Towards Adaptive Cybersecurity for Green IoT

Talal Halabi
Université Laval
Québec, QC, Canada
talal.halabi@ift.ulaval.ca

Martine Bellaiche
Polytechnique Montréal
Montréal, QC, Canada
martine.bellaiche@polymtl.ca

Benjamin C. M. Fung
McGill University
Montréal, QC, Canada
ben.fung@mcgill.ca

2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) | 979-8-3503-9645-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/IoTaIS56727.2022.9975990

***Abstract*—The Internet of Things (IoT) paradigm has led to an explosion in the number of IoT devices and an exponential rise in carbon footprint incurred by overburdened IoT networks and pervasive cloud/edge communications. Hence, there is a growing interest in industry and academia to enable the efficient use of computing infrastructures by optimizing the management of data center and IoT resources (hardware, software, network, and data) and reducing operational costs to slash greenhouse gas emissions and create healthy environments. Cybersecurity has also been considered in such efforts as a contributor to these environmental issues. Nonetheless, most green security approaches focus on designing low-overhead encryption schemes and do not emphasize energy-efficient security from architectural and deployment viewpoints. This paper sheds light on the emerging paradigm of adaptive cybersecurity as one of the research directions to support sustainable computing in green IoT. It presents three potential research directions and their associated methods for designing and deploying adaptive security in green computing and resource-constrained IoT environments to save on energy consumption. Such efforts will transform the development of data-driven IoT security solutions to be greener and more environment-friendly.**

***Index Terms*—Green computing, green IoT, green cybersecurity, adaptive cybersecurity, energy-efficient security.**

I. Introduction

The large-scale of today's data centers and Internet of Things (IoT) networks has led to distressing increase in energy consumption and carbon emission, creating serious climatic variation issues [1]. In fact, the accelerated development of IoT in various application domains such as smart home, industry, and transport entailed several challenges related to real-time communications, reliable service delivery, security and privacy, for which numerous green-agnostic solutions were proposed. For example, network redundancy boosts Quality of Service (QoS) and availability but does not necessarily adhere to green computing criteria. Therefore, the environmental sustainability of IoT technologies remains a major challenge.

The Industrial IoT (IIoT) paradigm combines automated machines and advanced data analytics techniques to improve productivity and efficiency [2]. However, it produces massive amounts of data and relays heavy traffic generated by billions of connected devices, which also require energy to perform sensing, processing, and computing tasks. Moreover, cloud data centers running in the background of IoT applications are highly energy-hungry. Apart from the excessive manufacturing and massive shipment of IoT devices contributing to the greenhouse gas (GHG) emission, it has been shown that 5G-enabled communications of IoT devices incur the highest level of energy consumption [3] - estimated to consume 46TWh energy by 2025 [4].

Green IoT emerged as an energy-efficient and environment-friendly paradigm to reduce power consumption and carbon emissions by leveraging on-demand protocols, customized optimization algorithms, and Artificial Intelligence (AI) approaches [5]. Its lifecycle includes green design, production (manufacturing), utilization, and disposal [6]. Green IoT is usually accompanied by green cloud computing concepts focusing on higher resource utilization (e.g., multi-tenancy), cost-effective power management, and efficient workload coordination via dynamic provisioning at the server and data center levels [7].

Ensuring security and privacy in edge/cloud computing environments as well as IoT systems in a sustainability-aware fashion has also been considered as a priority research axis in green computing. This is crucial since the communications of billions of resource-constrained IoT devices as well as the overburdened cloud data centers running and providing IoT services and vast BigData analytics will require significant amounts of resources to deploy security solutions at a very large scale. These solutions will push power usage constraints in the opposite direction, especially if deployed suboptimally and in scenarios where they are not fully needed. Therefore, the design efficiency of communication protocols, computing paradigms, and security mechanisms will become a key aspect. Recently, several energy-efficient security solutions have been designed in IoT and edge computing including autonomous network monitoring [8], resilience against data transmission attacks [9], and low-overhead encryption algorithms [10].

Security deployment in large-scale IoT and complex cyber-physical systems already entails major scalability and performance issues. Hence, optimizing the design and deployment of security architectures will not only contribute to green cybersecurity efforts, but will also help addressing such issues [11]. The idea of adaptive cybersecurity has lately received significant attention as a way to achieve optimized security [12]–[14]. Indeed, by monitoring the security risk state of the edge infrastructure and IoT environment, security processes can be built to operate optimally [15]. This is a potential research direction that can greatly contribute to green cybersecurity research efforts in both the green computing and green IoT paradigms.

