Literature Review: Enhancing IoT Security with Analog AI-Based Host-Based Intrusion Detection and Prevention Systems

Hadi Saghir

Computer and Information Science

2023

Introduction

Background

Internet of Things (IoT) refers to a network of everyday devices that communicate and exchange data, using both high and low power wireless networks [1]. When it comes to low-power wireless networks like Zigbee and Bluetooth, the IoT is particularly susceptible to network security issues, rendering IoT devices vulnerable to threats like illegal access or denial-of-service (DoS) [2].

With the increasing sophistication of attacks and the constant evolution of threats rendering traditional signature-based approaches inadequate and costly [2,3], this prompted a new security concern. To address this concern, researchers have been exploring, amongst other solutions, machine learning-based Host-Based Intrusion Detection and Prevention Systems (HIDPS) [3]. These systems detect and prevent attacks by monitoring system logs and network traffic of the host machine. However, developing effective HIDPS presents unique challenges as IoT devices often have limited computing power, memory, and diverse architectures.

One possible solution to overcome these challenges is using analog artificial intelligence (analog AI). Analog AI is an emerging field of artificial intelligence that leverages analog computing techniques to perform machine learning tasks [4]. Traditional digital computing requires large amounts of data processing, storage, and energy consumption, which is often not feasible with the physical constraints found in IoT devices. Analog AI, on the other hand, can perform the same computations with low energy consumption and higher speeds in exchange for less scalability, less flexibility, and less precision.

[5] have developed an effective analog machine learning HIDPS with a memristor hardware simulation, evaluated in real-time with a final detection accuracy of 89.72%. In addition, the research claimed successful energy and space efficiency. Analog AI can work in tandem with digital computing, providing a more efficient and accurate solution to IoT security challenges without overloading the device's memory or computing power.

Problem

While machine learning based HIDPS have shown promise in improving the security of IoT devices, their effectiveness is limited by the device's computing power, memory, and diverse architectures. Exploring the use of analog AI in tandem with digital AI could be beneficial in handling machine learning for efficient and effective HIDPS.

This hybrid approach could allow for more complex machine learning algorithms to operate in real-time could enhance the responsiveness of the HIDPS implemented on IoT devices, which face the issue of limited computing power, memory, and diverse architectures.

Research questions

1. What effect does analog AI's integration have on the efficiency, effectiveness, and compactness of IoT devices in regard to machine learning capabilities?
2. How can we leverage analog AI to develop machine learning based HIDPS for IoT devices?
    a. What are the opportunities and benefits of analog AI in overcoming the challenges of developing effective HIDPS for low-power wireless networks?
    b. What are the limitations and challenges of analog AI in IoT security, and how can they be addressed?

Methodology

The research questions require a comprehensive and structured analysis of existing literature to identify the state of knowledge and potential gaps in a particular field [6]. It is particularly useful when the research question involves synthesizing information from multiple studies to arrive at a more robust conclusion in a novel, niche topic [7]. The systematic literature review approach was chosen to provide a comprehensive and reliable overview of the state of research on machine learning based HIDPS for IoT devices, including their benefits, limitations, and potential applications.

In contrast, a Design and Creation Research (DCR) allows conducting original research to collect new data and test the postulated hypothesis, such as ones brought forward in this study [6]. This will allow us to quantitatively compare the effectiveness and efficiency of developing digital AI

and analog AI based machine learning based HIDPS for IoT devices. However, the resource-intensive nature of developing an analog AI machine learning-based HIDPS made it infeasible to conduct DCR within the constraints of this research project.

Systematic literature Review

The search queries used in this research are as follows:

1. "Analog" AND "machine learning" AND "IoT" OR “Internet of Things”
2. "Analog" AND ("IoT" OR “Internet of Things”)
3. ("Analog AI" OR "Digital AI") AND ("HIDS" OR "HIPS" OR "intrusion detection" OR "intrusion prevention")
4. "Machine learning" AND "IoT" AND ("HIDS" OR "HIPS" OR "intrusion detection" OR "intrusion prevention")

Screening and selection

The screening method for this study will be separated into two phases: titles and abstracts in the first phase, and full-text papers in the second. The material will be screened to determine if they meet the inclusion criteria, which is as follows:

- Studies that focus on the use of analog AI in IoT security.
- Studies that focus on the use of analog AI in machine learning.
- Studies that discuss machine learning based HIDPS for IoT devices.
- Studies that provide empirical evidence regarding the effectiveness and efficiency of analog AI in HIDPS.
- Studies that address the limitations and challenges of developing effective HIDPS for low-power wireless networks.
- Studies that are published in English.
- Studies that are peer-reviewed.
- Studies that are relevant to research questions.

