ACIT'2017
The International Arab Conference on Information Technology
Yassmine Hammamet, Tunisia
December 22-24, 2017

A proposed framework for Botnet Spam-email Filtering using Neucube

AmmarALmomani
IT-department, Al-Huson University College, Al-Balqa Applied University, P. O. Box 50, Irbid, Jordan
Ammarnav6@bau.edu.jo

Mohammad Alauthman
Department of Computer Science, Faculty of information technology, Zarqa University, Zarqa, Jordan
malauthman@zu.edu.jo

Omar Almomani
Department of Network and Computer Information System
Faculty of Information Technology
The World Islamic Sciences & Education University, Jordan
Omar.almomani@wise.edu.jo

FirasAlbalas
Jordan University of Science And Technology, Irbid-Jordan. P.O.Box 3030. Postal code: 22110.
faalbalas@just.edu.jo

Abstract

The voluminous amount of SPAM emails that originated from different botnets worldwide has a direct effect on the limited capacity of mailboxes, security of personal mail, space-loss from the communication as well as the time that is required to identify and address the spam emails. These issues are crucial to the Internet and Networks OS that need a serious attention from the research community. As a result of such sophistication, attackers employ Botnet infrastructure for distributing spam email messages for malicious purposes. The proposed research will address the source of the above issues through identifying the SPAM emails before causing any further disturbance to the networks normal operations, due to the complexity of spamming techniques which are evolving from traditional spamming technologies (direct spamming) to more sophistication techniques (zero-day spam). Therefore, the proposed Online Botnet Spam E-mail Filtering Framework (BSEFF) uses the principles of a new spiking neural network architecture called Neucube algorithms [1, 2], we will focus on adaptive Dynamic Evolving Spiking Neural Network (deSNN) algorithm. The proposed algorithm is designed to handle large and fast spatio/spectro temporal data through applying the spiking neural networks (SNN) as the core processing module. To the best of our knowledge, the proposed framework can be considered as the first Spam detection approach that utilizes Neucube algorithm. BSEFF will inherit the feature of Neucube algorithm that adopts hybrid (supervised/unsupervised) learning approach, and use this algorithm in an online framework with long life learning inorder to classify input while the framework is learned.

Keywords: ***Botnet Spam-mail, NeuCubealgorithms, spiking neural networks, evolving spatio-temporal data machines (eSTDM)***

I. INTRODUCTION

Spam is not only disturbing, but it is also a problem that requires time and effort from users and administrators. Furthermore, 83% of spam can be consideredas highlydangerous because it can contain a URL to phishing sites and Trojan infections which are just one click away [3-8]. Other shortcomings of the spam emails are the space and time waste of the consumer storage in the servers, therefore, congesting the communication channels and causing adelay of services until the administrator takes some action. Also, some important emails can be wrongly deleted with the huge amount of received spam emails. Spam email is also a well-regard malware carrier in order to infect computers with viruses or deceive users to follow certain links.

According to the recent reports by D. Gudkova et. Al [9] and as reported in McAfee Labs Threats Report on March 2016 [10], during Q4 of 2016, the KelihosBotnet resides a top position which reaches about 95% of its Q3 volume. Besides its famous pharmaceutical spam, Kelihos gained another essenceby means of focusing on the recipients of Chinese who have "job offer" themed campaigns in which the Botnet of type lethic size is growth to be 60% thru Q4, essentially with campaigns which are pushing knock-off designer wristwatches.

The total cost of spam for businesses will grow to $257 billion per year if spam continues to flourish at its current rate[11]. Moreover, in the recent spam report [12] published in March 2011, 83.1% of email spam was received via Botnets. Bots are inexpensive, easy to deploy and difficult to detect, which compensate their Botmasters financially.

Nowadays, spam emails remain the most popular technique used by cybercriminals and the spammers to perform a wide variety of malicious activities.

Problem statements: The issue of botnet spamitself can be expanded and defined as follows:

- Botnet spam attack will consume all resource such as CPU, network and storage.
- The current methods used to distinguish the emails have difficulty in identifying the "zero days" attack[13]. This leads to high level of false positives rates (FPR), and a low degree of accuracy in the classification process.
- Most of the current SPAM detection techniques consume memory, especially during the learning process to detect new spam emails. For example, current machine learning algorithm suffers from difficulties with selecting the structure of the spam email or forgetting previously learned knowledge after further training[5]. The proposed approach, however, will handle the above issues under one solution that operate on online mode.

