network. For clarity, Fig. 6(c) illustrates the dynamics of worm attacks in a network i without any inhibition strategy. According to this figure, it takes approximately 10 minutes for both epidemic and pandemic attacks to infect all the entities in this network (i.e., represented by 1.0 of the y-axis). In the following, we present the simulation results for each inhibition strategies in the network i.

a) Node Quarantine Analysis: We present the effect of two commonly used attack identifiers, i.e., node ID and attack signature, on the quarantine strategy (refer to Fig. 7(a)). In comparison to the unprotected network, it can be observed that both the ID-based and the signature-based quarantine strategies are capable of slowing down the attack propagation in the network. It is also apparent that the ID-based quarantine is more efficient than the signature-based quarantine for this particular purpose. However, due to its aggressive nature, the ID-based strategy may introduce a significant number of false alarms (i.e., an entity with its ID is in the graylist will be quarantined, regardless of its exact nature). Thus, we hasten to emphasize the inappropriateness of utilizing ID as an attack identifier for the quarantine strategy. Further, as attacks from external networks are prohibited from entering the network i, the dynamic curve is limited to epidemic attacks, which represent 70% of the total attacks.

b) Rate Limiting Analysis: Here, we present the effect of two different rate limiting schemes, i.e., inter-network, and a combination of both inter-network and intra-network (refer to Fig. 7(b)). In the first scheme, only the APC has the capability of limiting the traffic entering/leaving their respective networks. In the second scheme, besides the APC the rate limiting is also implemented by several other entities in the network such as SGSNs, RNCs, network routers, BSCs, and so on. From this figure, we can see that the implementation of rate limiting at both levels (inter-network and intra-network) outperforms the first scheme (intra-network). Note that the inter-network is only efficient for restricting pandemic attacks but not epidemic attacks. This result emphasizes that the inhibition performance can be improved if more number of nodes are involved in performing this strategy.

c) The Proposed Inhibition Strategy: In this analysis, the proposed inhibition strategy is compared with the previously discussed strategies. Given their superior ability in their respective classes, we only consider the results for ID-based quarantine and, inter-network and intra-network traffic rate limiting, (refer to Fig. 7(c)). It can be observed that our proposed inhibition strategy, which is composed by both quarantine and rate limiting provides the best solution for slowing down an attack propagation. Moreover, owing to the implemented quarantine approach in the proposed strategy, the adversaries are limited to epidemic type of attack, and thus avoiding the 100% infection in the network.

In regards to heterogeneous networks, we present the impact of the proposed inhibition strategy on individual networks, as shown in Fig. 7(d). Based on the attack propagation time of individual networks, it is apparent that wired networks are more prone to malicious worm attacks compared to wireless networks (i.e., due to the medium of transmission). The proposed strategy is also more efficient for restricting anomaly propagation in UMTS compared to WiMAX. Since the inhibition strategy in WiMAX is implemented only at its APC (i.e., Access Service Network Gateway (ASN-GW)), it takes less time to infect all entities in this network compared to the UMTS (i.e., when the strategy is implemented at GGSN, SGSN, and RNC). In addition, Fig. 7(e) shows the logical growth of attacks in the heterogeneous network for two scenarios; with and without the proposed inhibition strategy. The result considers the logical growth of attacks in individual networks, which is computed as, $\sum_{i=1}^{5} \frac{I_i(t)}{N_i}$. Without any inhibition strategy, it takes about 100 minutes for the worms to infect all entities of the heterogeneous network, whereas for the proposed strategy it takes approximately 1000 minutes. This clearly shows the ability of our proposed inhibition strategy in slowing down any attack propagation in the heterogeneous network.

