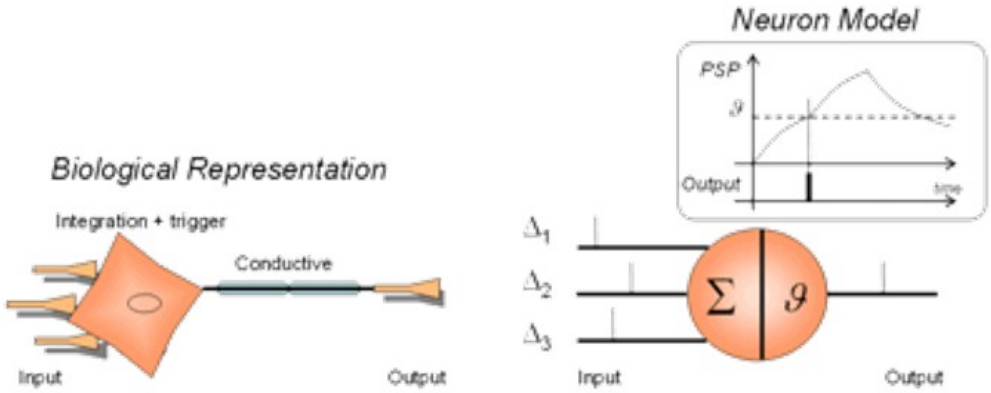
Spiking Neural Networks

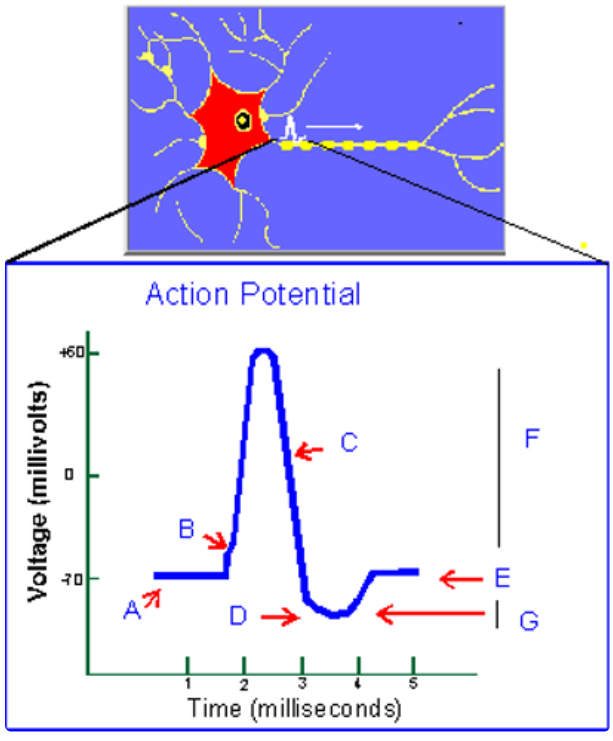
Subjects: Computer Science, Artificial Intelligence
Contributor: Konstantinos Demertzis

Spiking neural networks (SNNs) are artificial neural network models that more closely mimic natural neural networks. In addition to neuronal and synaptic state, SNNs also incorporate the concept of time into their operating model. The idea is that neurons in the SNN do not fire at each propagation cycle (as it happens with typical multi-layer perceptron networks), but rather fire only when a membrane potential – an intrinsic quality of the neuron related to its membrane electrical charge – reaches a specific value. When a neuron fires, it generates a signal which travels to other neurons which, in turn, increase or decrease their potentials in accordance with this signal (ref (https://en.wikipedia.org/wiki/Spiking_neural_network)).

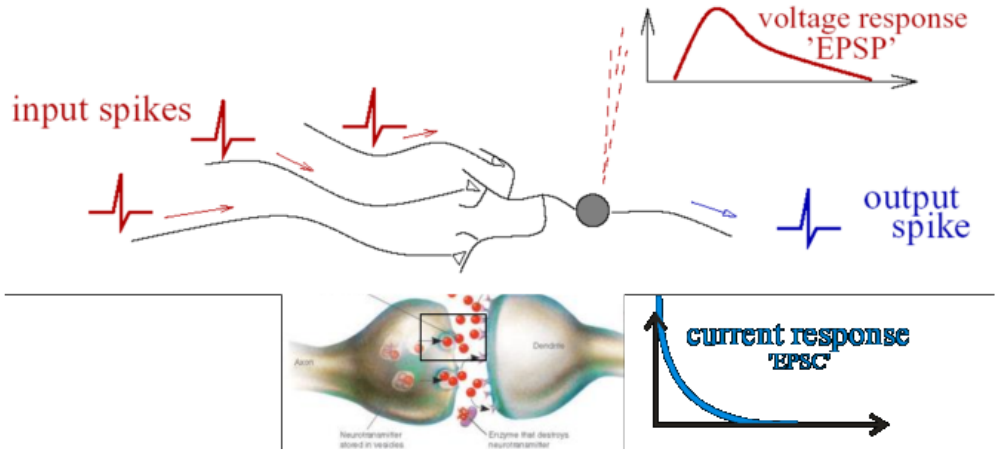
Keywords: Spiking ; Neural Network ; Membrane ; Machine Learning ; Artificial Intelligence