Proposed objectives: Theultimate aim of this proposed is to build a framework for an evolving stream data mining that leads to improving the classification performance and accuracy in identifying SPAM emails generally and Botnet spam specifically, especially the zero-day attack in an online mode. The proposed approach will achieve its ultimate aim through addressing the following objectives:

General objective

- Study the spam features in the first 3 layer in TCP/IP model to build more accurate framework.
- Minimize the threat of SPAM attack and increase different organization's trust in performing online transactions and other e-commerce businesses.

Specific objectives

- To enhance a learning rateusingan online method that is cost effective and analysed data for more detection accuracy.
- To minimize the memory consumption of the proposed classifier process and to reduce the time needed for dynamically classifying the emails.
- To evaluate the proposed framework detection ability using known benchmark datasets and to compare the obtained results against other approaches in Botnet spam email detection.

Based our proposed Online Botnet Spam E-mail Filtering Framework (BSEFF), we expect to have more accurate frameworkespecially to work with a zero-day attack in Botnet spam filtering framework**.** The rest of the paper is organised as follows: Section 2presents the related works,Sections 3 discuss the proposed methodology and framework prototype, Section 4discuss Expected contributions in the future work.

II.Related works

A number of most often used applications for CutwailspamBot(in the year 2013–2014) include spam email that helps in deploying the Zeus banking malware [14]. Almost three years ago, WaledacBotnet brought back to life through launching a new spamming campaign. The RustockBotnet has also come to the fore where Pharmaceutical emails are detected. The widely-used methods for filtering Botnet spam email are explained below:

Email spamming Botnet detection techniques: Filtering spams is often carried out using email spam filters or some other filtering system [15][16-21]. The importance of filtering for researchers and security administrators can be vital for the production of online data streaming. The filtering methods have limited capability in that they can classify spam of unsolicited email or ham (legitimate email) but cannot track down the whole Botnet emails family.

A. Passive Techniques for Email Spamming Botnet Detection: The passive techniques have limited functions concerned with detecting parts of online data depending on C&C behavior as explained below:

1. **Signature Based Techniques:** They comprise spotting spamming Botnets by means of leveraging malware executable signatures/rules. First, spam signature and fingerprints are created for famous spam context in the payload. Then, such signatures can sort out spams and detect them as in [22],[23],[24].

2. **DNS-Based Techniques**: They depend on commands from command and control centre to deals with bots through DNS queries to spot the IP address. This detection method tries to detect Botnet DNS traffic or queries a monitoring DNS activities and suspiciousbehavior. However, the efforts for exploring

DNS features for detecting spam sending bots and their families are still lacking[25, 26].

3. **Anomaly Based Techniques**: In these techniques, any suspicious email traffic that does not match any predictable normal behavior is closely observed to detect email spamming Botnets. Such detection heavily depends on a number of network anomalies such as network traffic on unusual and unused ports, network latencies, unusual system behaviors or high volumes of traffic for a mid-class network. Here,search is ongoing for the availability of spamming bots in the network. One can have an idea of such approaches in [26-29].

B. Active Techniques for Email Spamming Botnet Detection

Recently, the studied approaches for spamming Botnets rely on actively incorporate spamming Botnet detection in the Botnet operation by means of establishing a client that mimics' C&C protocol. Consequently, after the Botnet participates, the size of the Botnet can be accurately estimated which can take down the whole parts of the Botnet[30]. Accordingly, the categories of the active detection methods can be divided into three classes: 1) Infiltration based, 2) Controlled Environment based, and 3) Sink-holing based [31].

Nowadays, one of the great issues is called "Zero-Day" Botnet spam e-mail. The Zero-Day attack isdefined when the spammer gains anadvantageby using hosts that are not excluded or using techniques that avoid known methods in spam detection [32].Indeed, Botnet spam email is so complex and cannot be easily detected by the conventional methods due to the fact that the Botnet master, can use new unusual vulnerabilities, which have not ever been grasped previously. A number of promising solutions to Botnet spam email have been proposed but have up till now to be proven effective.

