Toward a Balance Between Energy Consumption and Security in IoT Networks: A Survey

Michaël Mahamat, Ghada Jaber, Abdelmadjid Bouabdallah

***Abstract*—The advent of the Internet of Things (IoT), with thousands of connected, heterogeneous, and energy-constrained devices, enables new application domains and improves our everyday life. To minimize maintenance costs and maximize network lifetime, developers and companies use energy management methods. In addition, heterogeneity and the deployment of IoT networks in open environments increase the attack surface. A successful attack can dramatically impact an IoT network and causes physical or economical harm. However, securing a network against these threats incurs additional energy consumption that may be unbearable for energy-constrained devices, thus depleting their batteries and reducing network lifetime. In the literature, there is a huge number of research works that propose solutions for either security or energy management for IoT networks. However, research on joint optimization of security and energy is scarce. In addition to that, existing surveys focused also either on IoT energy management or on IoT security. In this paper, we present a survey based on a new approach that tackles jointly the problem of security and its impacts on the energy efficiency of IoT networks. We propose a taxonomy of recent solutions that reduce energy consumption while efficiently securing IoT networks. We consider context-aware security for IoT networks as an interesting way to secure IoT networks while reducing the overall energy consumption. We also present recent advances and new paradigms such as artificial intelligence and Software-Defined Networking (SDN) and their use in the development of efficient energy aware security solutions for IoT. Finally, we present a general model for the development of energy-efficient IoT security solutions to go toward a good trade-off between security and energy consumption.**

***Index Terms*—Internet of Things (IoT), Green IoT, Security, Energy, Energy Harvesting, Energy Management, Context-aware security.**

I. Introduction

The Internet of Things (IoT) is growing so fast and objects around us become connected, whether they are in our everyday life such as smart factories, smart farms, or in an open hostile environment. IoT has seen the development of multiple applications, from the industrial perspective [1] to smart cities and smart agriculture systems [2]–[4]. The use of IoT is drastically improving the quality of our lives and the efficiency of industrial production. Companies using or creating IoT applications will have to adapt their business model to succeed in their projects [5]. In addition to that, the energy sector [6] is gradually increasing its use of IoT for energy and microgrid management.

IoT networks are naturally heterogeneous systems, as multiple types of devices are connected. They may include Wireless Sensor Networks (WSNs), RFID sensors networks, Mobile Ad-hoc Networks (MANETs), actuators, or other smart objects. Due to this heterogeneous nature, the limited energy capacity of devices, and the existence of multiple technologies enabling IoT networks [7], [8], several challenges for IoT networks arise. Energy and security are considered as two important challenges among economical costs, scalability or interoperability for instance. Moreover, the applications deployed in an IoT network are more and more complex and connect more and more devices, which are smaller and limited in terms of energy storage. Hence, it is mandatory to develop lightweight protocols and applications to reduce the energy consumption of such constrained devices, and consequently, maximize their lifetime. Furthermore, since IoT networks are mostly deployed in open environments, with various technologies, security breaches and attack surfaces are increasing [9]. Thus, there is an urgent need to protect IoT networks from attacks and malicious entities. Indeed, successful attacks may lead to economic losses, outages, or critical issues if IoT networks are deployed for critical applications, such as the energy sector [6]. Then, it is important to deploy highly secure solutions to protect sensitive networks. Nevertheless, deploying a secure solution creates an additional energy consumption and hence, a faster battery depletion which may lead to the reduction of network lifetime or even industrial process failure. Thus, designing IoT security solutions that are energy-efficient, but also in the same time, efficient against multiple threats, appears to be a tedious quest.

In this paper, we study the impact of security solutions on energy consumption in order to develop security solutions for IoT networks that do not affect energy efficiency, hence improving network lifetime. We aim to give researchers, developers, and manufacturers, insights on how to design security solutions that are energy-efficient and efficient against ever-evolving threats. Our contributions in this survey can be summarized as follows:

- We present a review of existing surveys in the field of IoT energy management methods, IoT security solutions, a discussion about their limitations, and show how our survey outperforms existing surveys.
- We study the impact of security solutions on the energy consumption of IoT nodes, i.e. how can security solutions

Michaël Mahamat is with Heudiasyc laboratory, Sorbonne Universites, Universite de Technologie de Compiegne, 60203, Compiègne, France (email: michael.mahamat@hds.utc.fr).

Ghada Jaber is with Heudiasyc laboratory, Sorbonne Universites, Universite de Technologie de Compiegne, 60203, Compiègne, France (email: ghada.jaber@hds.utc.fr).

Abdelmadjid Bouabdallah is with Heudiasyc laboratory, Sorbonne Universites, Universite de Technologie de Compiegne, 60203, Compiègne, France (email: madjid.bouabdallah@hds.utc.fr).

This work is co-funded by the multidisciplinary initiative “Mastery of Safe and Sustainable Technological Systems” of the Sorbonne University Alliance.

consider energy consumption. We present a comparison and a classification of existing research works which may help the reader to select the appropriate security solution for a specific IoT application domain.
- We present and discuss design challenges of energy-efficient and adaptive IoT security solutions including recent advances and new paradigms such as Software Defined Networks (SDNs) and artificial intelligence that are used in the development of energy-efficient and secure solutions for IoT.

The rest of this paper is organized as follows. In section II, we discuss the limits of existing surveys and we present a classification of recent surveys according to several criteria. In section III, we recall different energy management techniques for IoT networks. In section IV, we address fundamentals on security and present some recent works on IoT security. In section V, we study the impacts of security mechanisms on energy, and we present solutions trying to find a trade-off between security and energy. In section VI, we discuss the identified limits in previous sections and expose challenges for the design of secure, robust, and energy-efficient IoT networks. Finally, we conclude the paper.

II. Related works

In the past years, several surveys in the IoT field (from IoT architectures to IoT security solutions) have been published. We present in this section existing surveys regarding energy efficiency and security solutions for IoT. We classify the studied surveys in table I regarding their scope and give relevant comments on each of them.

A. IoT Energy Efficiency

Energy is a scarce resource for many IoT devices as they may be hard to reach or recharge. Then, using energy management methods and Energy Harvesting (EH) techniques can extend their lifetime.

In [11], Sah et al. surveyed different techniques to manage energy consumption and the different existing renewable Energy Harvesting (EH) schemes for the WSNs. For energy management, clustering, load balancing, energy balancing, coverage awareness, and node placement are the main approaches that are used to reduce energy consumption and improve network lifetime. Different renewable energies may be harvested such as solar energy, wind energy, kinetic energy, thermal energy, etc. However many challenges arise regarding energy harvesting. One of them is the design of the harvesting units. They must not be intrusive and should be designed to be compatible with the sensor. Energy harvesting models should also consider the chaotic nature of the environment and weather to reduce prediction errors.

In [10], Alsamhi et al. investigated the different enabling technologies and algorithms for greener IoT networks (green RFID, green WSNs, green cloud computing, green data centers, and green communication networks) which are being used to reduce the energy consumption and CO_2 emissions in smart cities. Green RFID can be enabled by using smaller tags as they are hard to recycle. Green wireless sensors networks may use duty-cycling schemes, data reduction techniques, energy harvesting, and transceiver power optimization. Green cloud computing may use virtual machines, better components, and better resource allocation schemes to produce less CO_2 and reduce the overall energy consumption. Relay nodes and better routing algorithms can reduce CO_2 emissions. These techniques are useful for convergence toward a greener IoT, but they may have impacts on network performances such as a lower QoS, longer delays, etc. The authors considered also that drones (UAVs) are going to be useful in future green smart cities for pollution monitoring and reducing the energy consumption of other devices.

In [12], authors surveyed the different existing harvesting techniques for IoT. They provide a taxonomy of the different harvestable energies in five categories: ambient, human, mechanical, organic, and hybrid sources. They also discuss the advantages and drawbacks of using each energy source and present energy harvesting models. These models are either deterministic or stochastic. Stochastic models, such as Markow processes or Kalman filters, can consider the natural uncertainty of energy harvesting mechanisms. Along the provided taxonomy and studied models, authors presented two case studies for IoT. The first case is a beacon-based on BLE powered by solar energy. The second case is a beacon powered with RF energy, also based on BLE. Both beacons have embedded sensors to monitor their environment. These platforms allowed authors to quantify the effectiveness of such harvesting techniques and challenges linked to energy harvesting. These challenges involve economical costs, utilization of a specific energy source for specific applications, energy storage, or the use of multiple energy sources.

B. IoT Security

Security methods for IoT are abundant and many research has been conducted. Without implementing security solutions, networks might face outages or data theft. Several surveys have been written to cover existing threats and security solutions for IoT. Table II compares the most important IoT security surveys with our work.

