Biologically Inspired Security attacks and Defences in the Data plane of Networks

Publication History
Received: 23 January 2015
Accepted: 3 March 2015
Published: 1 April 2015

Citation
Thamayanthi M, Sathesh kumar C. Biologically Inspired Security attacks and Defences in the Data plane of Networks. Discovery, 2015, 30(116), 10-16
Biologically Inspired Security attacks and Defences in the Data plane of Networks

Thamayanthi.M\(^1\)
Computer Science and Engineering
St.Joseph’s College of Engineering and Technology
Thanjavur, India
iamthami@gmail.com

Sathesh kumar.C\(^2\)
Computer Science and Engineering
Vandayar Engineering College
Thanjavur, India
csathiz@gmail.com

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 can be accomplished by integrating existing and emerging access networks via a common Internet Protocol (IP) based platform. 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 networks to identify security attacks, 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. 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.

Keywords — Heterogeneous network security, biologically inspired security, danger theory, epidemiology.

I INTRODUCTION

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. 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: (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 and governing bodies, it has not been the case for the latter. Owing to the boundless communication paradigm in heterogeneous 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.

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 \(\backslash\)external attacks. 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/organisms about the event. Another interesting avenue for inspirations exists in the field of epidemiology, specifically on diseases control strategies. Motivated by these 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.

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

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.

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. 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) and the impact of limited network capacity on quarantine strategy.

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 that a host is allowed to initiate to new machines may reduce the attack rate, without significantly hindering normal communications. 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.

B. Anomaly Inhibition

The lymphatic 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 nonself elements.

III. ANOMALY DETECTION FRAMEWORK

The 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.

A. Anomaly Detection

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.

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. 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) and the impact of limited network capacity on quarantine strategy.

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 that a host is allowed to initiate to new machines may reduce the attack rate, without significantly hindering normal communications. 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.

B. Anomaly Inhibition

The lymphatic 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 nonself elements.

Fig. 1. General interworking framework of heterogeneous networks.

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

III. ANOMALY DETECTION FRAMEWORK

The 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.

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. 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) and the impact of limited network capacity on quarantine strategy.

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 that a host is allowed to initiate to new machines may reduce the attack rate, without significantly hindering normal communications. 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.
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 lymphatic 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.

![Fig. 2. DT principle of the anomaly detection framework.](image)

**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 heterogeneous 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 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 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. 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.

**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 topologies. These heterogeneous traffic flows inherit disparate characteristics due to different 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.

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.

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 $X$ and $Y$ 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,

$$R_{XY}(z) = R_{XY}(-z), \quad \forall z: -log \leq z \leq log,$$

where $log$ is the lag generated from the cross-correlation function. Now, let $d_m$ represents the mirror effect parameter such that,

$$d_m = \frac{1}{2}(R_{XY}(z) - R_{XY}(-z)).$$

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. 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 $A$ 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.

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

1) Intra-network Update: The principal idea of the intranetwork 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 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.

![Fig. 3. Danger Zone creation and CS disseminations in the network.](image)

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. 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

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.

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.

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.

V. EVALUATION

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.

It provides a mechanism to identify the “significance” of the identified anomaly, as well as to further reject false positives in the detection. 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.

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.

B. 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.

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.

VI. CONCLUSION

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.

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