Current Artificial Intelligent methods can be employed to detect Botnet spam email based on predefinedfeatures and rules. However, very few machine learning methods are designed to work in online mode. In online mode, data arrive one at a time, and local learning is achieved upon the coming of each datum, and it works when the internet is connected. Conversely, in offline mode, the entire dataset is open for global learning. It should be noted that the error level in the classification process grows over time, particularly when dealing with unknown Zero-Day Botnet spam e-mail[33].Thus we will try to solve this entire problem in our proposed framework.

IIIProposed methodology

Botnet Spam E-mail Filtering Framework (BSEFF) collects and filters e-mails separately and sequentially based on analyzing the network traffic in the online mode. In the proposed framework, Neucube based on evolving Spatio-temporal data machines algorithms [1]is adapted to consider the similarity among many of spam email features, as presented in Figure 1.

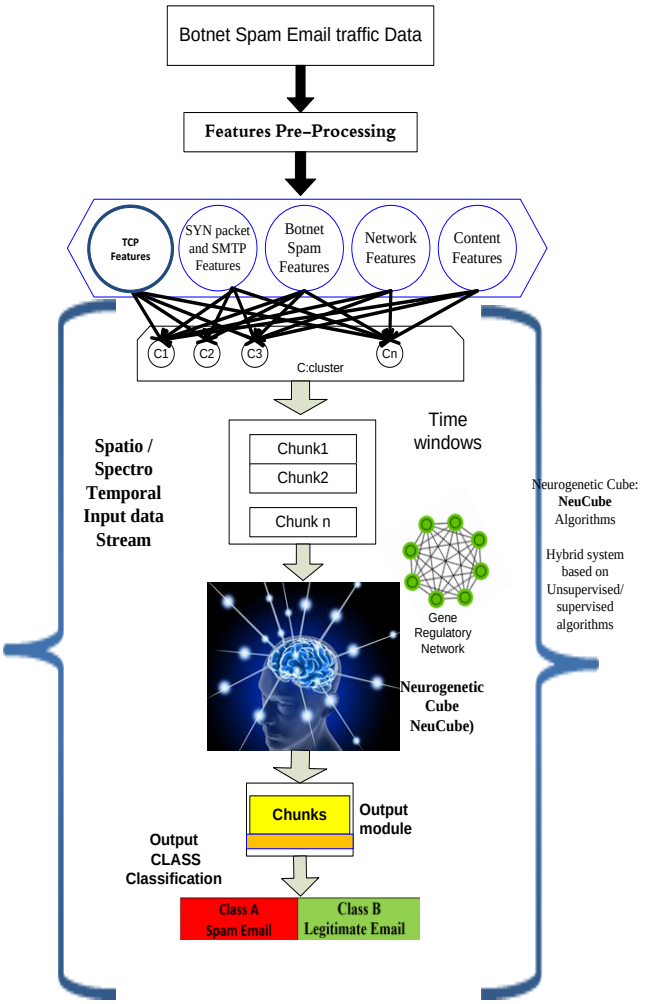

Fig1. Online Botnet SpamE-mail Filtering Framework (BSEFF) usingNeucubealgorithms.

Figure1. visualizes the proposed BSEFFwhichis divided into three consecutive stages and will be sequentially utilized in the first three layers: i) application layer, ii) transport layer, and iii) network layer.

In the *first stage*, data collection and feature extraction are pre-processed. We are concerned with collecting the full content packet traces from the border of the standard email

This phase of thejobsuggested to be implemented on the main controller (main server), with analyzing the full features in each layer as shown in Figure 2.