This paper explores three lines of research that will help achieve adaptive cybersecurity in green IoT, namely: 1) Dynamic threat prevention via Moving Target Defense

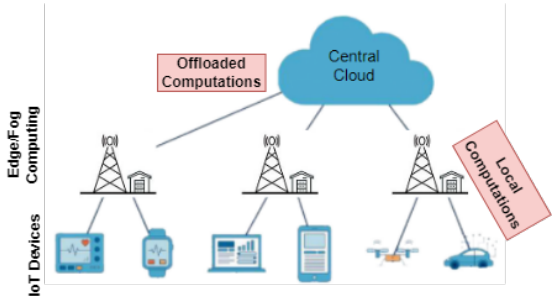

Fig. 1: Connected IoT devices usually offload heavy computations to edge or cloud data centers.

(MTD); 2) Optimized design and deployment of Intrusion Detection Systems (IDS); and 3) Risk-driven attack mitigation solutions. The paper is structured as follows. Section II describes the fundamentals of green computing and IoT architectures. Section III emphasizes the security challenges surrounding the realization of green IoT environments. Section IV discusses the three research directions that will help achieve green cybersecurity through adaptiveness. Finally, Section V concludes the paper.

II. Green Computing and IoT

IoT has brought new service opportunities across various sectors such as digitized health, autonomous transportation, and intelligent manufacturing, and has played a crucial role in building smart cities [16]. IoT involves smart devices that can upload data to the Internet and control the decisions of cyber-physical processes [2]. The IoT paradigm involves three main layers: the perception layer consisting of sensors and actuators performing data collection and device control; the communications layer responsible for the transmission of data from devices for processing and storage in the edge or cloud; and the application layer leveraging the cloud environment to perform computational and data analytics tasks. Fig. 1 depicts a generic architecture of IoT and edge computing.

As in green cloud, the early stages of IoT development focused on improving the performance and QoS of resource-constrained devices and delay-intolerant applications, while today's IoT solutions have started to prioritize energy-efficient designs to promote eco-friendliness. Hence, novel greenness metrics in IoT are anticipated to be developed, similar to the ones used to evaluate green clouds such as data center infrastructure efficiency and power usage effectiveness.

Green computing models are normally deployed at the software, hardware, and network levels. Software-related techniques reduce the number of active servers by implementing auto-scaling systems, virtualization solutions, and server consolidation approaches. Also, many of these techniques leverage machine learning for predictive data analytics and workload management. Hardware-related solutions can decrease energy consumption by enabling flexible control of server frequency and voltage, efficient heat dissipation to reduce cooling needs, and various sleeping models in physical devices [17]. At the network level, the goal is to reduce traffic between edge virtual machines or IoT devices as well as to minimize the power consumption of the wireless data path. This can be achieved by adopting the following approaches: i) Enabling idle or sleep modes for the sensors when not transmitting data; ii) Using context-aware processing and storage algorithms to reduce the data overhead at the edge; and iii) Configuring energy-efficient routing protocols [5].

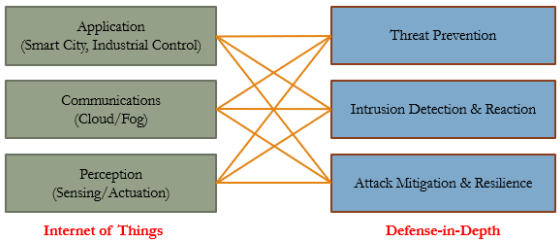

Fig. 2: Defense-in-depth principles should ideally be applied to every layer of the IoT architecture.

The concepts and characteristics of green IoT have already been applied in the following areas:

- Designing energy-aware communications protocols [18], [19], congestion control algorithms [20], and green wireless communications in IoT [21].
- Developing green resource allocation [22] and application deployment [23] algorithms.
- Implementing green control of cyber-physical operations in IIoT (e.g., SCADA [24]).
- Deploying green caching and data storage approaches at the network edge [25].
- Building green AI in IoT and edge systems [26].
- Designing energy-efficient cryptographic hardware [27], [28] and secure sensors [29] in IoT systems.

