A Chaotic Complexity Measure for Cognitive Machine Classification of Cyber-Attacks on Computer Networks

Muhammad Salman Khan, Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, MB, Canada

Ken Ferens, Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, MB, Canada

Witold Kinsner, Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, MB, Canada

ABSTRACT

Today’s evolving cyber security threats demand new, modern, and cognitive computing approaches to network security systems. In the early years of the Internet, a simple packet inspection firewall was adequate to stop the then-contemporary attacks, such as Denial of Service (DoS), ports scans, and phishing. Since then, DoS has evolved to include Distributed Denial of Service (DDoS) attacks, especially against the Domain Name Service (DNS). DNS based DDoS amplification attacks cannot be stopped easily by traditional signature based detection mechanisms because the attack packets contain authentic data, and signature based detection systems look for specific attack-byte patterns. This paper proposes a chaos based complexity measure and a cognitive machine classification algorithm to detect DNS DDoS amplification attacks. In particular, this paper computes the Lyapunov exponent to measure the complexity of a flow of packets, and classifies the traffic as either normal or anomalous, based on the magnitude of the computed exponent. Preliminary results show the proposed chaotic measure achieved a detection (classification) accuracy of about 98%, which is greater than that of an Artificial Neural Network. Also, contrary to available supervised machine learning mechanisms, this technique does not require any offline training. This approach is capable of not only detecting offline threats, but has the potential of being applied over live traffic flows using DNS filters.

Keywords: Anomaly Detection, Artificial Neural Network, Chaos, Cognitive Machine Learning, Cyber Threats, Data Traffic, DNS, DDoS Amplification, Internet, Lyapunov Exponent, Volterra Series

DOI: 10.4018/IJCINI.2014070104
1. INTRODUCTION

Object classification literature shows that computer software and hardware algorithms are increasingly showing signs of cognition and are necessarily evolving towards cognitive computing machines to meet the challenges of today’s engineering problems (e.g., (Kinsner, Challenges in the design of adaptive, intelligent and cognitive systems, 2009) (Wang, Zhang, & Kinsner, Advances in Cognitive Informatics and Cognitive Computing, 2010) (Xiaonan Wu & Banzhaf, 2010)). For instance, in response to the continual mutating nature of cyber security threats, basic algorithms for intrusion detection are being forced to evolve and develop into autonomous and adaptive agents, in a manner that is emulative of human information processing mechanisms and processes (Kinsner, Towards cognitive security systems, 2012). Indeed, the challenges posed by today’s cyber threats on the security of computing systems and networks requires intelligence beyond that provided by the outdated and ineffectual conventional algorithms (Haykin, Cognitive Dynamic Systems: Perception-Action Cycle, 2012) (Haikonen, 2003) (Modi, et al., 2013). Todays’ object classification researchers are actively investigating ways of increasing the cognitive abilities of computationally intelligent algorithms, such as artificial neural network (ANN), artificial immune system (AIS), evolutionary computing (EC), and particle swarm optimization (PSO) to combat the ever mutating strains of cyber threats (Xiaonan Wu & Banzhaf, 2010). Moreover, researchers are exploring ways in which the mechanisms within the Human Immune System (HIS) can model cyber-threat intrusion detection systems in computer networks (Harmer, Williams, Gunsch, & Lamont, 2002) (Kim, 2003). However, base-line applications of these algorithms still have limitations in performing object classification sufficiently well and are still less efficient than human beings at performing classification (Xiaonan Wu & Banzhaf, 2010). What is missing?

This paper investigates the use of complexity, as a measure of similarity and difference in objects, to help these computationally intelligent algorithms perform the object classification task more reliably. In particular, this paper extends the evolving trend of computationally intelligent algorithms to cognitive machines by introducing measures of object complexity to the computationally intelligent algorithms. This paper applies chaos theory to measure the complexity of Internet packets to determine if they are normal or anomalous, and so, uses computationally intelligent algorithms coupled with chaos theory to develop computer network intrusion detection systems.

Internet and cyber security are major concerns of many people and organizations across the world. Within the last decade, the Internet has become part of everyday life and virtually everything has been connected to the cyber world. Government operations, health services, banking, the economy and individuals are increasingly dependent on cyber technologies. This transformation is an enabling factor for improving the economy and the quality of life of people. However, the increasing dependence on cyber infrastructure has also made good citizens and organizations vulnerable to cybercrimes and threats that include viruses, worms, botnets, denial-of-service attacks, intrusion, data stealing, and insider threats. Contemporary antivirus and firewall technologies are limited to detecting known threats, because they are unable to acquire the knowledge required to identify new and unidentified threats in real-time, such as new generations of smart viruses and threats, which emerge continuously and can evade detection from the contemporary systems. Like bacteria that can generate resistance against a medical drug, the Internet based threats are mutating to evade conventional security and antivirus defenses. With this transmutation of cyber-threats, an evolution of detection strategies is required to detect and thwart these cybercrimes and threats.

Internet application data, such as individual email, Facebook, Yahoo, and general software applications are broken down into a sequence of packets, which are transmitted from source to destination over the Internet. In the past early
Related Content

Measuring the Semantic Relatedness Between Images Using Social Tags
[www.igi-global.com/article/measuring-the-semantic-relatedness-between-images-using-social-tags/101814?camid=4v1a](www.igi-global.com/article/measuring-the-semantic-relatedness-between-images-using-social-tags/101814?camid=4v1a)

Impact of Individual Differences on Web Searching Performance: Issues for Design and the Digital Divide
[www.igi-global.com/chapter/impact-individual-differences-web-searching/6631?camid=4v1a](www.igi-global.com/chapter/impact-individual-differences-web-searching/6631?camid=4v1a)
A Formal Specification of the Memorization Process
www.igi-global.com/chapter/formal-specification-memorization-process/27306?camid=4v1a

Regression-Based Automated Facial Image Quality Model
www.igi-global.com/article/regression-based-automated-facial-image-quality-model/195017?camid=4v1a