In [13], the authors reviewed the threats and the existing security solutions for the IoT. The authors considered an IoT network with four layers (sensing layer, network layer, middleware layer, and application layer). Each layer has to cope with specific threats. They identified four categories of solutions: blockchain-based solutions, fog-computing-based solutions, machine learning (ML) based solutions, and edge-computing-based solutions. Each category of solutions focuses on particular threats. This survey presents existing solutions and discusses how the different categories of solutions take into account the heterogeneity, privacy concerns, and resource constraints. In [14], authors surveyed security and privacy solutions for IoT networks and their applications in various domains. They exposed the weaknesses of old security solutions with regard to scalability, heterogeneity and mobility. They presented new solutions based on SDN, Blockchain, and the importance of context-aware security for adaptive security solutions. In [15], Tahsien et al. also surveyed IoT

Surveys	Scope	Comments
[10]	Green IoT technologies and applications	Presentation of green IoT technologies in smart cities. This paper does not present security issues.
[11], [12]	Harvesting methods and IoT prediction models	Presentation of energy harvesting methods, modeling and prediction methods. These papers do not present security issues.
[13]–[17]	IoT security solutions	Presentation of IoT security solutions based on emerging technologies (machine learning, blockchain, etc.). [16] presents threats against WSNs, RFID networks and tools (simulators, analyzers) used in the surveyed works.
[9], [18], [19]	Iot objects and vulnerabilities	Detailed taxonomies of threats and vulnerabilities in IoT. [9] describes vulnerabilities in commercial IoT objects and the associated communication protocols, with a focus on fitness and smart home solutions.
[20], [21]	Energy-efficient mechanisms for IoT security	Presentation of energy-efficient mechanisms for security solutions to alleviate computations and decrease the energy consumption of security solutions. Authors focus on secure data aggregation in [21].
[22]	Security mechanisms for energy-harvesting enabled IoT	Presentation of security solutions for energy harvesting network, with a major focus on physical layer and physical properties.
Our survey	Trade-off between IoT security mechanisms and energy consumption	Survey of recent security methods and exploration of trade-off between security and energy consumption.

TABLE I
TABLE SUMMARIZING THE SCOPE AND REMARKS OF STUDIED SURVEYS.

Survey	Year	Emerging technologies	Energy-efficiency for security
[20]	2017	−	+
[16]	2018	∼	−
[18]	2019	∼	−
[13]	2019	+	−
[14]	2018	+	−
[22]	2020	−	∼
[19]	2020	∼	−
Our survey	2021	+	+

TABLE II
STUDIED SURVEYS BETWEEN 2017 AND 2020 REGARDING IOT SECURITY.

Legend −: Subject is not discussed, +: Subject is discussed, ∼: Subject is partially discussed.

security solutions based on machine learning algorithms. In [16], authors conducted a review of security solutions for IoT networks. They considered a three-layer architecture: a perception layer, a network layer, and an application layer. They presented possible attacks against RFID nodes and WSNs, and security solutions or services as solutions. In [17], Yugha et al. also surveyed security protocols for each network layer and simulation tools for IoT networks. In [18], Neshenko et al. presented an extensive taxonomy of IoT vulnerabilities, the linked attacks, their impacts, and the corresponding countermeasures. Authors also presented for each class of vulnerability, the impacts on security objectives, and countermeasures. They identified for each vulnerability class, the state of current research, and the limits. Authors in [19] focused their survey on threats and vulnerabilities in WSNs and IoT networks and discussed cybersecurity strategies for IoT networks. Menghello et al. in [9] studied existing security vulnerabilities and attack surfaces for widely used communication technologies (ZigBee, Bluetooth Low Energy (BLE), 6LoWPAN with CoAP and LoRaWAN). They highlighted the severe security problems present within commercial solutions based on those communication technologies. Especially, in ZigBee and BLE solutions, security and privacy are not the primary concerns of manufacturers.

In [20], the authors surveyed energy-efficient mechanisms for IoT security services and gave a taxonomy of those mechanisms. They discussed the need for energy-efficient and energy-aware security solutions that may use confidentiality, authentication, access control, signature and verification, and key establishment. Due to the heavy operations involved in many security primitives, there is a need to design energy-efficient security solutions. The energy-efficient mechanisms are classified into six categories: online/offline security, outsourcing, adaptive security, low-power security protocols, data compression, and hybridization. This survey is the first survey to detail energy-efficient mechanisms for security solutions. However, it mainly focuses on authentication methods, signature methods, and key management systems, as they may consume a lot of energy. In addition to that, they did not discuss security measures and linked (if they exist) energy-efficient mechanisms using PHY-layer properties.

In [21], Yousefpoor et al. surveyed various methods to secure the data aggregation process for WSNs and established a taxonomy depending on the network architecture. Data aggregation is a well-known method used to reduce the energy consumption in WSNs.

In [22], Tedeschi et al. presented the different methods of Energy Harvesting (EH) and surveyed the existing security solutions for energy harvesting networks, as they exhibit particular properties. Moreover, they considered that EH networks have less available energy. They focused their study on EH networks harvesting RF energy. Authors presented specific threats in energy harvesting networks such as beamforming vector poisoning attacks, leeching, greedy, and cheating attacks. To overcome those threats, authors presented multiple security methods for different kinds of EH networks. Those methods can be categorized into two parts: cryptography methods and data secrecy methods using PHY-layer properties. On one-hand, cryptography methods for EH networks focus on pre-computation techniques, computation offloading, optimization of the implementation to reduce the energy consumption, or a dynamic adaptation of the security service. On the other hand, PHY-layer methods

and properties guarantee data secrecy. This review is more focused on the security of EH networks than using EH methods to improve security solutions for IoT networks.

The presented surveys focus on different methods to secure IoT networks with different approaches. However, energy conservation is not the main focus of these surveys. Energy is a resource that may be protected against sleep deprivation attacks for instance, but it has not been discussed as a resource to be well managed along security services in IoT networks. In [22], authors considered security for EH-WSNs networks. Authors in [20] focused on the reduction of the energy cost of security solutions used in IoT networks. In [14], authors exposed context-aware security solutions that are energy-efficient, but they did not provide an in-depth explanation on the energy-efficiency of context-aware security. Moreover, the energy efficiency of security solutions is not the main focus of their survey. Authors in [21] only focused their study on data aggregation. There is no survey considering the optimization of the energy consumption of a whole security solution, from the physical layer to the application layer.

In our study, we found that few surveys tackled the problem of energy for security solutions and the need for a trade-off between the security level and energy consumption. Whether we consider EH-enabled IoT networks or generic IoT networks, there is an urgent need to consider the energy factor in the design of security solutions. Indeed, their energy cost is not negligible and it impacts the available energy for other tasks. Hence, this will be detailed in the rest of our survey.

III. IoT energy saving mechanisms and energy harvesting

Since IoT devices have limited energy resources, it is necessary to enhance them with energy management and optimization solutions in order to maximize their lifetime. In this section, we will present a review of energy management and optimization techniques that we classify into two main categories: energy management mechanisms and energy harvesting mechanisms.

- Energy management methods save energy to improve network lifetime. Duty-cycling or global strategies are examples of such mechanisms.
- Energy harvesting mechanisms allow a node to harvest energy from the surrounding environment. This category includes energy transfer methods, wireless transfer methods, and energy harvesters.

We summarize in figure 1 the different categories presented in this section. We do not aim to present all existing techniques. Instead, we give the readers a quick overview of existing harvesting and management techniques. Extensive research has been conducted in this field and complete reviews have been written [10]–[12].

A. Energy management mechanisms

Energy in IoT networks can be efficiently managed and saved using different techniques issued from *green IoT* research. Green IoT can be defined as an IoT network where greenhouse impacts are lower than a traditional IoT network or nullified. Green IoT networks aim to decrease energy footprint and respect the environment. Each layer of a green IoT network is concerned, from the sensing layer to the deployed applications.

In [23], the authors investigated the different green principles and techniques to move toward green IoT. These techniques may be software-based, hardware-based, policy-based, or awareness-based. Moreover, changing the habits of the users or recycling devices may lead to green IoT networks too. Interoperability should also be heavily researched because having interoperable systems could reduce the carbon footprint of future IoT systems. It will also reduce economical costs.

1) Duty-cycling:

The first efficient way to save energy is using duty cycling mechanisms. Duty-cycling allows a node to cycle between states (active, listening, sleeping for instance) to consume less energy. In [24], authors studied duty-cycling for nodes in a smart home environment. They designed an algorithm implementing duty-cycling for IoT nodes and conducted experiments on a small test-bed with an Arduino. Their results show that the Arduino consumed less energy during off and pre-off cycles than in the active cycle state.

In [25], the authors studied Content-Centric Networking (CCN) for WSNs and provided an algorithm to reduce the energy consumption for content forwarding: ADDC-CCWSN (Adaptive and fully distributed duty-cycle algorithm for content-centric wireless sensor networks) based on duty-cycling. Nodes having a high activity rate for forwarding content have a high duty cycle and it is reduced if these nodes do not forward a lot of contents. This duty-cycling algorithm is adaptive and can be increased or decreased depending on the users interest. Authors show that reducing the activity of nodes does not impact the functionalities of the protocol and reduces energy consumption. Presented concepts can be applied to IoT as duty-cycling can be used to reduce the activity of less active IoT nodes.

2) Clustering:

Clustering is used to group nodes into clusters. In a cluster, a cluster head (CH) is elected and is in charge of scheduling communications for its cluster members. There exist different clustering algorithms and one famous clustering algorithm is LEACH [26]. Authors in [27] presented an adaptive clustering solution based on LEACH and energy harvesting. Their solution works in two phases. One phase is the setup phase where a CH sets up communications in its cluster. The second phase is the operational phase where cluster members sense and send data to their CH. In their simulations, the effectiveness of their solution is validated with an increased network lifetime and a better throughput.