Nonetheless, green security approaches that can apply to the global IoT architecture have not yet received their fair attention. These approaches can be critical to ensure sustainable IoT development considering the substantial amount of resources required to implement various security features at every layer of the IoT architecture, as depicted in Fig. 2. Moreover, the defense-in-depth paradigm cannot be sacrificed given the extensive threat landscape in emerging Internet-connected cyber-physical systems [30]. Therefore, this paper investigates the potential of adaptive cybersecurity and introduces several ideas about green security design, deployment, and configuration for threat prevention, detection, and mitigation, which will help the research community in advancing the field of green cybersecurity.

III. Security Challenges in Green IoT

IoT raises many vulnerabilities that can lead to security threats [31]. Attacks at the perception layer include side channel, device tampering, and fake node injection [32]. Network layer attacks include Sybil and man-in-the-middle. Finally, attacks carried out against the application layer are mainly driven by malware such as viruses and worms [33] as well as data corruption and Distributed Denial of Service (DDoS) attacks, which could affect the cloud server and delivered services [34]. On the other hand, green IoT will introduce new security vulnerabilities as well as additional constraints on security deployment due to the limited resource

capabilities at the network edge. Hence, fully achieving green IoT will entail several security and privacy challenges.

A. Green IoT Requirements

Green IoT networks and systems may become more vulnerable to security attacks compared to traditional green-agnostic networks due to additional system requirements and energy constraints. Also, fog and edge computing data centers cannot provide the same level of security enabled by cloud computing due to their intrinsic features such as decentralized architectures, distributed computing, and resources limitation [35]. Hence, an adversary may discover new, greenness-driven malicious ways to target the green IoT network [36].

In green IoT, meeting the required and sufficient security and privacy specifications is critical; otherwise, we might end up overwhelming IoT devices with the burden of unnecessary security mechanisms, which may lead to increased energy consumption and reduced performance [37]. Furthermore, green IoT leverages different approaches, techniques, and algorithms (e.g., software, hardware, communications, architecture), whose layered deployment and heterogeneity may create security holes within the system [38]. This exacerbates the need to shape future cybersecurity solutions to fit the complex green IoT landscape and respond to challenging interoperability requirements.

B. Limitations of Conventional Security

Most of conventional security mechanisms may not be well suited for green infrastructures because they are not designed with energy-efficiency in mind (e.g., public-key encryption). These security methods normally use additional resources on IoT devices that result in heavy energy consumption [39]. Making these security solutions green might compromise their effectiveness and increase the risk of the IoT system to security threats, thus introducing an adverse effect.

Also, in recent years, new privacy regulations such as the EU General Data Protection Regulation have been enforced in many regions. As a result, many organizations are exploring privacy-enhanced technologies and data anonymization solutions on different data sharing scenarios [40], [41]. The general objective of these privacy-preserving technologies (PETs) is to achieve certain capabilities such as classification analysis but without compromising individual privacy. Recently, these techniques are being incorporated into the IoT paradigm [42]. However, most of them involve complex cryptographic protocols and are often computationally expensive and energy-hungry. Hence, they do not fit well with the requirements of green security and privacy protection.

C. Green AI-based Security

Intrusion detection in IoT networks and systems often rely on data-driven security solutions that gather contextual insights and enable automated reasoning based on knowledge representation to achieve cybersituational awareness [43]. For instance, anomaly-based detection makes use of statistical patterns as a baseline for standard behavior to detect malicious activities (e.g., using machine and deep learning techniques) [44]. AI techniques and BigData analytics help understand attackers better, detect both known and unknown attacks, and immediately react to threats by looking for anomalies in data and logs from multiple sources and identifying the relationships between threats such as malicious files and suspicious IP addresses [43]. But unlike signature-based detection, anomaly-based detection normally generates many false positives when trying to identify zero-day attacks. It can also increase operational overhead significantly.

In the roadmap of green security for sustainable IoT, deploying energy-efficient anomaly detection systems based on machine and deep learning is key [45]. From a green security perspective, proactiveness is costly, and ensuring real-time visibility into security threats may create performance burden on IoT systems. Also, training deep learning models which consume billions of data points from structured and unstructured sources yields a huge power consumption that can have adverse effects on the environment [46]. Nonetheless, AI has become intrinsic to modern, large-scale IDS and cannot be abandoned. Hence, we must explore new, efficient ways to deploy AI models for cyber defense - there exists an inherent link between green cybersecurity and green AI [47].