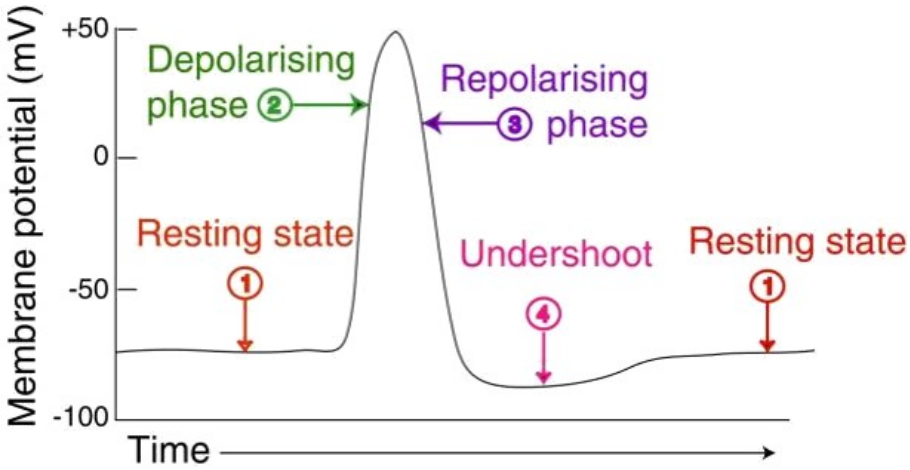
A typical spiking neuron model consists of dendrites, which simulate the input level of the network, which collects signals from other neurons and transmits them to the next level, which is called Soma. The soma is the process level at which when the input signal passes a specific threshold, an output signal is generated. The output signal is taken from the output level called the axon, which delivers the signal (short electrical pulses called action potentials or spike train) to be transferred to other neurons. A spike train is a sequence of stereotyped events generated at regular or irregular intervals [1].



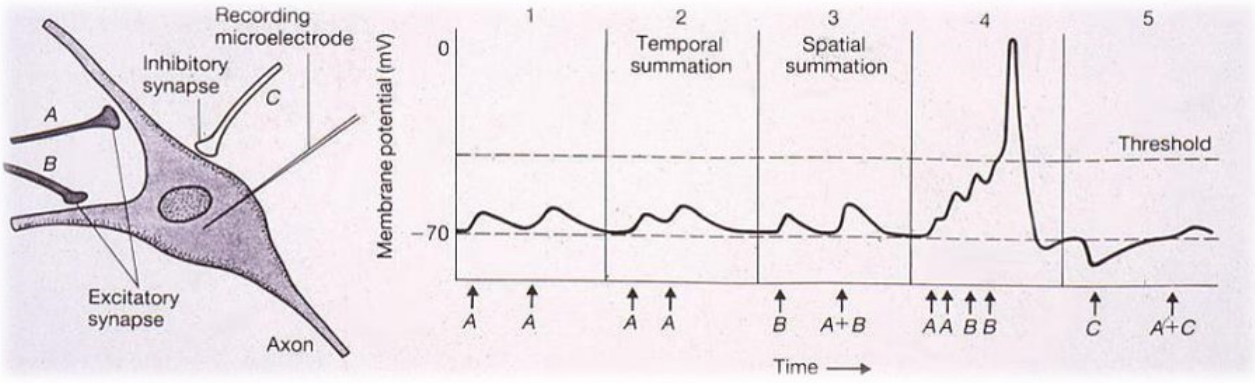
Typically, the spikes have an amplitude of about100 mV and a duration of 1-2 ms. Although the same elements exist in a linear perceptron, the main difference between a linear perceptron and a spiking model is the action potential generated during the stimulation time [2].