C. Discussions

1) Complexity and Attack Detection Time: While the first two processes of the DT inspired anomaly detection framework are relatively similar (in terms of functionalities) to the existing NIDS, the third process (Co-stimulation) imposes additional delay to the overall detection process. Before a mitigation process can be triggered, the network have to wait for a confirmation signal (*CS*) from the APC. While this precautionary action benefits the anomaly detection performance, it has significantly affected the detection time, as shown in Fig. 8(a). In this figure, the attack detection time of the traffic envelope and the CUSUM are normalized by the DT inspired's detection time. It can be observed that both methods require smaller attack detection time than the proposed DT inspired approach. Owing to this Co-stimulation Process, an extra computational overhead is also introduced to the proposed framework. However, as this process is handled by the APC (highest entity of the domain), the generated complexity from these operations can be considered as trivial given the APC's computational capability.

2) Impact on Quality of Service (QoS) Performance: Besides the security aspect, it is important to examine the effect

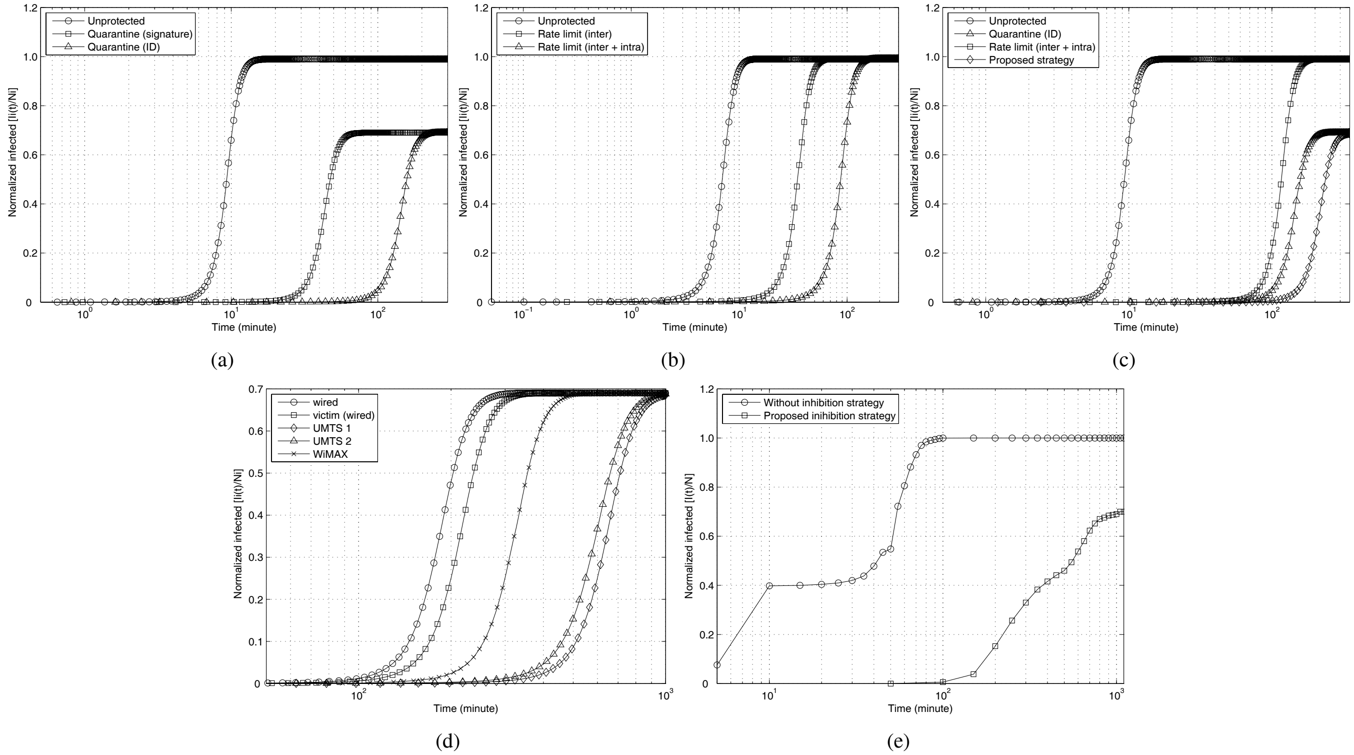


Fig. 7. (a) Node quarantine analysis. (b) Rate limiting analysis. (c) Comparison of inhibition strategies. (d) Attack dynamics of individual networks. (e) Effect of inhibition strategy (no strategy vs. proposed strategy).