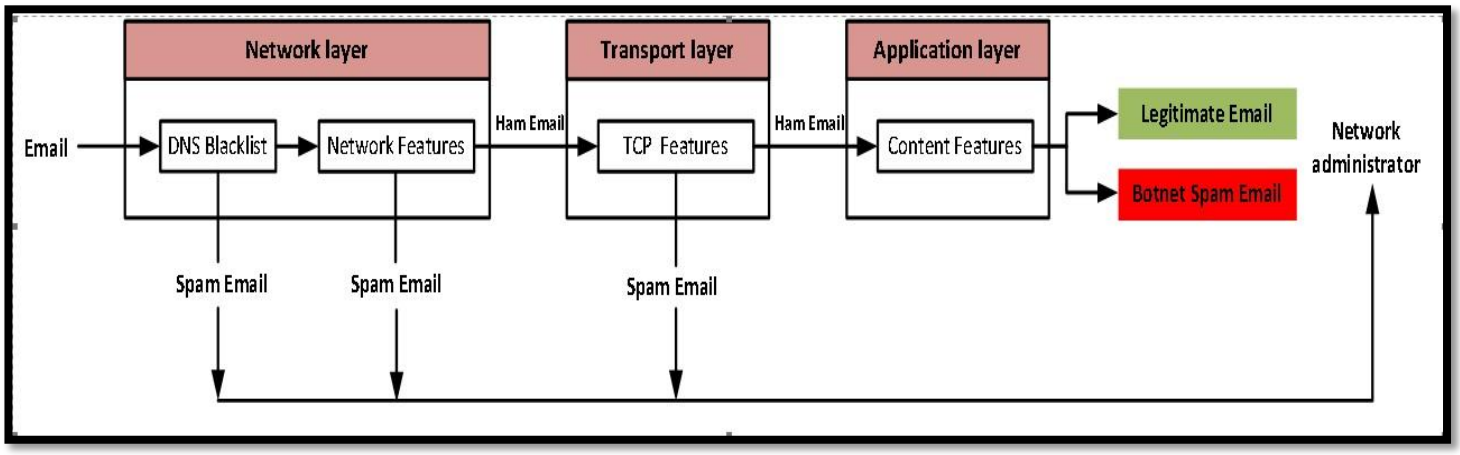

Fig2: The process flow to filter spam email from network layer to application layer

In Figure 2, this part will discuss in more details in extension paper, however each phase focus on some network traffic information. Although this approach is more accurate at botnet spam filtering, it is computationally expensive to apply. In this proposed, we suppose the fourth stage, content filters. Our research investigates the accuracy values between the phases, and then the result used by the fourth phase to support the final decision.

The *second stage* is done by dividing the input data as chunk for training phase in the unsupervised mode. To build cluster mode, which is the best way to work with zero-day attack and to known unlabeled data,

The *third stage* comprises the evolving spatio-temporal data machines (eSTDM) using neuromorphic (Neucube algorithms), brain-like information processing principles (eSTDM)[1]. Which means that the algorithm can classify the activity while it is learning. So it is good for long life learning,with the unstopped system.

However**,** Neucupe algorithms depend on Spiking neural networks (SNNs)generally and Dynamic evolving Spiking Neural Network (deSNN) specifically: SNNscome into the third generation of the neural network by increasing the level of naturalness in a neural simulation [34]. Besides to the neuronal and synaptic state, SNNs also combine the principle of time into their model.In addition, temporal and spatial data can be encoded in an SNN based on the positions of synapses and neurons and time of their spiking activity respectively. SNN may be divided into two main classes (1) Spike-Time-Dependent-Plasticity (STDP) [35]. (2) Spike Driven Synaptic Plasticity (SDSP) [36].

Finally, the framework will be able to classify the input traffic information as legitimate email or malicious spam email.

Botnet Spam E-mail Filtering Framework (BSEFF) in our proposed classifier to tackle the problem. In each stage, our BSEFF will detect and do away with a ‘‘sure spam’’ while another deals with ‘‘sure ham’’ messages and transfer them to the user's emails. Thus the number of uncertain messages will be minimized in the next stage. It should be noted that this pipeline is mainly a conceptual framework which may vary with reference to techniques and other considerations such as storage cost and operational efficiency[37]. Neucupe algorithms worked based on deSNN algorithm to build a hybrid (supervised/unsupervised) learning approach, to detect

the Botnet spam email dynamically included unknown zero-day attack before it gets to theuser account. So that BSEFF is suggested to work for high-speed "life-long" learning with low memory footprint.

IVExpected contributions in the future work.