In [28], Wang et al. presented a solution that includes solar energy harvesting sensors, cluster head re-selection, wireless charging, and tour planning. Regarding the clustering section

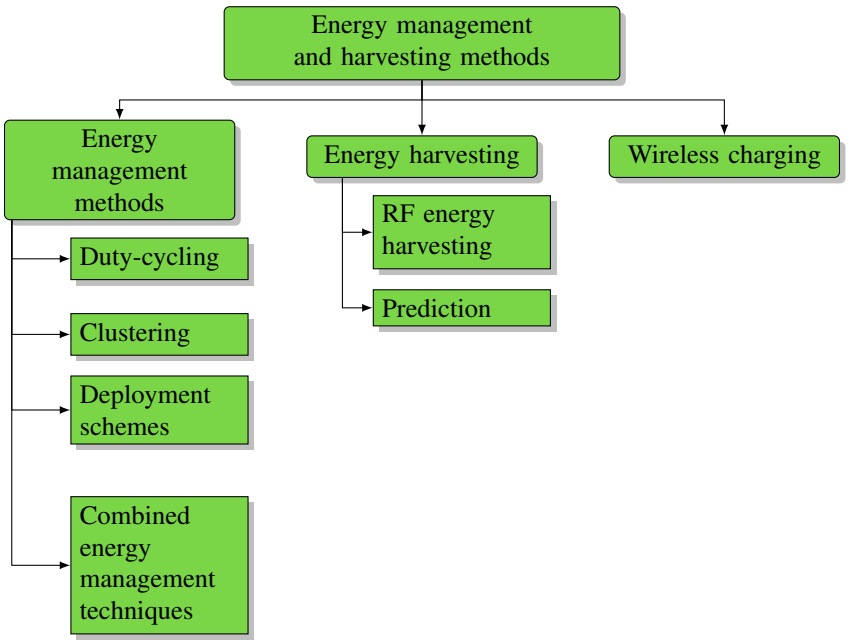

Fig. 1. Subfields of energy management methods and harvesting mechanisms presented in this survey.

of their work, authors studied cluster head re-selection when the weather is rainy and a CH harvesting solar energy cannot fulfill its duties anymore (due to a lack of energy). Cluster head re-selection increases network lifetime.

3) Deployment schemes:

Deployment schemes focus on node deployment to reduce the cost or the energy needed to transmit messages in the network. In [29], the authors introduced a deployment scheme to minimize the energy consumption of the IoT network. It is focused on relay nodes as they are economically expensive. Authors considered an approach similar to the Steiner tree and provided an algorithm to solve the underlying problem. Although the proposed method is interesting in the deployment phase (offline) and shows lower energy consumption in their simulations, it suffers from a high computational cost, even if in some cases, the Steiner tree can be solved in a linear time.

Authors in [30] provided an energy-efficient architecture model for Industrial IoT (IIoT) networks. The node deployment model is a hierarchical deployment model. It is done using three layers: a sensing layer, a gateway layer, and a control layer. Authors advocated that this hierarchical deployment should also consider link traffic constraints to achieve energy-efficient IIoT. Their approach has been validated in experiments where deployed nodes showed a lower energy consumption and a higher resource utilization rate.

In [28], authors also investigated deployment schemes for solar harvesting nodes. They provided two algorithms: one for a discrete deployment space and one for a continuous deployment space (solar nodes can be deployed everywhere). Their algorithms give acceptable solutions due to the NP-hardiness of the deployment problem.

4) Combined energy management techniques:

Combining multiple management methods allows the designer to create efficient energy management systems. In [31], Said et al. combined three strategies to design an Energy Management Scheme (EMS) for green and heterogeneous IoT Networks. This EMS is managed by servers which observe the level of energy in nodes. The first strategy aims to minimize the amount of transmitted data in the IoT network since radio transmissions consume a lot of energy. The second strategy schedules the tasks to reduce energy consumption. The last strategy aims to guarantee fault tolerance. These strategies are applied on energy-based nodes and the chosen strategy depends on the energy level of the considered node. The presented simulations demonstrated the efficiency of their EMS compared to another system without EMS. Indeed, fewer nodes are dead and the throughput is $53\ \%$ better.

In [32], Ejaz et al. presented energy-efficient solutions and an optimization framework for smart cities. To reduce the energy consumption of green IoT applications, solutions such as lightweight protocols, scheduling, predictive models for energy consumption, or enhanced transceivers are needed. The proposed optimization framework covers the different objectives and the associated mathematical tools. Aside from energy management techniques, energy harvesting can be used in smart cities to increase network lifetime. Authors studied the problem of scheduling energy transmitters (with unlimited energy) to transfer energy to nodes in a network. They also showed that number of tasks and number of energy transmitters have an impact on the energy consumption of the network.

B. Energy harvesting schemes

On the other hand, IoT nodes can use energy harvesting to re-fill their energy storage (battery, capacitor, or supercapacitor) by converting the harvested energy into a Direct Current (DC). Energy harvesting in IoT (and previously in WSNs) is inspired by the existing harvesting methods for renewable energies (solar, wind, geothermic, and hydroelectricity). Existing taxonomies organize energies into multiple categories: controllable or uncontrollable, predictable or unpredictable, amount of harvested energy, etc. [11], [12], [33], [34]. Intensive research has been conducted in this domain and many results, regarding harvester technology, energy prediction, or amount of harvested energy are available.

1) RF energy harvesting:

Radio-frequency (RF) energy harvesting has attracted research due to the abundance of RF energy in the environment. In [35], the authors presented a system model for Wireless Energy Harvesting (WEH). The considered energy source is the RF energy produced by a sink node. The main contribution of their work is the introduction of a Power Management Unit (PMU) with a duty-cycling policy linked to a Wake-Up Radio (WUR). The PMU manages the allocation of the available energy to the different components. The WEH possesses a rectifier that converts RF energy into a stable direct current. In their experiments, the proposed method drastically improved network lifetime, up to $510\ \%$ for the Adhoc topology.

In [36], the authors provided state-of-the-art of architectures for Wireless Powered Communication networks (using RF energy) which are WET (Wireless Energy Transfer), SWIPT (Simultaneous Wireless and Information Power Transfer), and WPCN (Wireless Powered Communication Network). WET is a building block for the two other architectures. In SWIPT networks, signals used for data transmission and energy transfer are the same, while for WPCN, an energy signal is sent downlink and the harvested energy will be used to send data in the uplink.

In [37], Mishra et al. explored different scenarios and methods to improve the efficiency of RF energy harvesting with a focus on multipath energy routing (MPER). RF energy harvesting suffers from losses and interference, and MPER could limit the impacts of those problems. Indeed, MPER reduces charging time and allows for a higher number of nodes that never run out of energy.

2) Prediction of the amount of harvested energy:

Some natural energy sources cannot be controlled, as they are far away (e.g. the Sun), chaotic (e.g. the wind), or disrupted by hostile weather conditions. Thus, it is important to predict in the near future how much energy nodes can harvest to adapt their activity.

One of the first proposed models to predict the amount of harvested solar energy is the Exponentially Weighted Moving-Average (EWMA) method [38]. It takes advantage of sun cycles as they begin and end, in a given season, roughly at the same time each day. A day is decomposed into time slots of 30 minutes (a total of 48 time slots). The main assumption of the model is that the amount of harvested energy during the day d at the time slot t is similar to the energy harvested during the previous day $d-1$ at the same time slot. Although it can adapt to seasonal changes, EMWA is not suited to environments subject to chaotic weather conditions.

In [39], a novel energy prediction (PROfile Energy prediction, Pro-Energy) model for solar and wind energy is presented. Previous models such as Exponentially Weighted Moving Average (EWMA) and Weather-Conditioned Moving Average (WCMA) [40] lack the ability to consider multiple previous observations for the prediction of harvested energy in the current time slot. Pro-Energy may be used for short-term predictions with a weighting parameter α and medium-term predictions by using a single or multiple past profiles. Their experiments validated the effectiveness of Pro-Energy compared to EMWA and WCMA regarding energy prediction and prediction errors.

In a more recent model [41], authors proposed an energy prediction algorithm for solar energy harvesting for WSNs called QL-SEP. As opposed to previous works, the proposed work uses Q-learning to be able to capture weather variations during the day. It may use similar observations from previous days. In their simulations, QL-SEP performed better than EWMA and Pro-Energy but showed weaknesses during winter with high error predictions (due to the bad weather).

C. Wireless Charging

Wireless Charging is a special case of energy harvesting where Mobile Chargers (MCs) make tours to charge the battery of devices. MCs can also collect data while charging nodes.

In [28], along with clustering and deployment schemes, authors also considered the wireless charging problem. They highlighted that in previous works, only full recharges were considered. Thus, they decided to use partial recharges and optimize the trajectory of mobile chargers according to these partial recharges. Due to similarities with the Traveling Salesman Problem with Neighborhoods (TSPN), authors designed a heuristic to optimize the charging time of nodes. Their simulations showed the efficiency of their complete framework regarding energy savings and trajectory optimization.