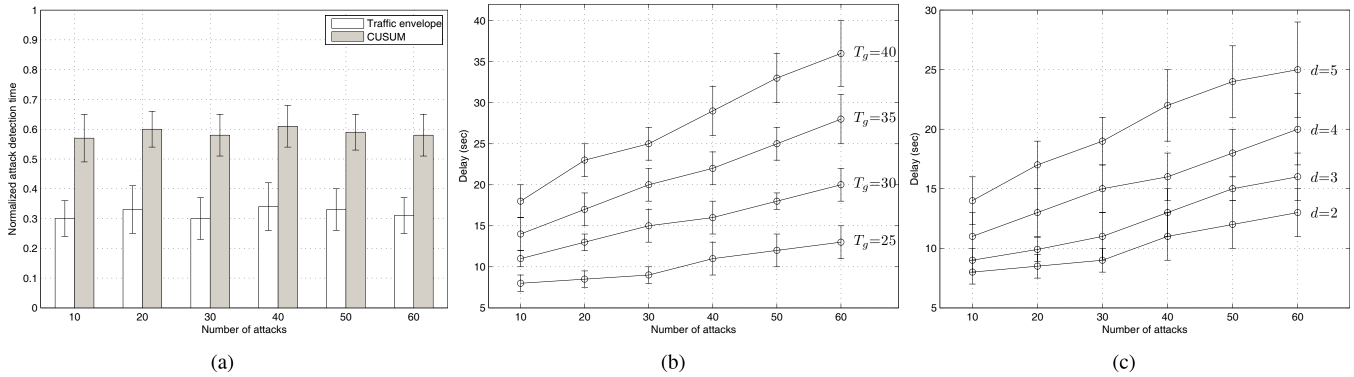


Fig. 8. (a) Attack detection time, normalized by the DT inspired's detection time. (b) Effect of Tg to delay performance. (c) Effect of d to delay performance.

of the proposed security framework on the QoS performance. One of the issues that needs to be addressed is the impact of the rate limiting strategy, in particular the T_g and d on the delay performance of legitimate traffic. Fig. 8(b) illustrates the impact of the T_g (i.e., time of node's ID stays in graylist) on the delay performance of a single transmission from a legitimate node A. Here, we assume that node A has been quarantined for T_q time, and then it starts to transmit legitimate traffic, but is subjected to the rate limiting strategy as its ID is still in the graylist (Fig. 4: line 9). In this figure, $T_g = 25$ means that node A's ID remains in the graylist 5 seconds after its T_q expires (recall that $T_q = 20$), and the same explanation applies to other T_g as well. It can be seen that the transmission delay of node A's traffic increases as the number of attacks increases, and it is severely aggravated at larger T_g values.

The same issue occurs to parameter d, which is the time-out period used by the rate limiting strategy to discharge packets from the queue. Intuitively a larger value of d will provide a better inhibition performance, unfortunately it may also violate the delay requirement of specific traffic classes (e.g., conversational and streaming). As shown in Fig. 8(c), whenever a large number of attacks exists in the heterogeneous network, using a large value for d will significantly affect the delay performance of legitimate traffic. It is apparent that as $d > 3$, the delay increases significantly and violates the delay criteria of several traffic classes. This issue can be addressed by using an appropriate scheduling mechanism in the rate limiting queue or avoiding to rate limit several types of traffic (especially conversational and streaming traffic).