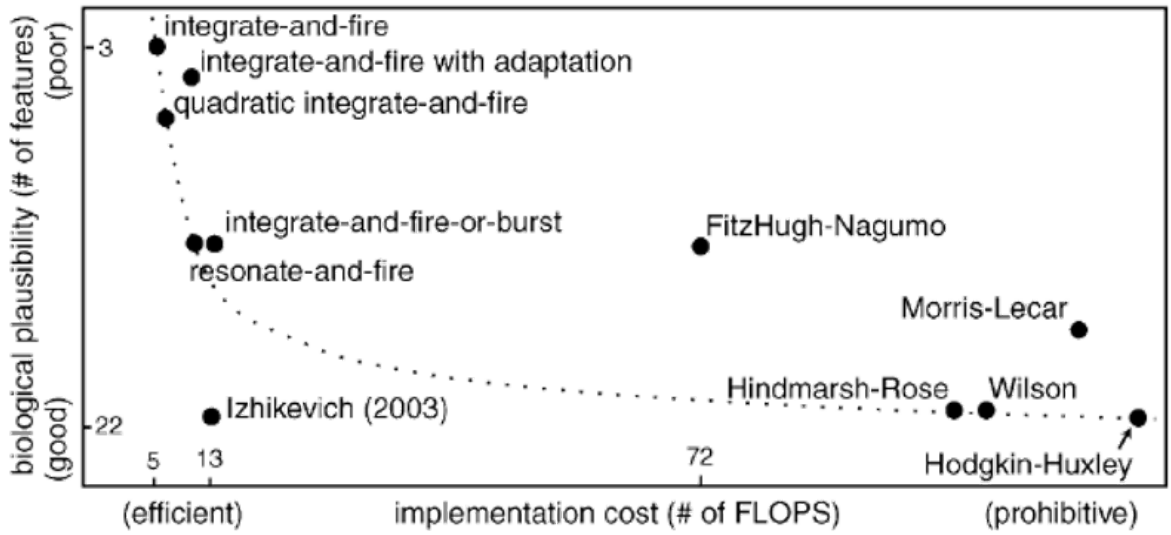
Furthermore, the activation function used in spiking models is a differential equation that tries to model the dynamic properties of a biological neuron in terms of spikes. The form of the spike does not carry any information, and what is important is the number and the timing of spikes [3].



The shortest distance between two spikes defines the absolute refractory period of the neuron that is followed by a phase of relative refractoriness where it is difficult to generate a spike [4].



Several spiking models have been proposed in the last years aiming to model different neurodynamic properties of neurons. Among these models, we could mention the well-known integrate-and-fire model, resonate-and-fire and Hodgkin-Huxley model [5].



Bio-inspired machine learning (like SNNs) and bio-inspired optimization algorithms are recognized in artificial intelligence to address optimal solutions of complex problems in information science and engineering [6][7][8][9]. However, cybersecurity problems are usually nonlinear and restricted to multiple nonlinear constraints that propose many problems such as time requirements and high dimensionality to find an optimal solution[10][11][12][13][14]. To tackle these problems, recent trends have tended to apply bio-inspired machine learning and bio-inspired optimization algorithms in hybrid frameworks that represent a promising approach for solving complex cybersecurity problems[15][16][17][18].

