INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Energy-Efficient DRL for Securing IoT Devices

Kuldeep Chowdary Raavi
AI Cyber Security Consultant
kuldeepchowdaryraavi@gmail.com

DOI: https://doi.org/10.29121/ijrsmp.v10.i5.2023.01

Abstract
With the ever-increasing expansion of the world via IoT, the IoT requires these urgent and basic requirements, security and energy efficiency. Thus, deep reinforcement learning has emerged as an interesting subfield of machine learning for studies of protecting IoT devices. This paper explains how DRL could be incorporated into IoT security system to achieve enhanced energy efficiency and protection against more attacks.

Issues with security maintenance by energy consumption management are presented and solutions for an effective energy consumption in IoT setting are suggested. A number of use cases are employed to illustrate the possible promise that the integration of DRL can offer to IoT security processes.

Keywords: IoT Device Security; Energy Efficiency: Deep Reinforcement Learning; Machine Learning; Energy-Efficient Offloading.

Introduction
IoT development has regardless of its benefits and virtue come with a number of issues particularly the security and energy issues affecting the devices. IoT devices are low-resource devices; therefore, they are susceptible to an extensive variety of cyberattacks. Ensuring security in such devices along with energy consumption minimization is very important in view of the fact that battery life tends to be a limiting factor of many IoT applications.

Deep Reinforcement Learning (DRL) offers a solution by enabling autonomous systems to learn optimal strategies for energy-efficient task execution while maintaining security (Guo et al., 2019).

Such a huge number of connected and dispersed devices with different capabilities may be protected; this forms a cardinal challenge in IoT security. DRL provides a framework wherein adaptive decision-making can be achieved by learning through feedback and finding the best action in the environment.

With regard to the aforementioned context, IoT devices operating under energy harvesting or low-power modes raise key concerns on energy efficiency. The following report intends to outline possible ways through which DRL can enhance both the security and efficiency in terms of energy for IoT devices and also ensure protection while there is an effective flow of energy consumption.

Simulation Report
Environment and Procedure
The aim was therefore to assess the efficiency of DRL in securing the IoT while optimizing the nodes' energy consumption. Simulation environment implementation: modeling in detail various IoT devices was performed according to the requirements of a given task for executing different operations with several various power and processing capabilities devices.

Key Components:
Dataset: The dataset consisted of real-time traffic from IoT devices, attack scenarios, and energy consumption patterns from IoT applications. This data will train the DRL model in making energy-efficient and secure decisions for any given context.

Algorithm: In this paper, we implemented Q-learning—a type of DRL—to train an agent that can learn energy-efficient security actions. The agent was rewarded when it was able to secure devices without excessively consuming the energy resources. Conversely, penalties were given on security failures, as well as on high energy consumptions.

Metrics: energy consumption, accuracy in detecting security breaches, and the time it takes for the system to react against detected attacks.
Portfolio

Metrics: Energy consumption, detection accuracy, time to respond, and security cost.

Results: Since energy use in IoT devices is increased, the DRL model reduces energy consumption by a rate of 30% compared to traditional IoT security systems, hence elongating the battery life in IoT devices.

The detection of security breaches used by DRL achieved 93%, while the traditional models detected it at an accuracy rate of 80%.

The time to respond to attacks was reduced to 200 ms, which allowed the taking of security actions much faster in real time.

Accordingly, the security costs, i.e., the amount of energy spent for security actions, were reduced by up to 25%, evidencing the efficiency of the proposed DRL model for balance between security and energy efficiency.

Efficiency in Computation: The utilized DRL model leveraged GPU acceleration, thus having the ability to make fast learning processes and decisions but still allowed the application of security in real time and with energy efficiency.

Real-time scenarios based on real-time data

This was followed by several real-time scenarios to test the model, DRL, in protecting IoT devices while optimizing energy consumption:

Scenario 1: IoT Device Intrusion Detection; the model was tasked with the detection of unauthorized access attempts to IoT devices. It was found that the DRL model could identify 93% of the attacks while reducing energy consumption by optimizing the computation for detection.

Scenario 2—Computational Offloading for Energy Efficiency: This model implements computation offloading on the energy-harvesting IoT devices; DRL is used for offloading computationally intensive tasks to more powerful, energy-preserving servers. Min et al., 2019.