3) Detectability of Unknown Anomaly: The DT inspired anomaly detection framework can also be extended for detecting other types of anomalies. Note that the Initiation Process involves the response of network node to a possible danger condition. In this case, the network administrator may create a set of policies that define all possible danger conditions, e.g., low throughput and high delay, to indicate abnormal activities in the heterogeneous network. Thus, it is up to the Recognition Process and the Co-stimulation Process to determine the exact cause of the danger condition. The correlation between these three processes (subject to appropriate types of IDS in each process) enables the framework to identify malicious anomalies. Moreover, by using the spectral analysis method, the APC may create a unique signature for every traffic flow that it has examined. Since the APC is considered as the global security database in its domain, the signature of detected malicious traffic can be submitted to other local security database (i.e., using coordinated approach described in Section IV-B1).

4) Implementation Strategy and Issues: Since in a network domain any entity can come under attacks, the proposed anomaly detection framework utilizes cooperations between the entity under attack and its corresponding APC. In particular, the anomaly detection process is handled by two different network entities; the distressed node and the APC of the respective network domains. In light of this cooperative approach, the proposed framework can be considered as lightweight as it reduces the burden of the under attacked node during the detection and mitigation process. In the case that the danger condition is detected by the APC (e.g., pandemic attack), all three processes (i.e., Initiation, Recognition, and Co-stimulation) will be handled by this entity. Note that the primary responsibility of the network administrator is to define the threshold values of each process, which will be used as an indicator to trigger the three danger signals (*IS*, *RS*, *CS*).

VI. Concluding Remarks

This paper highlighted two classes of external attacks in heterogeneous networks, which may exist in the form of epidemic and pandemic attacks. With the emphasis on three dominant attacks; DoS, DDoS, and worms, this paper proposed a biologically inspired security framework for governing the attack detection and attack mitigation processes in heterogeneous networks. The proposed security framework incorporated two key security components; namely, an anomaly detection framework and a security control framework. The anomaly detection framework is responsible for detecting epidemic and pandemic attacks, whereas the security control framework governs the security update process, the autonomous anomaly mitigation and the recovery processes. Inspired by the capability of the HIS in detecting infectious microbes in the human body, the anomaly detection framework adopted the DT concept, in particular the *lymphotic laws* to identify malicious anomalies in a heterogeneous network environment. 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. To reduce the impact of malicious attacks on the network, the attack recovery process incorporated two inhibition strategies, which were inspired from the disease control in the real world; namely, the node quarantine and the rate limiting strategies. Given that the proposed framework emulates the working principles of the HIS and the epidemiology, the framework inherits their monumental advantages, and therefore are able to facilitate robust and adaptive anomaly detection, and autonomous mitigation mechanisms to the heterogeneous network.

References

[1] ITU-T Rec. Y.2001, “General overview of NGN."

[2] 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.

[3] H. Moiin, “Next generation mobile networks beyond HSPA & EVDO," white paper, NGMN Alliance, pp. 1-72, Dec. 2006.

[4] M. Shin, J. Ma, A. Mishra, and W. A. Arbaugh, “Wireless network security and interworking," *Proc. IEEE*, vol. 94, no. 2, pp. 455-466, Feb. 2006.

[5] 3GPP, Security aspects for inter-access mobility between non 3GPP and 3GPP access network (Release 8), TS 33.822, Dec. 2008.

[6] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, “Self-nonself discrimination in a computer," in *Proc. IEEE Symp. Sec. Privacy*, pp. 202-212, Oakland, CA, May 1994.

[7] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. Longstaff, “A sense of self for Unix processes," in *Proc. IEEE Symp. Sec. Privacy*, pp. 120-128, Oakland, CA, May 1996.

[8] S. Forrest, S. A. Hofmeyr, and A. Somayaji, “Computer immunology," *Commun. ACM*, vol. 40, no. 10, pp. 88-96, Oct. 1997.