In [42], Abid et al. provided charging strategies and an architecture based on solar energy harvesting and wireless charging for WSNs. The network has an Energy Harvesting Base Station (EHBS) supplying a mobile charger. The goal is to improve network lifetime while considering the costs of deploying EHBS with MCs. The three charging strategies provided by the authors for the MCs are: on Demand energy Distribution Protocol (DDP), Periodic energy Distribution Protocol (PDP), and Periodic energy Distribution Protocol with Priority (PDPP). They made experiments to analyze network lifetime along with deployment costs for each protocol and different numbers of EHBSs. They found out that the best trade-off between network lifetime and deployment cost is the use of one EHBS and PDP protocol.

In [43], authors presented a framework to minimize the energy consumption of a MC charging devices. Best Charging

Efficiency (BCE) allows a MC to charge multiple nodes at once. BCE is designed as a first algorithm to compute the charging cost. A second algorithm, Branching Second Best Efficiency Algorithm (BSBE), is designed to overcome cluster selection problems when the number of nodes increases. BSBE takes the second best clusters, but it provides a trade-off between performance and computation time. The charging path is determined by considering the energy in the MC and the remaining energy of nodes. In their experiments, BCE is computationally faster than BSBE. Nevertheless, BSBE has a better charging cost and performs better than BCE in large networks.

In [44], authors also tackled the optimization of charging tours and charging time. They provided two algorithms in their framework: Charge Time Optimization of Wireless Mobile Charger (CTOWMC) and Route Optimization of WMC algorithm (ROWMC) algorithms. Their solution, compared to other works, use two MCs, one MC dedicated to lifetime balance (minimizing the variance of the lifetime) and one spare MC to charge nodes which have low energy levels (under a threshold). In their experiments, the variance of the remaining lifetime for ROWMC is lower than other schemes, whether it is in low-density networks or high-density networks.

Research in the field of energy management and energy harvesting is important and multiple surveys on the matter exist [10]–[12] as presented in section II.

On one side, energy management schemes allow nodes to save energy in an efficient manner but they introduce new challenges such as designing cross-layer protocols to consider these energy-saving mechanisms with each aspect of IoT networking. On the other side, energy harvesting methods replenish energy containers with variable efficiency. RF energy is an abundant energy source but the converted power is low. Solar and wind energy can yield more power, however, they are uncontrollable. Nodes harvesting these energies must be deployed in the best zones to harvest the highest amount of energy.

MCs can drastically improve network lifetime if they are used along with energy harvesting nodes. However, MCs need to have considerable batteries to charge nodes and they are expensive. Indeed, in [44], authors did not consider that WMCs consume energy to move and they considered that WMCs have unlimited energy. These assumptions are not quite real, as WMCs have a limited energy budget.

Moreover, techniques based on node monitoring to choose a strategy, such as in [31], are not secured. If malicious nodes report wrong energy levels to the Energy Management System, it can take wrong decisions and impact badly the network. Some schemes are not secured, which is a disadvantage in a world with many cyber threats and attackers. Hence, there is a need to secure IoT nodes to keep them alive as long as possible.

IV. Recent advances in IoT security

In this section we firstly recall basic notions of IoT security, then we present some recent security solutions and discuss their limits regarding energy efficiency. We also present intelligent security mechanisms using learning techniques which are useful to provide adapted security services. Hence, IoT networks become more reactive to threats when using intelligent security methods. Figure 2 lists the different points we are going to present in this section.

A. Fundamentals of IoT security

Due to the existence of multiple technologies in an IoT network, the number of potential attacks and vulnerabilities increases. Researchers have presented multiple taxonomies and existing attacks in previous surveys and articles [9], [13], [18]–[20], [22], [45].

Security methods for IoT networks need to fulfill multiple security services:

- Confidentiality: data must be protected from malicious entities.
- Integrity: data must be accurate and protected against malicious modifications.
- Availability: data must be available as much as possible and unavailable to malicious entities.
- Non-repudiation: Actions or messages sent by a node cannot be repudiated by this node.

Confidentiality, integrity, and availability are called the CIA attributes. In addition, the privacy of the users is also a challenging issue in IoT networks.

Two types of attackers can target IoT networks and impair one or multiple CIA attributes:

- Passive attackers who do not actively seek to impair the network. Eavesdroppers are an example of passive attackers.
- Active attackers who actively try to impair the network. Denial of Service attacks and jamming attacks are active attacks.

When deploying security solutions in an IoT network, both classes of attackers should be considered.

There are also two classes of attacks: cyber threats targeting the different layers of an IoT node or IoT network and physical threats which target the physical device such as its destruction.

A baseline approach to secure communications in IoT networks is encryption. This is done to protect the content of a message from an attacker and to do so, encryption relies on the use of keys. There exist two types of encryption: symmetric-based encryption and public-key encryption. In symmetric-based encryption, the key used for encryption and decryption is the same. In a network, each node must have the same key if they use a symmetric-based encryption scheme. Public-key encryption considers a pair of keys (public and private) to encrypt and decrypt messages. The public key of a node can be known from other nodes and is used for encryption whereas the private key of this node, as its name suggests, is only known to this node and is used for decryption. For both classes of encryption, keys must be generated and distributed in the network.

Authentication methods are used to authenticate the sender of a message. It is needed in an IoT network as a lot of

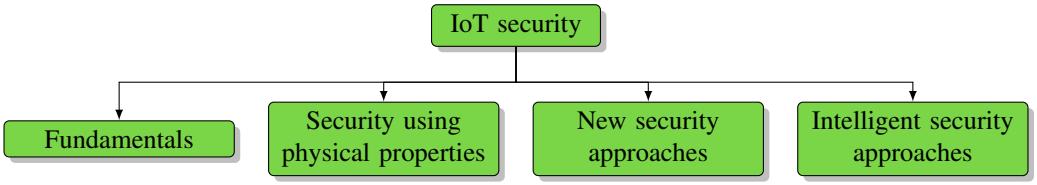

Fig. 2. Oultine of the studied classes of security solutions.

data can be generated and the number of nodes is significant. If malicious nodes are present and try to impersonate other nodes, authentication can prevent these malicious nodes to access sensitive data. For instance, in [46], the authors provided an authentication protocol based on Elliptic Curve Cryptography (ECC) for IoT edge devices, ECCbAP, with a focus on BLE and RFID tags. Their protocol has two phases: registration phase and login (plus authentication) phase. Authors removed the hash function from edge devices. This reduces the computational cost of the protocol for the edge nodes. They claimed that, compared to other protocols having three or four phases, ECCbAP is secure against the same attacks and provides additional security against impersonation attacks, message integrity attacks, and replays attacks.

B. Security based on physical properties

In this part, we consider different security solutions based on physical properties. The use of physical properties such as Received Signal Strength (RSS) may be useful for IoT security and may protect the network from threats such as eavesdropping or DoS attacks. Tedeschi et al. in [22] presented security solutions for the physical layer of energy harvesting networks.

Ghahramani et al. presented in [47] an authentication method based on Received Signal Strength (RSS) to overcome weaknesses of authentication protocols studied in their state of the art. RSS is used to determine the presence of malicious nodes. If malicious nodes are in the network, nodes solve an optimization problem to find their position. Their simulations showed that their method had a lower distance error and saved energy, even if RSS computation may incur additional energy costs for some nodes.

Chen et al. presented in [48] three scheduling schemes to protect data secrecy when an untrusted relay is present: Optimal Scheduling (OS), Threshold-based Scheduling (TS), and Random Scheduling (RS). They observed during the simulations that a higher number of sensors in a cluster improves the energy efficiency and security of OS scheme. They also observed that TS is a trade-off between OS and RS regarding energy efficiency and data secrecy.

C. New security approaches

New technologies such as blockchain or Software-Defined Networking (SDN) [49], [50] may be used to create enhanced IoT security solutions. Indeed, SDN offers the possibility to program network functionalities, such as routing, packet filtering, or security rules. Control and data planes are separated and thus, it enables scalability and quick responses to changes and threats. In addition, trust systems are useful for IoT security as they monitor nodes behavior and conduct analyses to detect malicious nodes.

In [51], Szymanski explored security and privacy concerns for green IoT networks. The proposed approach to achieve a good security level considers a combination of a centralized control plane with SDNs and deterministic virtual networks (DVNs) with a lightweight encryption protocol using long keys. The SDN control plane can detect unauthorized and unplanned data flows. The use of FPGA with silicon photonics, along with SDN, increases the available bandwidth while reducing economical costs and communication delays. Author claims that strong security is achieved thanks to the optical switches, using multiple SDN control planes along with a voting system, and lightweight encryption with long keys.

In [52], authors proposed a decentralized and secure energy management framework based on blockchain and SDN for microgrid networks. SDN is used within microgrids to secure communications and to implement security policies (such as access control and whitelists). Microgrid Master Controllers (MGMC), which are powerful devices deployed in microgrids, use blockchain technology to secure data exchanges with each other. MGMCs also manage the SDN control layer and use asymmetric cryptography to interact with the blockchain.

In [53], authors provided a security solution based on blockchain to secure a smart home IoT network. They also used AI to offer intelligent services to the users. They provided a proof of concept with a light sensor, a smart curtain, and lights.