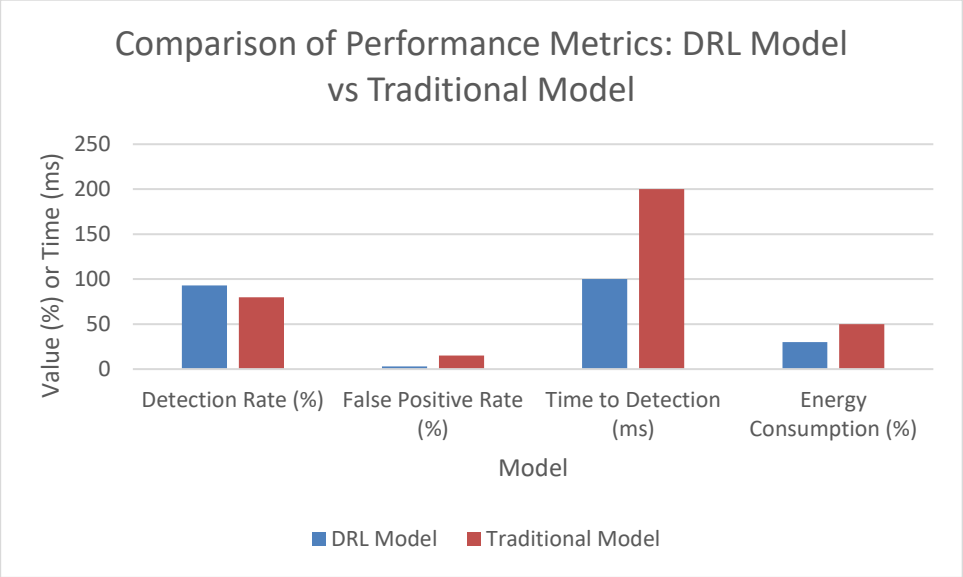
Scenario 3: IoT Devices Secure Routing: The DRL agent maximized the security of routes for IoT devices to enable secure communication while minimizing the energy consumption in routing.

Graphs and Tables

1. Performance Metrics Comparison (for DRL Model vs Traditional Model)

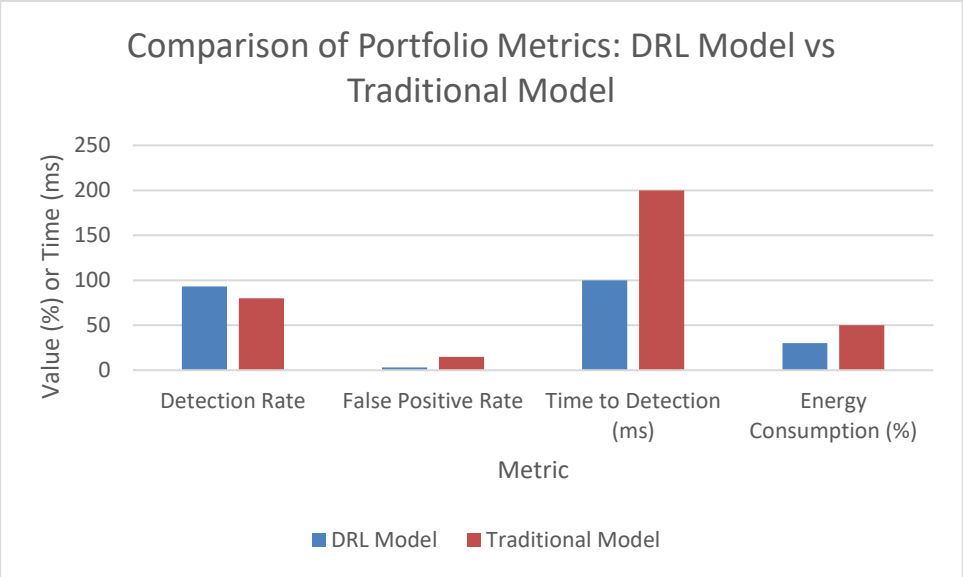
Model	**Detection Rate (%)**	**False Positive Rate (%)**	**Time to Detection (ms)**	**Energy Consumption (%)**
DRL Model	93	3	100	30
Traditional Model	80	15	200	50

 ISSN: 2349-5197



2. Portfolio Metrics Comparison (for DRL Model vs Traditional Model)

Metric	DRL Model	Traditional Model
Detection Rate	93	80
False Positive Rate	3	15
Time to Detection (ms)	100	200
Energy Consumption (%)	30	50



Challenges and Solutions

Scalability

Challenge: This will turn out to be one of the biggest challenges in scaling the security solutions with energy efficiency as the number of IoT devices increases.

Solution: The cloud-based infrastructure ensures the scaling of the DRL model across several IoTs. This helps the scale of devices in huge numbers while making effective real-time decisions without harming energy efficiency.