The problem of Spam emails has been significantly developed over the last decade. The problem itself is not only affecting end users, but also small enterprises might become a victim of such scams that may lead to other attacks. This is due to the complexity of spamming techniques which are evolving from traditional spamming technologies (direct spamming) to more sophistication techniques (zero-day spam). The main expected contribution of this proposalis the Online Botnet SpamE-mail Filtering framework Based on Dynamic Evolving Spiking Neural Networks Architecture (BSEFF) which will adopts the hybrid (supervised/unsupervised) learning approach. This framework expected to have many sub-contributions in the field of SpamBotnet email detection as follows:

1. Adaptive online is enhanced by offline learning to build life-long learning system able to dynamically detect the Zero-Day spam Botnet e-mails without prior knowledge of the spamBotnet e-mail itself.
2. Achieves high detection performance which including a high level accuracy.
3. Save money on most Servers of institutions and companies based on filtering storage, memory and time from Botnet spam email.

The future work will discuss the stages of proposed in full details and mathematically how it does it work to detect zero day attack compare with other algorithms and try to build real time implementation.

ACKNOWLEDGEMENT:
This work was supported by Faculty of Information Technology, The World Islamic Sciences & Education University, Jordan, and Al-Balqa Applied University, Al-Huson University College, Dept. of Information Technology, 50, Irbid, Jordan.

References :

[1] N. Kasabov, N. M. Scott, E. Tu, S. Marks, N. Sengupta, E. Capecci, *et al.*, "Evolving spatio-temporal data machines based on the NeuCube neuromorphic framework: design methodology and selected applications," *Neural Networks*, vol. 78, pp. 1-14, 2016.

[2] E. Capecci, N. Kasabov, and G. Y. Wang, "Analysis of connectivity in NeuCube spiking neural network models trained on EEG data for the understanding of functional changes in the brain: A case study on opiate dependence treatment," *Neural Networks*, vol. 68, pp. 62-77, 2015/08/01/ 2015.

[3] D. Schatzmann, M. Burkhart, and T. Spyropoulos, "Inferring spammers in the network core," in *International Conference on Passive and Active Network Measurement*, 2009, pp. 229-238.

[4] K. Al-Saedi, A. ALnajjar, and S. Ramadass, "A survey of Learning Based Techniques of Phishing Email Filtering."

[5] A. Almomani, A. Obeidat, K. Alsaedi, M. A.-H. Obaida, and M. Al-Betar, "Spam E-mail filtering using ECOS algorithms," *Indian Journal of Science and Technology*, vol. 8, pp. 260-272, 2015.

[6] R. M. Saad, A. Almomani, A. Altaher, B. Gupta, and S. Manickam, "ICMPv6 flood attack detection using DENFIS algorithms," *Indian Journal of Science and Technology*, vol. 7, pp. 168-173, 2014.

[7] A. Almomani, T.-C. Wan, A. Manasrah, A. Altaher, M. Backlizet, and S. Ramadas, "An enhanced online phishing e-mail detection framework based on evolving connectionist system," *International Journal of Innovative Computing, Information and Control (IJICIC)*, vol. 9, pp. 169-175, 2013.

[8] A. Almomani, B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *IEEE communications surveys & tutorials*, vol. 15, pp. 2070-2090, 2013.

[9] D. Gudkova, M. Vergelis, N. Demidova, and T. Shcherbakova, "Spam and phishing in Q3 2016," *AO Kapersky Lab*, 2016.

[10] B. Cruz, D. Gupta, A. Kapoor, L. Haifei, D. McLean, and F. Moreno, "McAfee Labs Threats

Report – March 2016," *McAfee Inc., Santa Clara, CA,*, 2016.

[11] s. laws. (2016, 25-1-2017). *Spam Statistics and Facts*. Available: http://www.spamlaws.com/spam-stats.html

[12] W. Z. Khan, M. K. Khan, F. T. B. Muhaya, M. Y. Aalsalem, and H.-C. Chao, "A Comprehensive Study of Email Spam Botnet Detection," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 2271-2295, 2015.

[13] A. Almomani, B. Gupta, T.-c. Wan, A. Altaher, and S. Manickam, "Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email," *arXiv preprint arXiv:1302.0629*, 2013.

[14] TrustWave. *Spam statistics*. Available: https://www3.trustwave.com/support/labs/spam_statistics.asp

[15] A. Brodsky and D. Brodsky, "A Distributed Content Independent Method for Spam Detection," *HotBots*, vol. 7, pp. 3-3, 2007.

[16] R. Beverly and K. Sollins, "Exploiting transport-level characteristics of spam," 2008.