[9] D. Dasgupta and F. Gonzǽlez, “An immunity-based technique to characterize intrusion in computer networks," *IEEE Trans. Evolutionary Computation*, vol. 6, no. 3, pp. 1081-1088, June 2002.

[10] Z. Jinquana, *et al.*, “A self-adaptive negative selection algorithm used for anomaly detection," *Progress Natural Science*, vol. 19, no. 2, pp. 261-266, Feb. 2009.

[11] M. Burgess, “Computer immunology," in *Proc. Syst. Administration Conf.*, pp. 283-297, Dec. 1998.

[12] M. Burgess, ‘Automated system administration with feedback regulation," *Software-Practice Experience*, vol. 28, no. 14, pp. 1519-1530, Dec. 1998.

[13] M. Burgess, “Two dimensional time-series for anomaly detection and regulation in adaptive systems," *Lecture Notes Comput. Science*, vol. 2506, pp. 169-180, Jan. 2002.

[14] M. Burgess, “Probabilistic anomaly detection in distributed computer networks," *Science Comp. Programming*, vol. 60, no. 1, pp. 1-26, Mar. 2006.

[15] U. Aickelin and S. Cayzer, “The danger theory and its application to AIS," in *Proc. Conf. Artificial Immune Syst.*, pp. 141-148, Oeiras, Portugal, Sep. 2002.

[16] J. Greensmith and U. Aickelin, “Dendritic cells for SYN scan detection," in *Proc. Genetic Evolutionary Computation Conf.*, pp. 49-56, London, UK, July 2007.

[17] Y. Al-Hammadi, U. Aickelin, and J. Greensmith, “The DCA for bot detection," in *Proc. IEEE World Congress Evolutionary Computation*, pp. 1807-1816, Hong Kong, June 2008.

[18] J. Kim, W. Wilson, U. Aickelin, and J. McLeod, “Automated worm response and detection immune algorithm (CARDINAL) inspired by T-cell immunity and tolerance," in *Proc. Conf. Artificial Immune Syst.*, pp. 168-181, Alberta, Canada, Aug. 2005.

[19] J. Zhang and Y. Liang, “A double layers detection for DoS based on the Danger Theory," in *Proc. IEEE Comp. Modeling Simulation*, pp. 147-151, China, Mar. 2009.

[20] WHO Guidelines, WHO interim protocol: rapid operations to contain the initial emergence of pandemic influenza, 2007.

[21] C. C. Zou, W. Gong, and D. Towsley, “Worm propagation modeling and analysis under dynamic quarantine defense," in *Proc. ACM Workshop Rapid Malcode (WORM)*, pp. 51-60, Washington, DC, Oct. 2003.

[22] T. M. Chen and N. Jamil, “Effectiveness of quarantine in worm epidemics," in *Proc. IEEE International Conf. Commun.*, vol. 5, pp. 2142-2147, Istanbul, Turkey, June 2006.

[23] N. Jamil and T. M. Chen, “A mathematical view of network-based suppressions of worm epidemics," in *Proc. IEEE International Conf. Commun.*, pp. 1-5, Dresden, Germany, June 2009.

[24] M. Williamson, “Throttling viruses: restricting propagation to defeat malicious mobile code," in *Proc. IEEE Comp. Security Applications Conf.*, pp. 61-68, Las Vegas, NV, Dec. 2002.

[25] N. Jamil and T. M. Chen, “Effectiveness of rate control in slowing down worm epidemics," in *Proc. IEEE Globecom*, pp. 1-6, San Francisco, USA, Nov. 2003.

[26] A. Somayaji and S. Forrest, “Automated response using system-call delays," in *Proc. USENIX Security Symp.*, vol. 9, pp. 1-13, Denver, CO, Aug. 2000.

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

[28] S. Song, J. K. Y. Ng, and B. Tang, “Some results on the self-similarity property in communication networks," *IEEE Trans. Commun.*, vol. 52, no. 10, pp. 1636-1642, Oct. 2004.