References

1. Lazaros Iliadis; Konstantinos Demertzis; Detecting invasive species with a bio-inspired semi-supervised neurocomputing approach: the case of Lagocephalus sceleratus. *Neural Computing and Applications* **2016**, *28*, 1225-1234, 10.1007/s00521-016-2591-2.
2. Konstantinos Demertzis; Lazaros Iliadis; A Hybrid Network Anomaly and Intrusion Detection Approach Based on Evolving Spiking Neural Network Classification. *Communications in Computer and Information Science* **2014**, *441*, 11-23, 10.1007/978-3-319-11710-2_2.
3. Konstantinos Demertzis; Lazaros Iliadis; Evolving Computational Intelligence System for Malware Detection. *Trends in Enterprise Architecture Research* **2014**, *178*, 322-334, 10.1007/978-3-319-07869-4_30.
4. Konstantinos Demertzis; Lazaros Iliadis; Evolving Smart URL Filter in a Zone-Based Policy Firewall for Detecting Algorithmically Generated Malicious Domains. *Human Centered Computing* **2015**, *9047*, 223-233, 10.1007/978-3-319-17091-6_17.
5. Konstantinos Demertzis; Lazaros Iliadis; A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security. *Computation, Cryptography, and Network Security* **2015**, *1*, 161-193, 10.1007/978-3-319-18275-9_7.
6. Ilias Bougoudis; Konstantinos Demertzis; Lazaros Iliadis; Vardis-Dimitris Anezakis; Antonios Papaleonidas; Semi-supervised Hybrid Modeling of Atmospheric Pollution in Urban Centers. *Communications in Computer and Information Science* **2016**, *629*, 51-63, 10.1007/978-3-319-44188-7_4.
7. Ilias Bougoudis; Konstantinos Demertzis; Lazaros Iliadis; Vardis-Dimitris Anezakis; Antonios Papaleonidas; FuSSFFra, a fuzzy semi-supervised forecasting framework: the case of the air pollution in Athens. *Neural Computing and Applications* **2017**, *29*, 375-388, 10.1007/s00521-017-3125-2.
8. Konstantinos Demertzis; Lazaros S. Iliadis; Vardis-Dimitris Anezakis; Extreme deep learning in biosecurity: the case of machine hearing for marine species identification. *Journal of Information and Telecommunication* **2018**, *2*, 492-510, 10.1080/24751839.2018.1501542.
9. Vardis-Dimitris Anezakis; Lazaros Iliadis; Konstantinos Demertzis; Georgios Mallinis; Ioannis M. Dokas; Narjès Bellamine-Ben Saoud; Julie Dugdale; Paloma Díaz; Hybrid Soft Computing Analytics of Cardiorespiratory Morbidity and Mortality Risk Due to Air Pollution. *Trends in Enterprise Architecture Research* **2017**, *301*, 87-105, 10.1007/978-3-319-67633-3_8.
10. Konstantinos Demertzis; Lazaros S. Iliadis; Vardis-Dimitrios Anezakis; An innovative soft computing system for smart energy grids cybersecurity. *Advances in Building Energy Research* **2017**, *10*, 1-22, 10.1080/17512549.2017.1325401.

11. Konstantinos Demertzis; Panayiotis Kikiras; Nikos Tziritas; Salvador Llopis Sanchez; Lazaros Iliadis; The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence. *Big Data and Cognitive Computing* **2018**, *2*, 35, 10.3390/bdcc2040035.
12. Konstantinos Demertzis; Nikos Tziritas; Panayiotis Kikiras; Salvador Llopis Sanchez; Lazaros Iliadis; The Next Generation Cognitive Security Operations Center: Adaptive Analytic Lambda Architecture for Efficient Defense against Adversarial Attacks. *Big Data and Cognitive Computing* **2019**, *3*, 6, 10.3390/bdcc3010006.
13. Konstantinos Rantos; George Drosatos; Konstantinos Demertzis; Christos Ilioudis; Alexandros Papanikolaou; Antonios Kritsas; ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology. *Human Centered Computing* **2019**, *1*, 300-313, 10.1007/978-3-030-12942-2_23.
14. Konstantinos Rantos; George Drosatos; Konstantinos Demertzis; Christos Ilioudis; Alexandros Papanikolaou; Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem. *International Conference on Security and Cryptography* **2018**, *1*, 572-577, 10.5220/0006911005720577.
15. Konstantinos Demertzis; Lazaros Iliadis; SAME: An Intelligent Anti-malware Extension for Android ART Virtual Machine. *Human Centered Computing* **2015**, *9330*, 235-245, 10.1007/978-3-319-24306-1_23.
16. Konstantinos Demertzis; Lazaros Iliadis; Bio-inspired Hybrid Intelligent Method for Detecting Android Malware. *Modelling and Simulation in Management Sciences* **2016**, *416*, 289-304, 10.1007/978-3-319-27478-2_20.
17. Konstantinos Demertzis; Lazaros Iliadis; Vardis-Dimitris Anezakis; MOLESTRA: A Multi-Task Learning Approach for Real-Time Big Data Analytics. *2018 Innovations in Intelligent Systems and Applications (INISTA)* **2018**, *1*, 1-8, 10.1109/inista.2018.8466306.
18. Lazaros Iliadis; Vardis-Dimitris Anezakis; Konstantinos Demertzis; Stefanos Spartalis; Hybrid Soft Computing for Atmospheric Pollution-Climate Change Data Mining. *Lecture Notes in Computer Science* **2018**, *1*, 152-177, 10.1007/978-3-319-99810-7_8.