Data analysis

In the data analysis, the literature to be included in the study is studied with a focus on information that is considered relevant to answer the research question about the use of analog AI machine learning for HIDPS in IoT devices. Information will be divided into the following categories: analog AI techniques and features, comparison of digital and analog AI techniques and features, and the potential application in HIDPS for IoT devices. The analysis of the literature content will

provide an overview of the potential opportunities and benefits as well as limitations and challenges anticipated in the development of analog AI machine learning based HIDPS for IoT devices.

Literature Review

This literature review will employ the systematic literature review method described above. However, due to constraints in scope of this literature review, the literature will provide an overview rather than a comprehensive understanding of the current state of research on the topic of analog machine learning for HIDPS in IoT devices.

In [2], a HIDS/HIPS using lightweight convolutional neural networks (CNN) was developed. The authors used a digital GTX1650Ti and a core I7-10750H to train the model and achieved good results with an accuracy of 99.23% in 2 hours and 10 minutes and 150 epochs. However, the high-power consumption of digital AI-based systems limits their use in resource-constrained edge devices.

Analog AI offers a promising solution to address the power consumption limitations of digital AI. In [8], the authors compare analog and digital AI for processing ultra-low power. Analog AI is shown to be up to 30 times more efficient than digital AI, making it an attractive option for IoT security. Additionally, neuromorphic computing is a type of analog AI that mimics the structure and function of the human brain, offering new opportunities for efficient and effective HIDS/HIPS on IoT devices.

Memory Resistors (Memristor) crossbar arrays are passive electronic component that can change their resistance based on the amount of current that flows through them, making them useful for memory storage and are also a promising solution for developing neuromorphic computing. In [9], on-chip training of memristors for embedded neural networks-based systems was proposed. This approach achieved higher throughput, lower energy consumption, and higher tolerance to

variations and faults. In [10], a 14nm Multiply-Accumulate (MAC) chip was developed, which utilizes multiple 512*512 wide arrays of phase-change memory (PCM) while managing parallel operations at the location of the data. This chip provides a promising solution for analog AI-based HIDS/HIPS on IoT devices, with benefits in terms of space and area. However, there are limitations to large-scale systems, and the lack of an analog-to-digital converter (ADC) limits the flexibility of these systems. In [11], a ReSe2-based resistive random-access memory (RRAM) and circuit-level model for neuromorphic computing were developed, resulting in a 600mm2 device with 130,000 artificial neurons.

Overall, analog AI offers several opportunities and benefits for IoT security. However, there are still challenges and limitations that need to be addressed. The use of accelerators and specialized architectures, as proposed in [12], is a promising direction for improving the efficiency and performance of analog AI-based HIDS/HIPS for IoT security. The advancements in nonvolatile memories (NVM) also facilitate rapid progress in this field, as shown in [13].

One of the main limitations of analog AI highlighted in [8] is its accuracy and noise tolerance. However, this also proposes a hybrid approach that combines the strengths of both analog and digital processing to achieve better performance.

In addition, [14] stresses the importance of analog processing in machine learning applications but highlights that it poses challenges for designers of analog processors due to bias scalability. [15] discusses the need for scalability and flexibility in designing HIDS for IoT environments, while [16] proposes a new framework for federated learning-based intrusion detection that leverages analog computing to achieve these requirements.

The potential advantages of using analog computing for intrusion detection are also highlighted in [19], which discusses the limitations of traditional HIDS approaches. Moreover, [9] proposes a method for on-chip training of deep neural networks using memristor-based analog computing, which could be advantageous for resource-constrained edge devices. Overall, theses contribute to the ongoing discussion on

Although there is currently no direct research on the use of analog AI for HIDS/HIPS in IoT, it is important to recognize its potential advantages, such as increased efficiency, lower power consumption, and improved accuracy. This suggests that further investigation could be crucial for the next generations of IoT devices. The lack of research in analog AI for HIDS/HIPS in IoT could be attributed to multiple factors, such as the complexity of implementation and the novelty of the technology that make it a feasible option. However, significant research has been conducted on analog AI, its integration with digital AI in IoT security, and its use in related fields, such as network intrusion detection systems. Nevertheless, more research is needed to investigate its potential for HIDS/HIPS in IoT. It is important to recognize the importance of HIDS as an essential component in ensuring the security of a system, providing real-time monitoring, and valuable forensic information in the event of a security incident.