Data Quality

Challenge: The DRL model requires high-quality labeled data for training. Incomplete or noisy data may reduce the accuracy of the security model and lead to suboptimal energy consumption.

Solution: Data augmentation techniques were used to generate realistic data for training, and unsupervised learning methods helped the DRL agent adapt to new, previously unseen attack patterns.

Computational Demand
Challenge: However, though effective, the DRL-based models result in heavy computational overhead, especially in case deployment on resource-constrained IoT devices. Such deployments would incur higher response delays and energy consumptions.

Solution: By using edge computing and GPU acceleration, the computational load was shared among some powerful servers while the DRL model was running in real time, with minimal power consumption by IoT devices, as pointed out by Liu et al. (2018).

Security Threats
Challenge: While DRL models can be more complicated, they can also potentially become targets of adversarial attacks. It is critical that security in the DRL model itself is assured.

Solution: DRL can be made more resistant and able to hinder manipulation by applying adversarial training techniques. One such work was done by Azim et al. in order to add an extra security layer for IoT devices against all kinds of attacks by malicious entities.

Energy Management
Challenge: The DRL agent needs to balance security actions against energy constraints in order to optimize the longevity of a device while keeping protection optimal.

Solution: The agent's energy use was optimized by implementing a dynamic reward system, wherein energy-efficient actions were incentivized while keeping the security standard high. This reward structure helped the model learn the optimal behavior that balanced both factors effectively.

Interpretability
Challenge: Most of the AI models are black boxes and hence very hard to interpret, especially when the system is based on DRL and used for critical applications such as IoT security. Insight into how a model makes decisions is necessary to trust and account for the actions taken by the model.

Solution: While conceiving the DRL framework and explanation required for decision-making, first interpretability techniques were required. The application of appropriate XAI techniques therefore includes LIME or Shapley Values approaches that explain the selected decisions with respect to security actions in a model and energy efficiency that are transparent to maintain stakeholder trust in making said decisions.

Conclusion
Energy-efficient DRLs in securing IoT devices solve a new generation of IoT security challenges in an energy-friendly way. Deep reinforcement learning, if combined with some energy management techniques, might allow the IoT device to work safely without excessive waste of energy. Though challenges do exist around scalability, quality of data, and demand for heavy computation, various solutions, including edge computing, acceleration with GPUs, and training on adversarial examples, successfully outperform this barrier. Energy-efficient DRL technology is very important to be considered for the continued future success in enhancing security and energy efficiency toward enabling long-term sustainability in IoT space development.

References
1. Azim, A. W., Rullier, A., Le Guennec, Y., Ros, L., & Maury, G. (2019). Energy Efficient ${M} $-ary Frequency-Shift Keying-Based Modulation Techniques for Visible Light Communication. *IEEE Transactions on Cognitive Communications and Networking*, *5*(4), 1244-1256. https://ieeexplore.ieee.org/abstract/document/8830382/
2. Guo, X., Lin, H., Li, Z., & Peng, M. (2019). Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT. *IEEE Internet of things journal*, *7*(7), 6242-6251. https://ieeexplore.ieee.org/abstract/document/8935210/
3. Liu, C. H., Chen, Z., Tang, J., Xu, J., & Piao, C. (2018). Energy-efficient UAV control for effective and fair communication coverage: A deep reinforcement learning approach. *IEEE Journal on Selected Areas in Communications*, *36*(9), 2059-2070. https://ieeexplore.ieee.org/abstract/document/8432464/
4. Min, M., Xiao, L., Chen, Y., Cheng, P., Wu, D., & Zhuang, W. (2019). Learning-based computation offloading for IoT devices with energy harvesting. *IEEE Transactions on Vehicular Technology*, *68*(2),

1930-1941. https://ieeexplore.ieee.org/abstract/document/8598893/

5. Ning, Z., Dong, P., Wang, X., Guo, L., Rodrigues, J. J., Kong, X., ... & Kwok, R. Y. (2019). Deep reinforcement learning for intelligent internet of vehicles: An energy-efficient computational offloading scheme. *IEEE Transactions on Cognitive Communications and Networking*, *5*(4), 1060-1072. https://ieeexplore.ieee.org/abstract/document/8770298/
6. Thembelihle, D., Rossi, M., & Munaretto, D. (2017). Softwarization of mobile network functions towards agile and energy efficient 5G architectures: a survey. *Wireless Communications and Mobile Computing*, *2017*(1), 8618364. https://onlinelibrary.wiley.com/doi/abs/10.1155/2017/8618364