Hasan et al. aimed in [54] to optimize the number and the placement of trust systems in IoT-based SCADA systems for grid networks. Trust systems are used to manage cyberattacks with firewalls and intrusion detection systems but they are expensive. Their solution minimizes the number of trust nodes deployed by solving an optimization problem (thus minimizing the costs). Authors evaluated their approach on IEEE test system topologies. Compared to a greedy approach, their solution uses more trust nodes. It also provides a higher security level as the number of monitored network segments is higher.

Using evolutionary game theory as their main building block, authors presented in [55] an adaptive cybersecurity framework in IoT-based healthcare applications. In the considered scenario, the healthcare institution (the highest layer) is connected to smart homes which are connected to smartphones with wearables (the lowest layer). In their simulations, attackers and defenders are not aware of the choices of the

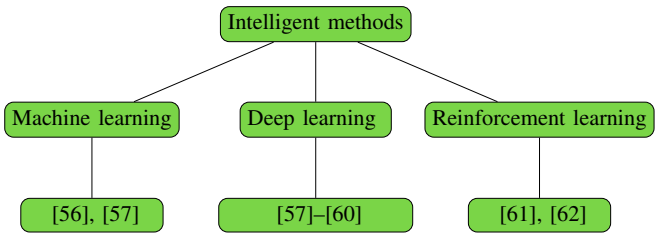

Fig. 3. Subfields of surveyed intelligent security methods.

other players and after around 160 runs, for both attackers and defenders, the average utility stabilizes. Both populations focus their actions on the highest layer (healthcare institution).

D. Intelligent security mechanisms

Security solutions may also consider learning-based techniques. Learning-based techniques are useful in Intrusion Detection Systems (IDS) or can be used to design adaptive security methods. The significant amount of data generated by IoT networks justifies the use of intelligent algorithms to secure them and research in this field has increased these last years. For instance, in [57], authors surveyed various machine learning and deep learning algorithms for IoT security. Figure 3 displays the three categories of intelligent solutions presented in this subsection and in table III, we sum up the contribution of each studied article in the field of artificial intelligence for security.

Each class of techniques has different characteristics and can be used to work on two kinds of tasks: classification and regression tasks. Machine Learning (ML) techniques are techniques learning from raw data representations relationships between variables. Deep Learning (DL) can be used in regression, classification tasks, or even in data generation (variational autoencoders or generative adversarial networks for instance). It heavily relies on artificial neural networks. Reinforcement Learning (RL) is a special case of machine learning where an agent interacts with its environment and tries to maximize the rewards it gains over time for each action taken. RL can use deep learning approaches in conjunction with RL algorithms, such as Deep-Q learning. RL mimics well the learning process humans have. The scope of this survey is not to present every existing learning technique and application domain, but to give a quick overview of recent learning techniques for IoT security.

1) Machine learning approaches:

In [56], authors proposed IoTArgos, a monitoring security system based on machine learning which detects anomalous behaviors and intrusions in the network. It is placed in the home router to monitor multiple layers and analyze data issued from different communication protocols. IoTArgos works in two phases: a first phase where IoTArgos is trained using supervised approaches (on known attacks) and a second phase where IoTArgos uses unsupervised learning to detect outliers. In their experiments, authors considered multiple learning algorithms to find the best combination with the best classification and error results. They showed that the deployment of IoTArgos with the best classification results uses random forests for the first phase and PCA for the second phase with an accuracy of $98.18\ \%$ and an Area Under the Curve (AUC) of $96.78\ \%$.

2) Deep learning based IoT security approaches:

In [58], authors presented a neural network approach in the MAC layer of MICA2 motes to detect DoS attacks and mitigate them. Each mote possesses a Multi-Layer Perceptron (MLP) linked to its MAC layer. The MLP takes as inputs the collision rate, packet request rate, average packet waiting time and a unit bias to give in return a suspicion factor in the interval $[0; 1]$. If this suspicion factor is above a predefined threshold, the node is shut down. Two training algorithms are considered: backpropagation (BP) and Particle Swarm Optimization (PSO). In their simulations, they considered 17 nodes with an attacker, and nodes are initialized with initial random battery values between 500 and 1000 units. They observed that PSO has lower mean square errors but a higher training time than BP. Moreover, a higher threshold decreases the network lifetime but it also decreases the number of false alarms.

In [59], authors investigated the use of an Improved Conditional Variational AutoEncoder (ICVAE), along a Deep Neural Network (DNN), to detect intrusions. ICVAE generates new attack samples from an initial training data set to increase the number of rare attacks in the data set. It also reduces data dimension and initializes the weights of the hidden layers of the DNN, which is used to detect attacks. Authors used NSL-KDD and UNSW-NB15 data sets to validate their model implemented with TensorFlow. ICVAE-DNN has the best detection results on the NSL-KDD dataset compared to other oversampling methods. For the UNSW-NB15 dataset, ICVAE-DNN has good detection rates for many attacks but falls behind other models for DoS, backdoors, analysis, fuzzers, and reconnaissance attacks compared to other oversampling methods.

Considering Deep Belief Networks (DBNs) and PSO algorithm, authors proposed in [60] an intrusion detection model for Unmanned Aerial Vehicle (UAV) networks. PSO algorithm optimizes the number of hidden layer nodes of the DBNs which detects the intrusions. To validate their model, authors used the KDD Cup99 dataset which mimics intrusions in a military network. With a DBN using four layers, their model reached an accuracy of $92.44\ \%$ and presented the best results compared to other approaches (such as C-SVC). They also compared the effects of different optimization algorithms for the number of nodes in each layer and PSO has the best results. However, their work has not been tested on a practical UAV network whose nodes are resource-constrained.

3) Reinforcement learning based IoT security approaches:

Article	Subfield	Learning methods	Security measure
[56]	Machine learning	Random forests, PCA	Intrusion detection in smart home networks
[58]	Deep learning	Multi-layer perceptron	DoS attacks detection and mitigation
[59]	Deep learning	Improved Conditional Variational AutoEncoder (ICVAE), Deep Neural Network (DNN)	Intrusion detection
[60]	Deep learning	Particle swarm optimization (PSO), Deep Belief Network (DBN)	Intrusion detection in UAVs
[61]	Reinforcement learning	Q-learning	Impersonation attack detection

TABLE III
INTELLIGENT SECURITY SOLUTIONS.

As opposed to machine learning and deep learning, reinforcement learning does not need to use an initial dataset to learn to detect threats. These methods, applied to IoT security can protect networks against known and unknown threats and provide ever-evolving security services. Indeed, in [62], authors surveyed existing reinforcement methods and stated that reinforcement learning can be efficiently used to develop IoT security solutions against DoS, spoofing, or jamming attacks.

In [61], Tu et al. applied Q-learning to detect impersonation attacks in fog computing. In the network, when receivers need to detect transmitting nodes using fake MAC addresses, they run a hypothesis test on each packet they receive from those suspicious nodes. The test uses Q-learning to dynamically adapt its threshold. They compared their approach with a fixed-threshold approach and observed that theirs has better accuracy and a lower average detection time. Average Error Rate (AER), False Alarm Rate (FAR), and Miss Detection Rate (MDR) are also lower for the Q-learning approach.

E. Remarks

The research works presented interesting results. However, they have clear limitations. For security solutions based on ECC, the main problem is the heavy computation cost. In [46], although the hash function has been eliminated, the energy consumption is not discussed in the paper as ECC is used. It should have been discussed as they claim that their solution is good for RFID nodes or BLE-enabled nodes.

Security solutions for the physical layer and using CSI or RSS may consider energy efficiency. As discussed in section II, Tedeschi et al. in [22] surveyed many security solutions for Energy-Harvesting (EH) networks using PHY-layer properties but solely focused their study on specific threats and did not fully explore the question of learning methods to reinforce security in EH networks.

Security solutions based on blockchain may have some difficulties when the network scales up, such as the size of the distributed register. If there are thousands or millions of nodes contributing to a blockchain, there is a need to limit the size of the blockchain. In [53], authors only use three smart things for a smart house network, which can be handled easily by a blockchain. Moreover, they did not develop the AI part in their PoC. In the future, a smart house may use more than a hundred of connected objects to deliver multiple services to its users.

Intelligent security solutions can face the complexity linked to the chosen model and the data. If data is not properly cleaned, it can greatly impact the effectiveness of the learning model. Moreover, if the model is not suited to the situation, it can negatively impact security (with a lot of false alarms or no alarms). Authors did not provide practical implementations in [60], [61] and that is why it is hard to determine if their methods can efficiently work in constrained environments. Other problems linked to reinforcement learning are the curse of dimensionality which is the difficulty of discretizing a continuous action space or working with a continuous action space.

Solutions based on adaptive security may be efficient against a wide array of attacks. However, the presented framework in [55] does not consider the heavily constrained nature of wearables and the limited battery of smartphones.

Moreover, the presented papers do not consider energy as a constraint. Each security solution induces additional energy costs in communications (higher message sizes within security headers), computations (ECC needs a lot of computation power), or memory usage (learning-based models can use a lot of memory space). We summarize in table IV the studied security solutions, their category, the underlying technologies, and the mitigated attacks.

In the next section, we introduce works measuring the energy cost of security solutions and energy-aware security solutions.