D. Evaluating Green Cybersecurity

The first step towards enabling green cybersecurity is to put in place the development standards and design frameworks required to ensure sustainability, as well as to systematically propose the evaluation procedures and metrics necessary for consistent implementation practices. For instance, the impact of cybersecurity solutions on carbon footprint should be quantitatively measured. The following metrics can be used to judge the greenness of future security mechanisms:

- Computing and communication overhead caused by the deployment of security policies and measures in edge IoT networks and cloud-enabled IoT services.
- Resource utilization by security and privacy methods and techniques at the IoT device (e.g., authentication and access control), server (e.g., anti-malware), and BigData levels (e.g., MapReduce tasks).
- Energy consumption by all resource types (e.g., CPU power, memory, bandwidth, databases) provisioned to deploy security controls in large-scale IoT networks and interconnected cyber-physical systems.
- GreenHouse Gas (GHG) emissions produced by all security-related operations including data collection, transmission, processing, and storage as well as decision making and surveillance in edge/cloud computing.

In addition, several other criteria or metrics may be imposed to assess the quality of green security designs with respect to maintaining acceptable performance levels and QoS such as response time, scalability, and fault tolerance.

IV. Adaptive Cybersecurity: Future of Green IoT

To address the above challenges, this paper presents three research directions that can guide future efforts in the field of adaptive cybersecurity as a fundamental enabler of green IoT paradigms. These directions focus on providing a holistically green defense-in-depth approach through adaptive security

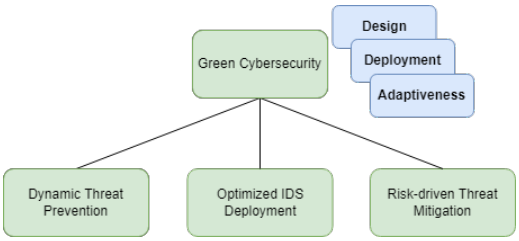

Fig. 3: Potential research directions to achieve green cybersecurity in large-scale IoT.

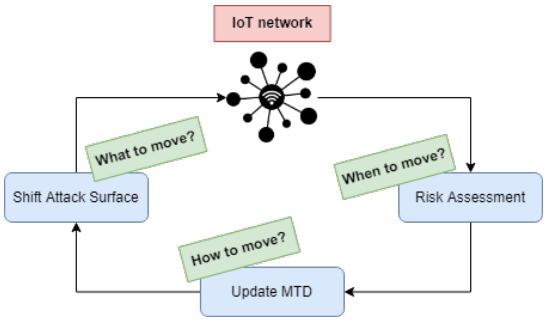

Fig. 4: Overview of the lifecycle of the adaptive MTD framework and its main design questions.

design and deployment from the perspectives of threat prevention, detection, and mitigation as shown in Fig. 3.

A. Dynamic Threat Prevention

Several approaches exist to optimize security deployment and enable dynamic network defense. For instance, MTD has been recently applied to protect IoT networks by dynamically shifting the attack surface and avoiding static configurations [48]. MTD aims to introduce uncertainty about the system or network's state and render the information collected by adversaries less valuable over time by continuously moving one or more configuration parameters (e.g., IP addresses, port numbers) through adaptation, randomization, or diversification [49]. IoT devices usually have low computational capabilities which make it difficult to implement advanced security features. Hence, the idea of MTD is very appealing to prevent attackers from infiltrating the network.

However, MTD movements on critical systems and low-power networks must not be performed randomly. They should be well calculated to avoid performance degradation and service disruption, especially in scenarios involving limited computational resources and hard QoS constraints. Fig. 4 shows the main stages and implementation aspects of a cost-effective MTD mechanism. Every stage can be exploited to create energy-efficient security solutions enabled by smart design and optimized deployment. Thus, using MTD, intrusion prevention systems in IoT networks can potentially be made greener and more sustainable on the long run, since they will be able to better respond to the functional requirements of green IoT compared to static and computationally-intensive cryptographic protocols, as discussed in Section III.

B. Optimized IDS Deployment

The communications between IoT devices and between devices and the edge necessitate high energy consumption [3]. Thus, green IoT security research efforts should focus on designing security mechanisms capable of operating under reduced data transmission (i.e., amount and frequency). Also, state-of-the-art green networking best-practices including selective routing, data compression, and low-power wireless communication protocols such as ZigBee should be adopted in future security architectures [50]. Finally, more focus should be given to optimizing the deployment of analytics-driven IDS in complex, large-scale cyber-physical systems.