[29] F. Hashim, M. R. Kibria, and A. Jamalipour, “Detection of DoS and DDoS attacks in NGMN using frequency domain analysis," in *Proc. Asia-Pacific Conf. Commun.*, pp. 1-5, Tokyo, Japan, Oct. 2008.

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

[31] A. Wald, *Sequential Analysis*. J. Wiley & Sons, 1947.

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

[33] S. Rushton and A. J. Mautner, “The deterministic model of a simple epidemic for more than one community," *Biometrika*, vol. 42, pp. 126-132, 1955.

[34] F. Feather, D. Siewiorek, and R. Maxion, “Fault detection in an Ethernet network using anomaly signature matching," in *Proc. ACM SIGCOMM*, pp. 279-288, Oct. 1993.

[35] H. Wang, D. Zhang, and K. G. Shin, “Change-point monitoring for the detection of DoS attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 1, no. 4, pp. 193-208, Oct. 2004.

Fazirulhisyam Hashim (S’07) is a Ph.D. candidate at the School of Electrical and Information Engineering, the University of Sydney, Australia. He received his Bachelor in Engineering (Computer and Communication Systems) and Master of Science (Electrical and Electronic Engineering) in 2001 and 2005, respectively. His research interests include network security and QoS in future generation networks. He is currently a researcher and a lecturer at the Wireless and Photonic Network Research Center of Excellence (WiPNET) at Universiti Putra Malaysia.

Kumudu S. Munasinghe (S’03-M’09) holds a M.Comp. and a M.Sc. (Hons) degree from the University of Western Sydney and a Ph.D. in Telecommunications Engineering from the University of Sydney, Australia. He currently holds the prestigious Australian Postdoctoral Fellowship (APD) awarded by the Australian Research Council (ARC) and attached to the Wireless Networking Group (WiNG) at the University of Sydney. His research primarily focuses on heterogeneous mobile and cellular networks. Kumudu has over 35 refereed technical papers in international journals, conference proceedings, and a book to his credit. He is a TPC member/reviewer for many international conferences and journals and won many research awards and grants including the National ICT Australia Prize for Next Generation Applications and the IEEE Student Award at the 50th Anniversary Global Communications Conference in Washington DC, 2007. Kumudu is a member of the Australian Computer Society.

Abbas Jamalipour (S’86-M’91-SM’00-F’07) holds a PhD from Nagoya University, Japan. He is the author of five books, nine book chapters, and over 200 technical papers, in the field of mobile communications. He is a Fellow of IEICE and IEAust, an IEEE Distinguished Lecturer and a Technical Editor of several scholarly journals including IEEE Communications, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, *ETRI Journal*, as well as a Division Editor for JCN. He was the Editor-in-Chief of the *IEEE Wireless Communications* 2006-2008. He disseminated fundamental concepts of the next generation mobile networks and broadband convergence networks; some are being gradually deployed by industry and adopted by ITU-T. He is currently leading the Wireless Networking Group (WiNG) at the University of Sydney, Australia and has an Adjunct Professorship at three other universities. He has been an organizer or chair in many international conferences including IEEE ICC and GLOBECOM and was the General Chair of the IEEE Wireless Communications and Networking Conference (IEEE WCNC2010). He is the Chair of Communications Switching and Routing Technical Committee, Vice Director of Asia Pacific Board, and a voting member of Conference Boards, Education Board, and Online Contents of the IEEE Communications Society. He has been a reviewer for several international research bodies including the Australian Research Council, NSERC (Canada), NSF (USA), European Science Foundation, Science Foundation (Ireland), and the Kentucky Science and Engineering Foundation’s R&D Excellence Program (USA). He is the recipient of several prestigious awards such as the 2006 IEEE Communications Society Distinguished Contribution to Satellite Communications Award and the 2006 IEEE Communications Society Best Tutorial Paper Award.