V. TRADE-OFFS BETWEEN SECURITY AND ENERGY

In the previous section, we have presented recent IoT security solutions. However, implementing security solutions in IoT networks increases energy consumption due to overheads in communications and computation. Hence, this reduces the lifetime of devices. Few research has evaluated the impact of security solutions on the energy consumption of the nodes. We will now tackle the different impacts of security on energy consumption and present existing security solutions that try to minimize nodes energy consumption while providing the required security level. If nodes are energy-efficient and rechargeable, they may have a longer lifetime and do not need battery changes.

In subsection V-C we present security solutions considering energy as a major constraint. In figure 4, we present the main categories of energy-efficient security solutions we will present in this section.

A. Measurement of the energy cost of security solutions

The discussed security solutions in section IV did not consider the energy consumption, which is problematic if they

Article	Category	Underlying technology	Resilient against
[46]	Authentication	Elliptic curve cryptography (ECC)	Impersonation attacks, message integrity attacks and replay attacks
[48]	PHY-layer security	Secrecy rate, CSI	Communication with an untrsuted relay
[47]	PHY-layer security	Received Signal Strength (RSS)	DoS attacks
[51]	Backbone security	Software defined networking (SDN), deterministic virtual networks (DVNs), optical switches	Unauthorized packets, cyberattacker detection
[52]	Cybersecurity for microgrids	Software-Defined Networking (SDN), blockchain	Data leakage, information distortion
[54]	Cybersecurity for SCADA (trust systems deployment)	Trust systems, linear programming	Intrusions, information distortion
[53]	Cybersecurity for smart homes	Blockchain, AI	Data leakage
[55]	Adaptive security	Evolutionary game theory	Not specified

TABLE IV
RECENT SECURITY SOLUTIONS STUDIED FOR IOT IN THIS SECTION.

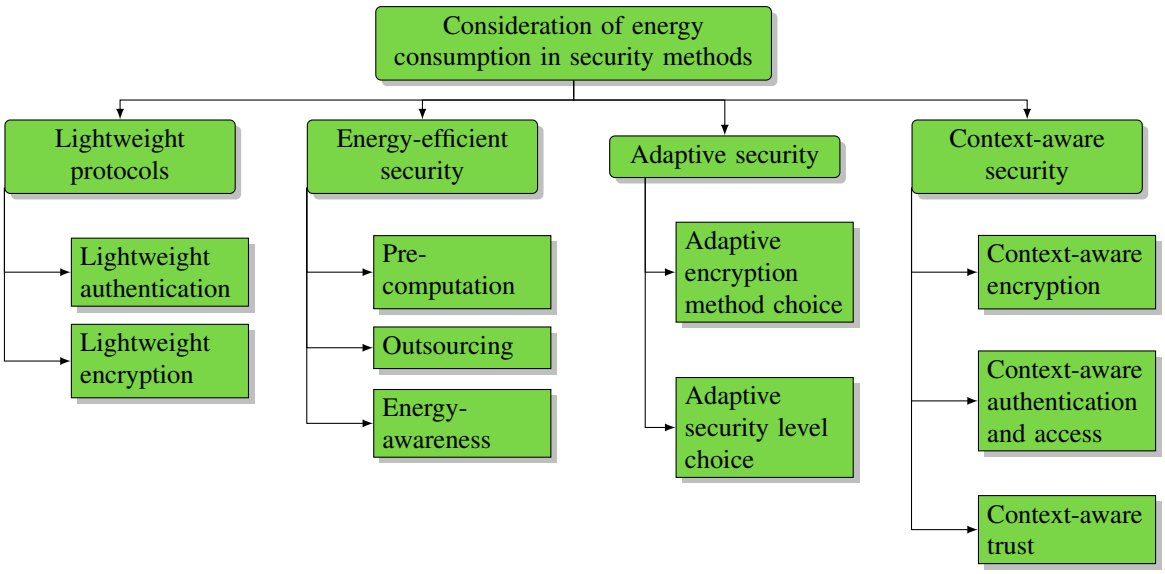

Fig. 4. Different categories of security solutions considering energy presented in this survey.

have to be deployed in constrained nodes. There exist numerous research works regarding energy costs for encryption methods, authentication, and signature protocols.

First of all, using a security service or solution impacts QoS, throughput, and energy consumption. Indeed, authors in [63] observed that, for the IEEE 802.15.4 protocol, using higher security levels negatively impact throughput, latency, and energy consumption. For a payload of 24 bytes, the overall energy consumption is increased by 31.5 % for the lowest security level and by 60.46 % for the highest security level (using encryption and authentication).

In [64], authors evaluated the energy cost of ECDH-ECDSA (asymmetric, use of SHA-1 and secp160r1) and Kerberos (symmetric, use of AES-128). They measured the energy cost of different modes (transmit, listen, receive, compute sleep) for two known platforms: MicaZ and TeloSB motes. They observed that ECDH-ECDSA consumes more energy than Kerberos, regardless of the platform they used (20 times on the MicaZ mote and 10 times for TeloSB).

In [65], the authors studied the energy cost of 18 authentication methods on a real test-bed with energy and computation constraints. They provided a design space to estimate the impact of each block of an authentication solution. Indeed, algorithm type (MAC-based or signature-based), security level (in bits), number of passes (1 or 2), voltage scaling, and the potential use of a hardware multiplier are all blocks impacting the cost of a whole authentication method. For MAC-based algorithms, authors considered SHA1, SH2, and Keccak which are widely used. For signature algorithms, they also considered known algorithms which are ECDSA, Winternitz, and Lamport. They conducted experiments on a MSP430 micro-controller powered by a supercapacitor and solar energy harvesting. Their results show that signature-based authentication protocols consumed more energy than MAC-based solutions. Moreover, they observed that using a higher CPU frequency reduces the energy consumption of authentication methods and a 32-bit hardware multiplier also reduces the energy consumption of ECDSA.

The energy cost for authentication or encryption may become unbearable for small and energy-constrained devices. In [66], Schaumont outlined that for a device using a piezo-electric harvester, a single ECDSA authentication can only be made every 20 minutes. He advocated the need for security designs based on available energy rather than the available

computing power.

In [67], authors evaluated the energy cost of three encryption algorithms on a microcontroller based on PIC18F45K22. These algorithms are Tiny Encryption Algorithm (TEA) [68], eXtended TEA (XTEA) [69] and SKIPJACK [70]. Two asymmetric signature algorithms, RSA and ElGamal, are also studied but are implemented with low-size keys (16-bit). Regarding encryption algorithms, the majority of energy is consumed during the sending phase. XTEA consumes less energy than the other encryption algorithms, with SKIPJACK consuming the most during encryption. However, SKIPJACK takes less time to complete encryption and data sending. For digital signature algorithms, signing time and energy costs are higher for RSA than for ElGamal.

In [71], authors presented a fast, secure and deployable architecture for IoT made of open-source and off-the-shelf components. They compared AES with and without hardware accelerators, XTEA, and SEA to study the memory performance, energy consumption, and execution time. It appeared that AES-128 and AES-256 without hardware accelerators have the worst performance, regarding energy, memory performance, and computation time compared to XTEA and SEA. However, if AES-256 uses hardware accelerators, the results are the best. XTEA and SEA provide a lower security level but are more energy and memory-efficient.

In [72], authors also observed that AES consumes more energy than Chacha and Acorn, regardless of the platform they used. However, encryption and decryption times depend on the platform. Atmega328 is the slowest platform, contrary to the ESP8266. Aerabi et al. confirmed in [73] that AES and its variants were not among the best performing block ciphers for the nRF51822 chip and Atmega328 platform. They also validated that RC6, TEA, and Simeck have the best performance, the lowest energy consumption, and few cycles spent per bit.

Girgenti et al. studied in [74] the energy cost, encryption, and decryption times of three Attribute-Based Encryption (ABE) schemes: Goyal-Pandey-Sahai-Waters's scheme (KP-ABE), Bethencourt-Sahai-Waters scheme (CP-ABE), and Yao-Chen-Tian scheme (KP-ABE). Through extensive simulations, they observed that the number of attributes has a direct impact on energy consumption, encryption, and decryption times. KP-ABE schemes are more energy-efficient than the CP-ABE scheme, but CP-ABE schemes are easier to implement.

Energy consumption of a given security service may impact the network lifetime and incur economical or material costs: batteries will be changed or replenished by operators. The less energy a security service consumes, the less costly it will be, whether it is economical or material. A first step to have a balance between energy consumption and the security service provided is to know how much energy is consumed by a specific authentication, encryption, or signature algorithm. A second step is to determine which encryption, authentication, or signature algorithms should be used according to the available resources. A third step is to efficiently incorporate them in composing security methods in order to cover multiple threats.

B. Energy model for security solutions

In the previous subsection, we outlined the works regarding encryption, authentication, and signature energy costs. These methods are the primary blocks to be used to ensure the primary security services (confidentiality, availability, integrity).