[17] A. Sperotto, G. Vliek, R. Sadre, and A. Pras, "Detecting spam at the network level," in *Meeting of the European Network of Universities and Companies in Information and Communication Engineering*, 2009, pp. 208-216.

[18] M. Ye, T. Tao, F.-J. Mai, and X.-H. Cheng, "A spam discrimination based on mail header feature and SVM," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*, 2008, pp. 1-4.

[19] C.-H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," *Expert Systems with Applications*, vol. 36, pp. 4321-4330, 2009.

[20] J.-J. Sheu, "An Efficient Two-phase Spam Filtering Method Based on E-mails Categorization," *IJ Network Security*, vol. 9, pp. 34-43, 2009.

[21] L. H. Gomes, C. Cazita, J. M. Almeida, V. Almeida, and W. Meira Jr, "Characterizing a spam traffic," in *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, 2004, pp. 356-369.

[22] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, and I. Osipkov, "Spamming botnets: signatures and characteristics," *ACM SIGCOMM Computer Communication Review*, vol. 38, pp. 171-182, 2008.

[23] L. Zhuang, J. Dunagan, D. R. Simon, H. J. Wang, I. Osipkov, and J. D. Tygar, "Characterizing Botnets from Email Spam Records," *LEET*, vol. 8, pp. 1-9, 2008.

[24] T. Mori, H. Esquivel, A. Akella, A. Shimoda, and S. Goto, "Understanding large-scale spamming botnets from internet edge sites," in *Proceedings of the Conference on E-Mail and Anti-Spam (CEAS)(Redmond, WA*, 2010.

[25] A. Ramachandran, N. Feamster, and D. Dagon, "Revealing Botnet Membership Using DNSBL Counter-Intelligence," *SRUTI*, vol. 6, pp. 49-54, 2006.

[26] W. K. Ehrlich, A. Karasaridis, D. A. Hoeflin, and D. Liu, "Detection of Spam Hosts and Spam Bots Using Network Flow Traffic Modeling," in *LEET*, 2010.

[27] P. Sroufe, S. Phithakkitnukoon, R. Dantu, and J. Cangussu, "Email shape analysis for spam botnet detection," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, 2009, pp. 1-2.

[28] O. Tsigkas, O. Thonnard, and D. Tzovaras, "Visual spam campaigns analysis using abstract graphs representation," in *Proceedings of the ninth international symposium on visualization for cyber security*, 2012, pp. 64-71.

[29] P.-C. Lin, P.-H. Lin, P.-R. Chiou, and C.-T. Liu, "Detecting spamming activities by network monitoring with Bloom filters," in *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, 2013, pp. 163-168.

[30] D. Mónica and C. Ribeiro, "Leveraging Honest Users: Stealth Command-and-Control of Botnets," in *WOOT*, 2013.

[31] Z. Li, J. Hu, Z. Hu, B. Wang, L. Tang, and X. Yi, "Measuring the botnet using the second

character of bots," *JNW*, vol. 5, pp. 98-105, 2010.

[32] A. Almomani, "Fast-flux hunter: a system for filtering online fast-flux botnet," *Neural Computing and Applications*, pp. 1-11, 2016.

[33] Symante, "Internet security threat report," 2016.

[34] S. Ghosh-Dastidar and H. Adeli, "Third Generation Neural Networks: Spiking Neural Networks," in *Advances in Computational Intelligence*, W. Yu and E. N. Sanchez, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 167-178.

[35] S. Song, K. D. Miller, and L. F. Abbott, "Competitive Hebbian learning through spike-timing-dependent synaptic plasticity," *Nat Neurosci*, vol. 3, pp. 919-926, 09//print 2000.

[36] S. Fusi, M. Annunziato, D. Badoni, A. Salamon, and D. J. Amit, "Spike-driven synaptic plasticity: theory, simulation, VLSI implementation," *Neural computation*, vol. 12, pp. 2227-2258, 2000.

[37] D. Sona, S. Veeramachaneni, E. Olivetti, and P. Avesani, "Inferring Cognition from fMRI Brain Images," in *Artificial Neural Networks – ICANN 2007: 17th International Conference, Porto, Portugal, September 9-13, 2007, Proceedings, Part II*, J. M. de Sá, L. A. Alexandre, W. Duch, and D. Mandic, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 869-878.