Bibliography

[1] W. A. Jabbar, H. K. Shang, S. N. Hamid, A. A. Almohammedi, R. M. Ramli, and M. A. Ali, "IOT-BBMS: Internet of things-based Baby Monitoring System for smart cradle," *IEEE Access*, vol. 7, pp. 93791–93805, 2019.

[2] D. Lightbody, D.-M. Ngo, A. Temko, C. Murphy, and E. Popovici, “Host-based intrusion detection system for IOT using Convolutional Neural Networks,” *2022 33rd Irish Signals and Systems Conference (ISSC)*, 2022.

[3] D. Kapil, N. Mehra, A. Gupta, S. Maurya, and A. Sharma, “Network security: Threat model, attacks, and ids using machine learning,” *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, 2021.

[4] G. Pedretti, P. Mannocci, C. Li, Z. Sun, J. P. Strachan, and D. Ielmini, “Redundancy and analog slicing for precise in-memory machine learning—part I: Programming techniques,” *IEEE Transactions on Electron Devices*, vol. 68, no. 9, pp. 4373–4378, 2021.

[5] M. S. Alam, C. Yakopcic, G. Subramanyam, and T. M. Taha, “Memristor based neuromorphic network security system capable of online incremental learning and anomaly detection,” *2020 11th International Green and Sustainable Computing Workshops (IGSC)*, 2020.

[6] A. Battal, G. Afacan Adanır, and Y. Gülbahar, “Computer science unplugged: A systematic literature review,” Journal of Educational Technology Systems, vol. 50, no. 1, pp. 24–47, 2021.

[7] M. Hammond and J. Wellington, Research Methods: the Key Concepts, New York: Taylor & Francis Group, 2012.

[8] S. Marzetti, V. Gies, V. Barchasz, H. Barthelemy, and H. Glotin, “Comparing analog and digital processing for ultra low-power embedded artificial intelligence,” 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), 2022. doi:10.1109/iotais56727.2022.9975931

[9] R. Hasan, T. M. Taha, and C. Yakopcic, “On-chip training of memristor based Deep Neural Networks,” 2017 International Joint Conference on Neural Networks (IJCNN), 2017. doi:10.1109/ijcnn.2017.7966300

[10] P. Narayanan, S. Ambrogio, A. Okazaki, K. Hosokawa, H. Tsai, A. Nomura, T. Yasuda, C. Mackin, S. C. Lewis, A. Friz, M. Ishii, Y. Kohda, H. Mori, K. Spoon, R. Khaddam-Aljameh, N. Saulnier, M. Bergendahl, J. Demarest, K. W. Brew, V. Chan, S. Choi, I. Ok, I. Ahsan, F. L. Lie, W. Haensch, V. Narayanan, and G. W. Burr, “Fully on-chip mac at 14 nm enabled by accurate row-wise programming of PCM-based weights and parallel vector-transport in duration-format,” IEEE Transactions on Electron Devices, vol. 68, no. 12, pp. 6629–6636, 2021.

[11] Y. Huang et al., “Rese2-based RRAM and circuit-level model for neuromorphic computing,” Frontiers in Nanotechnology, vol. 3, 2021. doi:10.3389/fnano.2021.782836

[12] D.-M. Ngo, D. Lightbody, A. Temko, C. Pham-Quoc, N.-T. Tran, C. C. Murphy, and E. Popovici, “HH-nids: Heterogeneous hardware-based network intrusion detection framework for IOT Security,” Future Internet, vol. 15, no. 1, p. 9, 2022.

[13] M. Rafiq, S. S. Parihar, Y. S. Chauhan, and S. Sahay, “Efficient implementation of Max-pooling algorithm exploiting history-effect in Ferroelectric-FinFETs,” IEEE Transactions on Electron Devices, vol. 69, no. 11, pp. 6446–6452, 2022. doi:10.1109/ted.2022.3207114

[14] P. Kumar, A. Nandi, S. Chakrabartty, and C. S. Thakur, “Bias-scalable near-memory CMOS analog processor for machine learning,” IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 13, no. 1, pp. 312–322, 2023. doi:10.1109/jetcas.2023.3234570

[15] K. Mittal and P. K. Batra, “Hybrid machine learning based Intrusion Detection System for IOT,” 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2022.

[16] S. Alam, C. Yakopcic, and T. M. Taha, “Memristor based Federated Learning for network security on the edge using processing in memory (PIM) computing,” 2022 International Joint Conference on Neural Networks (IJCNN), 2022.

[17] C. Yakopcic and M. Tarek Taha, “Analysis and design of memristor crossbar based neuromorphic intrusion detection hardware,” 2018 International Joint Conference on Neural Networks (IJCNN), 2018. doi:10.1109/ijcnn.2018.8489252