The use of models to evaluate the energy cost of security solutions is important and pinpoint the most costly blocks of a particular solution, not only regarding computation costs but also regarding communication costs. Indeed, in [75], the authors proposed an energy model to evaluate the energy cost for secure IoT networking. All phases of a security algorithm can be evaluated using this energy model. In symmetric cryptography methods, the energy cost of security solutions is low compared to asymmetric security solutions. The energy cost of single operations has already been studied in previous papers, but the networking part had not been considered. At a given time t, the energy consumed by a node d, knowing it has n connections, is given by:

$$E_d = \sum_{i=1}^{n} E_c(i) + E_{OS} \tag{1}$$

, with $E_c(i)$ the cost of the i^{th} connection of the node d and E_{OS} the energy cost spent by the node in the common tasks (routine). Connection between two nodes can be broken down in three phases (E_c): creation of the security context, data exchange and key update or revocation (if the connection has ended). The creation of the security context also consumes energy. It is based on the energy cost of asymmetric or symmetric procedures and the termination cost (which is low). The cost related to the secure communication phase is the sum of the energy needed for ciphering, integrity, and authentication. Finally, there is an energy cost linked to the transceiver. Simulation parameters were fixed using values from older works on the energy cost of cryptographic algorithms.

Works in the next subsection use their own model for the energy consumption, a common model taking into consideration each important block and the cost of each "consequence" does not exist. There is a need to propose general models able to grasp the cost of each security operation in a security solution.

C. Designing energy-efficient and energy-aware security solutions

Researchers remarked that security can impact the energy efficiency of IoT nodes. However, little research has tackled the ways to improve the energy efficiency of security solutions. As stated in [20], different energy-efficient mechanisms exist to take advantage of the available energy for security methods. These techniques are: online and offline security, outsourcing heavy computations, adaptive security, low-power security protocols, and size compression.

We present in this subsection a new taxonomy with four categories: lightweight protocols, energy-efficient solutions, adaptive security solutions, and context-aware security solutions.

Lightweight protocols (encryption and authentication) are designed to run on constrained nodes, energy-wise or computationally-wise.

Energy-efficient solutions use energy-efficient mechanisms to minimize the energy consumption of a given security solution.

Adaptive security solutions provide varying security levels in response to adaptive threats or various data types (adapt the security level to different data types). By adapting the security level to present threats or data, energy can be saved.

Context-aware security solutions consider the context to deliver an adapted security service; they may present similarities with adaptive security solutions.

In table V, we present the different surveyed solutions and classify them with regard to their category, the type of IoT network considered, and how energy is saved.

1) Lightweight protocols:

Lightweight protocols such as lightweight encryption and lightweight authentication are designed to cope with the constrained nature of IoT nodes. Research in this domain has increased in the past years and many surveys and lightweight methods have been designed. For instance, in [96], authors referenced lightweight cryptography algorithms for the IoT and classified them regarding their structure. They also provided a comparative study of the hardware and software performance of these algorithms and a security analysis.

In [76], authors provided two schemes for lightweight and mutual authentication and key agreement for IoT networks. The first scheme is designed for resource-constrained devices and considers the use of the elliptic curve Qu-Vanstone (ECQV) which is an implicit certificate scheme. The second scheme is based on certificateless authentication and key agreement (CL-AKA) and provides a slower but higher security level. In their simulations, they studied the overhead, which is lower than the majority of studied works and their schemes are faster than other works, but the second scheme is slower than the second scheme. However, the energy cost has not been studied in this work and they did not simulate their work in a heterogeneous network.

Seok et al. provided in [77] a secure Device to Device (D2D) communication system for 5G-based IoT networks. They used lightweight cryptography based on ECC and lightweight authenticated encryption with associated data (AEAD) ciphers. A token system based on ECDSA is used between IoT nodes and general Node-B (gNB, 5G base stations). They simulated their experiments and observed that AES had the highest delay compares to lightweight ciphers. Their system performs basic authentication using 5G-AKA and provides confidentiality and integrity of the exchanged data. It also provides anonymity and protection against impersonation attacks, eavesdropping, privacy sniffing, free-riding attacks, and location spoofing.

2) Energy-efficient security:

Energy-efficient security methods exploit different mechanisms for energy savings while providing an adequate security level. As stated previously, in [20], authors provided a first survey on energy-efficient mechanisms for IoT security solutions. In this subsection, we present recent solutions using energy-efficient mechanisms.

Kommuru et al. provided in [78] a scheme to reduce energy consumption while ensuring an adequate security level in WSNs. They used XOR encryption and asymmetric cryptography to secure the network while using PSO and LEACH to cluster nodes. They validated their solution in simulations and improved network lifetime compared to an approach only based on LEACH or PSO. However, they did not discuss the cost of their security method which may be high due to the use of asymmetric encryption.

Authors in [79] provided an outsourcing scheme called HELIOS for green WSNs. By outsourcing costly security operations in neighboring nodes, nodes with few energy may improve their lifetime. HELIOS is made of three methods: tHELIOS for trusted environments, dHELIOS for detection of malicious nodes, and iHELIOS for identification of malicious nodes. tHELIOS and dHELIOS decrease energy consumption of the delegating node, regardless of the chosen security level. iHELIOS increases the energy consumption of the delegating node for increasing the number of nodes and values of security levels.

Suslowicz et al. in [80] investigated the use of pre-computed values called coupons for security methods in IoT networks. Coupons can be used to optimize cryptographic operations that can be separated into an offline phase and an online phase. They are computed during the offline phase and used during the online phase. They validated their approach by using it on AES-CTR for key expansion and counter increments and observed that energy consumption and latency were reduced.

Fang et al. proposed in [81] two algorithms to send data in a single block or in multiple data blocks while considering security costs created by the headers. Security headers cause a supplementary but fixed cost (for a given security level). Each algorithm corresponds to a specific case: a case when nodes have harvested enough energy and a case when energy harvesting is not sufficient to supply the capacitor. Their simulations exposed that their algorithms achieved near-optimal results.

Authors provided in [82] a security solution based on ECC and MQTT to mitigate eavesdropping, replay attacks, and data tampering for IoT networks. Replay attacks and data tampering are managed by using a timestamp system along with a wake-up pattern mechanism. ECC is made energy-aware by assigning to each elliptic curve considered (193, 239, and 409 bit length), a key frequency exchange. When the available energy decreases, the method chooses a curve with a lower security level. Their model improved network lifetime during their experiments. However, as the available energy decreased, the number of messages exchanged for key re-generation increased, and the amount of energy spent in communications increased.

Mohd et al. in [83] provided a power-aware and adaptive encryption method. Their method maps different pre-

Article	Type of network	Class of security solutions	Concerned Security Solution(s)	How is energy saved?
[76]	Generic IoT	Lightweight authentication	Mutual authentication, ECQV	Use of lightweight cryptography
[77]	5G IoT	Lightweight authentication and encryption	D2D communications	Use of lightweight AEAD ciphers
[78]	WSNs	Energy-efficient security	XOR encryption	Use of LEACH and PSO to reduce the energy consumption of routing paths.
[79]	WSNs	Energy-efficient security	Discrete Log based schemes	Outsourcing.
[80]	Generic IoT	Energy-efficient security	AES-CTR, TRNG	Pre-computation.
[81]	Low-power sensors	Energy-efficient security	Lightweight encryption	Decide if data should be sent in one big packet or multiple packets with a security header for each packet.
[82]	Fog and edge IoT	Energy-efficient security	ECC	Choice of elliptic curve based on remaining energy
[83]	Generic IoT	Energy-efficient security	HIGHT Cipher	Mapping of different HIGHT implementations to pre-defined power levels.
[84]	5G IoT	Energy-efficient security	Anomaly detection in SDNs	A lightweight anomaly predetection module runs before activating a heavyweight detection module.
[85]	SDN-enabled IoT	Energy-efficient security	Public and private blockchain	Using both public and private blockchain in an SDN environment eliminates Proof of Work (PoW) and thus saves energy for all devices.
[86]	Generic IoT	Energy-efficient security	Adaptive encryption (AES)	Adaptive choice of AES method reduces energy consumption for resource constrained devices.
[87]	WSNs	Adaptive security	Secure MAC-Access, Key management	Energy levels considered and energy harvesting nodes.
[88]	5G-based IoT	Adaptive security	Adaptive encryption	Dynamic choice of a security level using reinforcement learning.
[89]	5G-based IoT	Adaptive security	Adaptive encryption	Adaptive security reduces energy consumption.
[90]	5G IoT	Adaptive security	Dummy signals countering rogue nodes	Optimization of security, privacy, energy consumption and QoS.
[91]	SDN-enabled IoT	Adaptive security	IEEE 802.15.4	Adaptive choice of a security level among the eight possible levels in function of threat level and available energy.
[92]	Smart home IoT network	Context-aware privacy	Differential privacy	Choice of the best energy offer which satisfies privacy to have energy savings.
[93]	Generic IoT	Context-aware security	Encryption methods	Choice of an adapted encryption method regarding the context and available energy.
[94]	Mobile devices	Context-aware security	AES, RC5, HMAC-MD5	Allocation of adapted security levels to a user and the places they will visit.
[95]	Mobile devices	Context-aware security	Not specified	Dynamic choice of a security level when arriving in a new place.

TABLE V
ENERGY-EFFICIENT AND ENERGY-AWARE SECURITY SOLUTIONS.

determined power levels to a particular encryption method. In their experiments, compared to static security levels (use of a single encryption method with a fixed number of rounds), their method consumed 39 % less energy than a method using 2 rounds and 32 iterations. 35 % of energy is saved compared to the encryption made with one round and 32 iterations.