For instance, Fig. 5 illustrates a multi-layered IDS architecture for the Internet of Vehicles (IoV). The IDS monitors Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications to look for suspicious behavior. However, a green IDS architecture needs to incorporate green design practices into every aspect of the IDS operations including the anomaly detection algorithms, collection and processing of security-related information, and deployment of local IDS components onto IoV infrastructure devices and vehicles.

Therefore, the IDS architecture in Fig. 5 may incorporate built-in optimization algorithms to avoid collecting anomaly-related data from the entire vehicular network in real time. Hence, selective monitoring of static and dynamic IoV components can be enabled in a risk-aware fashion to reduce communication overhead [51]. Furthermore, the IDS can leverage Reinforcement Learning (RL) algorithms to dynamically learn an adaptive security policy [52], as shown in Fig. 6. Here, the defense strategies can be continuously updated by observing their impact on the IoV infrastructure and assessing the anticipated threats. Hence, by integrating the metrics of energy efficiency into the design of the reward function of

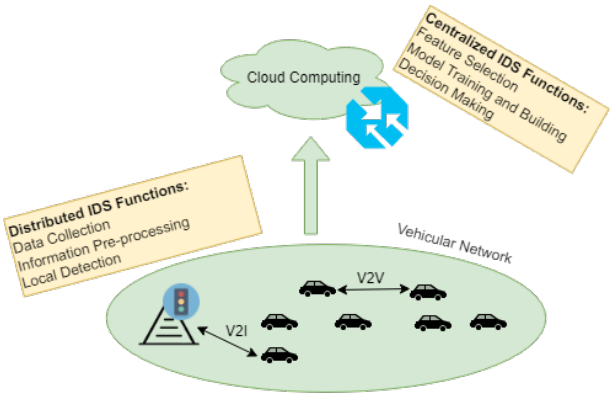

Fig. 5: Multi-layered IDS architecture in IoV.

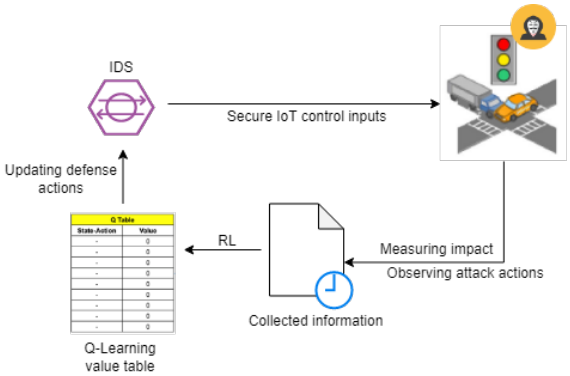

Fig. 6: RL application in IDS design to produce optimized, energy-efficient security actions.

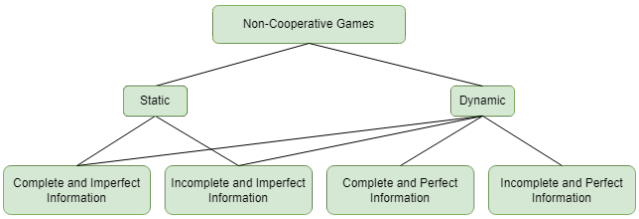

Fig. 7: Main game theory classes that can be leveraged for the design and deployment of adaptive IoT security schemes.

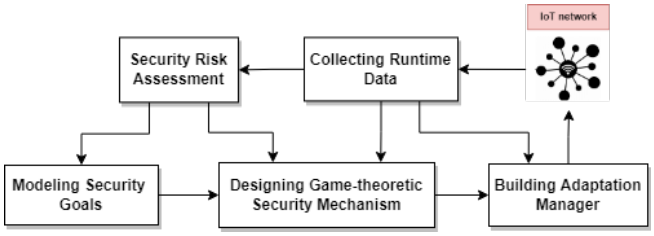

Fig. 8: Game-theoretic, risk-driven adaptive security framework for energy-efficient decision-making in large-scale IoT networks.

the autonomous IDS agent at the edge, the generated defense policy can adhere to the vehicle's energy constraints.

C. Risk-driven Threat Mitigation

Adaptive security architectures may potentially be built around risk assessment [53]. They can be driven by the dynamic evaluation of security threats in the network at a given point in time as well as the impact of security attacks in case they materialize. For instance, adaptiveness can be triggered when dealing with sensitive or safety-critical IIoT data, since securing non-sensitive data may consume unnecessary energy. Instead of configuring a heavy-overhead security control in a risk-agnostic fashion, only the required security controls should be implemented following careful vulnerability and threat assessment of the infrastructure. Moreover, these controls may be necessary only in some parts of the system (e.g., specific components, subset of devices, network portions), which may be more exposed to attacks.

Game theory is another approach that can be leveraged for security modeling and optimization under the umbrella of green IoT. It provides an extensive set of mathematical frameworks and tools useful for conducting risk-driven, macroscopic security studies. Various game-theoretic models have been used in the literature for developing security solutions [54]. These usually rely on formulating the attack/defense interactions with the objective of achieving the maximum payoff for the defense system [55]. For example, non-cooperative games are normally used to optimize the defense strategy against the adversary's actions, while cooperative games are used to effectively coordinate the collaborative behavior of nodes in peer-to-peer networks [51].

Fig. 7 depicts the main classes of non-cooperative game theory that can be used to perform continuous security risk assessment of the IoT system or network by studying the adversary's actions then adapting security deployments over time as illustrated in the security framework in Fig. 8. Dynamic game-theoretic models are a better fit for studying the attack-defense interactions in an adaptive fashion [15]. As shown in Fig. 7, these can be further categorized based on the information available about each player such as their strategies and payoffs (e.g., complete vs incomplete), as well as their knowledge of the history of played actions (e.g., perfect vs imperfect) [54]. Also, mean-field games [56] may be leveraged for designing optimized security solutions in IoT networks involving a large number of devices.

V. Conclusion

Green IoT has emerged as an energy-efficient and ecological paradigm to reduce carbon emissions by large-scale IoT systems and cloud-enabled IoT services. However, traditional cybersecurity approaches impose several barriers to the development of green IoT solutions. This paper presents three major research directions to help alleviate these barriers, namely designing energy-efficient threat prevention schemes, deploying security optimization at the network edge, and developing risk-driven threat mitigation solutions. These directions mainly aim at replacing static, programmable, and efficiency-agnostic security with dynamic and adaptive cybersecurity, which will highly contribute to achieving IoT greenness. In the future, we will explore in more details the greenness metrics needed to gauge the design and quality of green cybersecurity solutions in IoT and edge computing.

References

[1] S. Benhamaid, A. Bouabdallah, and H. Lakhlef, "Recent advances in energy management for Green-IoT: An up-to-date and comprehensive survey," *Journal of Network and Computer Applications*, vol. 198, p. 103257, 2022.

[2] D. G. Pivoto, L. F. de Almeida, R. da Rosa Righi, J. J. Rodrigues, A. B. Lugli, and A. M. Alberti, "Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review," *Journal of Manufacturing Systems*, vol. 58, pp. 176–192, 2021.

[3] M. A. Albreem, A. M. Sheikh, M. H. Alsharif, M. Jusoh, and M. N. M. Yasin, "Green Internet of Things (GIoT): applications, practices, awareness, and challenges," *IEEE Access*, vol. 9, pp. 38833–38858, 2021.

[4] S. Popli, R. K. Jha, and S. Jain, "Green IoT: A short survey on technical evolution & techniques," *Wireless Personal Communications*, vol. 123, no. 1, pp. 525–553, 2022.

[5] A. Malik and R. Kushwah, "A Survey on Next Generation IoT Networks from Green IoT Perspective," *International Journal of Wireless Information Networks*, pp. 1–22, 2022.

[6] S. Murugesan, "Harnessing green IT: Principles and practices," *IT professional*, vol. 10, no. 1, pp. 24–33, 2008.

[7] L.-D. Radu, "Green cloud computing: A literature survey," *Symmetry*, vol. 9, no. 12, p. 295, 2017.

[8] Z. S. Zaghloul, N. Elsayed, C. Li, and M. Bayoumi, "Green IoT System Architecture for Applied Autonomous Network Cybersecurity Monitoring," in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pp. 628–632, IEEE, 2021.

[9] R. Zhao, J. Xia, Z. Zhao, S. Lai, L. Fan, and D. Li, "Green MEC Networks Design Under UAV Attack: A Deep Reinforcement Learning Approach," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1248–1258, 2021.

[10] Z. Gu, H. Li, S. Khan, L. Deng, X. Du, M. Guizani, and Z. Tian, "IEPSBP: A Cost-efficient Image Encryption Algorithm based on Parallel Chaotic System for Green IoT," *IEEE Transactions on Green Communications and Networking*, 2021.

[11] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2018.

[12] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy-efficient mechanisms in security of the internet of things: A survey," *Computer Networks*, vol. 127, pp. 173–189, 2017.

[13] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in *2014 IEEE international conference on communications (ICC)*, pp. 920–925, IEEE, 2014.

[14] E. K. Wang, T.-Y. Wu, C.-M. Chen, Y. Ye, Z. Zhang, and F. Zou, "Mdpas: Markov decision process based adaptive security for sensors in internet of things," in *Genetic and evolutionary computing*, pp. 389–397, Springer, 2015.

[15] T. Halabi, "Adaptive Security Risk Mitigation in Edge Computing: Randomized Defense Meets Prospect Theory," in *2021 IEEE/ACM Symposium on Edge Computing (SEC)*, pp. 432–437, IEEE, 2021.

[16] M. A. Ferrag and L. Shu, "The Performance Evaluation of Blockchain-based Security and Privacy Systems for the Internet of Things: A Tutorial," *IEEE Internet of Things Journal*, 2021.

[17] H. Jayakumar, A. Raha, Y. Kim, S. Sutar, W. S. Lee, and V. Raghunathan, "Energy-efficient system design for IoT devices," in *2016 21st Asia and South Pacific design automation conference (ASP-DAC)*, pp. 298–301, IEEE, 2016.

[18] M. Capuzzo, C. Delgado, A. K. Sultania, J. Famaey, and A. Zanella, "Enabling Green IoT: Energy-Aware Communication Protocols for Battery-less LoRaWAN Devices," in *Proceedings of the 24th International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pp. 95–98, 2021.

[19] M. Morawski and P. Ignaciuk, "A green multipath TCP framework for industrial Internet of Things applications," *Computer Networks*, vol. 187, p. 107831, 2021.

[20] J. Bai, Z. Zeng, K. M. Abualnaja, and N. N. Xiong, "ADCC: An effective adaptive duty cycle control scheme for real time big data in Green IoT," *Alexandria Engineering Journal*, vol. 61, no. 8, pp. 5959–5975, 2022.

[21] A. Jaiswal, S. Kumar, O. Kaiwartya, M. Prasad, N. Kumar, and H. Song, "Green computing in IoT: Time slotted simultaneous wireless information and power transfer," *Computer Communications*, vol. 168, pp. 155–169, 2021.

[22] M. Yang, P. Yu, Y. Wang, X. Huang, W. Miu, P. Yu, W. Li, R. Yang, M. Tao, and L. Shi, "Deep Reinforcement Learning based Green Resource Allocation Mechanism in Edge Computing driven Power Internet of Things," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 388–393, IEEE, 2020.

[23] S. Forti and A. Brogi, "Green Application Placement in the Cloud-IoT Continuum," in *International Symposium on Practical Aspects of Declarative Languages*, pp. 208–217, Springer, 2022.

[24] X. Xiang, J. Gui, and N. N. Xiong, "An integral data gathering framework for supervisory control and data acquisition systems in green IoT," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 714–726, 2021.

[25] Y. Ren, X. Zhang, T. Wu, and Y. Tan, "In-network caching for the green Internet of Things," *IEEE Access*, vol. 9, pp. 76413–76422, 2021.

[26] S. Zhu, K. Ota, and M. Dong, "Green AI for IIoT: Energy Efficient Intelligent Edge Computing for Industrial Internet of Things," *IEEE Transactions on Green Communications and Networking*, 2021.

[27] U. Banerjee, C. Juvekar, A. Wright, A. P. Chandrakasan, *et al.*, "An energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in IoT applications," in *2018 IEEE International Solid-State Circuits Conference-(ISSCC)*, pp. 42–44, IEEE, 2018.

[28] A. Singh, N. Chawla, J. H. Ko, M. Kar, and S. Mukhopadhyay, "Energy efficient and side-channel secure cryptographic hardware for IoT-edge nodes," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 421–434, 2018.

[29] A. O. Akmandor, Y. Hongxu, and N. K. Jha, "Smart, secure, yet energy-efficient, Internet-of-Things sensors," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 4, no. 4, pp. 914–930, 2018.

[30] Y. Z. Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," *Journal of Systems and Software*, vol. 149, pp. 174–216, 2019.

[31] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[32] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.

[33] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[34] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, *et al.*, "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*, pp. 1093–1110, 2017.

[35] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," *IEEE access*, vol. 8, pp. 85714–85728, 2020.

[36] L. Li, Y. Luo, J. Yang, and L. Pu, "Reinforcement Learning Enabled Intelligent Energy Attack in Green IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 644–658, 2022.

[37] L. Caviglione, A. Merlo, and M. Migliardi, "Green-Aware Security: Towards a new Research Field," *Journal of Information Assurance & Security*, vol. 7, no. 6, 2012.

[38] A. Rehman, K. Haseeb, T. Saba, and H. Kolivand, "M-SMDM: A model of security measures using Green Internet of Things with Cloud Integrated Data Management for Smart Cities," *Environmental Technology & Innovation*, vol. 24, p. 101802, 2021.

[39] L. Tan, N. Shi, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered access control framework for smart devices in green Internet of Things," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 3, pp. 1–20, 2021.

[40] N. Mohammed, X. Jiang, R. Chen, B. C. Fung, and L. Ohno-Machado, "Privacy-preserving heterogeneous health data sharing," *Journal of the American Medical Informatics Association*, vol. 20, no. 3, pp. 462–469, 2013.

[41] D. Alhadidi, N. Mohammed, B. Fung, and M. Debbabi, "Secure distributed framework for achieving ε-differential privacy," in *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 120–139, Springer, 2012.

[42] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[43] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[44] A. Abusitta, O. A. Wahab, and T. Halabi, "Deep learning for proactive cooperative malware detection system," in *Edge Intelligence Workshop*, vol. 711, p. 7, 2020.

[45] L. Nie, W. Sun, S. Wang, Z. Ning, J. J. Rodrigues, Y. Wu, and S. Li, "Intrusion detection in green Internet of Things: a deep deterministic policy gradient-based algorithm," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 778–788, 2021.

[46] T.-J. Yang, Y.-H. Chen, J. Emer, and V. Sze, "A method to estimate the energy consumption of deep neural networks," in *2017 51st asilomar conference on signals, systems, and computers*, pp. 1916–1920, IEEE, 2017.

[47] R. Schwartz, J. Dodge, N. A. Smith, and O. Etzioni, "Green AI," *Communications of the ACM*, vol. 63, no. 12, pp. 54–63, 2020.

[48] H. Wang, F. Li, and S. Chen, "Towards cost-effective moving target defense against DDoS and covert channel attacks," in *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, pp. 15–25, 2016.

[49] J. Pawlick and Q. Zhu, *Game Theory for Cyber Deception*. Springer, 2021.

[50] H. T. Reda, P. T. Daely, J. Kharel, and S. Y. Shin, "On the application of IoT: Meteorological information display system based on LoRa wireless communication," *IETE Technical Review*, vol. 35, no. 3, pp. 256–265, 2018.

[51] T. Halabi, O. A. Wahab, R. Al Mallah, and M. Zulkernine, "Protecting the Internet of Vehicles against advanced persistent threats: a Bayesian Stackelberg game," *IEEE Transactions on Reliability*, vol. 70, no. 3, pp. 970–985, 2021.

[52] A. K. Bozkurt, Y. Wang, and M. Pajic, "Secure Planning Against Stealthy Attacks via Model-Free Reinforcement Learning," in *2021 IEEE International Conference on Robotics and Automation (ICRA)*, pp. 10656–10662, IEEE, 2021.

[53] I. Yassine, T. Halabi, and M. Bellaiche, "Security Risk Assessment Methodologies in The Internet of Things: Survey and Taxonomy," in *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 668–675, IEEE, 2021.

[54] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *2010 43rd Hawaii International Conference on System Sciences*, pp. 1–10, IEEE, 2010.

[55] Y. Wang, Z. R. Shi, L. Yu, Y. Wu, R. Singh, L. Joppa, and F. Fang, "Deep reinforcement learning for green security games with real-time information," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, pp. 1401–1408, 2019.

[56] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE transactions on wireless communications*, vol. 13, no. 3, pp. 1616–1627, 2014.