Wang et al. in [84] provided a machine-learning based scheme, to detect anomalies in wireless SDNs. They designed an energy-efficient detection module made of a lightweight anomaly pre-detector and a heavyweight anomaly detector. The heavyweight anomaly detector uses machine learning and likelihood-based techniques to detect if suspicious flows are signs of DoS and DDoS attacks or not. Their module consumed less energy, had a better detection rate and an overall lower false positive rate than other machine-learning based detection schemes.

Yazdinejad et al. in [85] provided an efficient SDN controller architecture to secure IoT networks while reducing the energy consumption of all devices. A public blockchain is used between SDN controllers and private blockchain is used between the devices of an SDN domain (managed by an SDN controller). Authors managed to eliminate Proof of Work (PoW) by using both categories of blockchain. If a device has a malicious behavior, its ID is registered in the public blockchain and it is blacklisted. They validated the effectiveness of their method in simulations and observed a reduced latency along with a lower energy consumption.

Farooq et al. provided in [86] a security framework for IoT networks with a focus on heterogeneous and constrained devices. Their method picks a security level according to the available resources and the needed throughput. Authors solved a multi-objective optimization problem with the use of the Hungarian algorithm. In their experiments, their method has a higher average throughput and a lower average resource utilization than a greedy approach (maximizing the throughput).

3) Adaptive security solutions:

Adaptive security solutions provide an adapted security response toward evolving threats or different classes of data. By choosing a lower security level if there are few or no ongoing threats, energy can be saved.

Mauro in [87] considered the problem of security and channel access in energy harvesting WSNs (EH-WSNs). He discussed adaptive security by assigning to each packet p_i a security value $H(p_i)$, which is a pair (encryption method, authentication). Each receiver has a lower security capability value and a maximum capability value. These values are sent within the beacons to advertise their security level. Then a safe route can be chosen to transfer packets. Energy can also be considered to choose an adapted security scheme. Thus, it provides an energy-aware and adaptive security level.

In [88], the focus is on adaptive security using Reinforcement Learning (RL) and Deep Reinforcement Learning (DRL). The goal is to determine the optimal security policy to choose in an IoT network using 5G and User Equipments (UEs). The choice of a security solution regarding multiple parameters such as available energy, harvested energy, or consumed energy can be modeled as an Infinite Horizon Markov Decision

Process (MDP). Thus, the choice of a security context (4 available levels) is energy aware by using RL and DRL techniques. Each packet type (user plane, control plane, and network discovery messages) has a set of allowed security levels. Nodes can also harvest energy from their environment, which is considered in the environment model used in RL and DRL models.

Hellaoui et al. proposed in [89] an adaptive security framework based on coalitional games to choose the optimal security level (encryption method and key length) for IoT devices during the establishment phase. During the use phase, the network uses a trust system to monitor, detect threats, and take appropriate and adaptive security decisions. They validated their framework through extensive simulations and observed a reduced energy consumption compared to a static approach where only the highest security level is used.

Mohammed et al. in [90] presented UbiPriSEQ, a deep reinforcement learning scheme to guarantee privacy, security, QoS, and reduce energy consumption in 5G-based IoT networks. UbiPriSEQ provides security against rogue nodes and jamming attacks while ensuring privacy through Laplace mechanism. Nodes use less energy by offloading tasks to other nodes. UbiPriSEQ is evaluated in simulations and compared to an approach based on Constrained Markov Decision Process (CMDP), their approach provides better privacy, a lower latency, and a better average utility. However, authors did not provide details on how much energy was saved and on average, how many tasks were offloaded.

Mao et al. in [91] presented a scheme to secure IoT networks based on energy harvesting and SDNs. There exists a prediction of harvested energy for the m future time slots. Their model allocates a security level for those m future time slots while considering potential threats. Their simulations validated their method and improved network lifetime, and throughput. Moreover, IoT nodes needing privacy protection have a higher security level than other IoT nodes with non-sensitive data.

4) Context-aware security:

Context-awareness for IoT security solutions allows a node to consider the context in which it operates. Context-awareness can provide a form of intelligence [97] in IoT networks. These solutions may have a reduced energy consumption compared to classical approaches. We do not aim to survey in detail what are the different works regarding context-awareness and security in the IoT. For instance, context-aware security can consist in context-aware authentication [98], anomaly detection [99] or context-aware trust systems [100]. We present in this subsection, works that consider the context to provide an adapted security service while having a lower energy consumption.

Zhou et al. provided in [92] PRCOES to preserve the privacy of the users based on their context in a smart home environment. PRCOES is also designed to save energy of smart home devices. Their scheme chooses, using an online RL model, the best Energy Offer (EO). PRCOES protects the privacy of the users by using Laplace mechanism on EOs and Exponential mechanism on user data. Authors simulated a smart home environment and fulfilled user satisfaction while saving energy and preserving user privacy.

Roy et al. in [94] provided a method based on dynamic programming to provide a context-adaptive and energy-aware security for mobile devices. The underlying problem is to allocate a security level to each place the user goes in order to respect an energy budget and security requirements. The authors opted for an off-line approach where places do not have preferences regarding security levels. Authors provided a greedy heuristic to solve this optimization problem similar to the knapsack problem.

Authors in [95] continued the work done in [94] and provided an online algorithm for security allocation for mobile users under energy constraints. As opposed to the work in [94], places have to respect a minimum security level. They provided two algorithms to tackle this problem: a greedy algorithm and an efficient algorithm. They observed during simulations that the benefits of the efficient algorithm are higher than those of the greedy algorithm. However, the greedy algorithm always allocates a security level, as opposed to the efficient algorithm which is a clear limit.

Massad et al. provided in [93] a scheme called MQTTSec (Secure MQTT) enhancing MQTT v5. MQTTSec consists of a selection algorithm, CASA, to choose an encryption algorithm given the context and available energy. MQTTSec also enhances CONNECT and CONNACK messages by adding new fields to those messages. They created a small test-bed and considered AES, DES, RSA, and Blowfish for the set of available encryption methods. Authors stated that MQTTSec provides security against multiple attacks such as broker impersonation attacks, eavesdropping, chosen plaintext attacks, chosen ciphertext attack, man-in-the-middle attack, and cryptanalysis.

D. Remarks and lessons learned

There is an increasing literature on benchmarks of encryption, authentication, and signature methods. The common point among these papers is that the energy consumption of AES is not negligible [71]–[73]. Moreover, lightweight encryption methods (such as SPECK or SIMON) are not the primary choice in lightweight or energy-efficient methods. ECC and AES are widely used in lightweight security solutions as they provide a good security level [80], [82], [86] and a widespread literature. However, neither ECC and AES are lightweight, compared to other methods. Thakor et al. present many lightweight encryption algorithms (with a software or hardware implementation) in [96] which may provide a sufficient security level with a lower energy consumption. The results exposed by Schaumont in [66] outline that the choice of ECDSA may not the best choice for small and heavily energy-constrained devices. Offloading heavy computations as presented in [79] may alleviate constrained nodes and improve their lifetime while guaranteeing a sufficient security. Encryption, authentication, and signature algorithms are the primary brick to ensure security primitives. If manufacturers and developers carefully choose appropriate methods, their

products may have a longer lifetime than those using only AES or ECDSA for instance.

Furthermore, as explained in section II, only Hellaoui et al. in [20] surveyed energy-efficient mechanisms for IoT security. Since 2017, more energy-aware security methods have been proposed by researchers. Authors in [83] provided power-aware encryption. But the approach is static with regard to threats because with decreasing energy levels, the security provided by the cipher decreases. Other methods using learning approaches [88], [90] or game-based approaches [89] for 5G-based IoT networks provide sufficient security against adaptive threats.

Context-aware security and privacy solutions use multiple data sources (historical data and contextual data, neighbor nodes, and servers) to secure an IoT network (or node). The solutions we have surveyed are energy-aware and context-aware. Both [94] and [95] considered context and user's energy budget to choose a security level when they arrive in a new place. Context-awareness combined with energy-awareness may provide improved security and better energy management. These solutions may consume less energy compared to a static approach. However, in [94] and [95], authors did not provide comparisons with static approaches for the energy costs. What is the result if only the highest (or lowest) security level is used in each place?

VI. Discussion and challenges

As IoT is used in many fields, some solutions are more appropriate due to the consideration of field-related parameters and environment constraints. In figure 5, we remind the different categories of solutions we have surveyed in the previous section (section V) which aim to balance security and their energy consumption.

A. Summary of studied solutions

Lightweights protocols [76], [77], [96] (authentication, encryption) are useful for resource-constrained nodes, since computational power and energy are limited. However, these protocols are static and offer only a fixed security level. They need to be combined with other methods to have a better consideration of energy and threats. Thus, they may be considered as a building block for future security solutions.

Energy-efficient security solutions can consider the use of lightweight protocols and use energy-efficiency mechanisms (described in [20]) to lighten the energy cost of such protocols. These solutions may also be limited in the security service provided. They may also adapt the security service to the remaining energy but not necessarily to threats, data, or users.

Adaptive security methods can cover a variety of threats by adapting the security level to the treat or data sensitivity [89]–[91]. In our study, these solutions are energy-aware and may use various lightweight protocols to provide an adapted security level with a decreased energy consumption. These solutions are dynamic with regard to the provided security service. The choice of an adapted security level instead of a static security level may save energy in the long run.

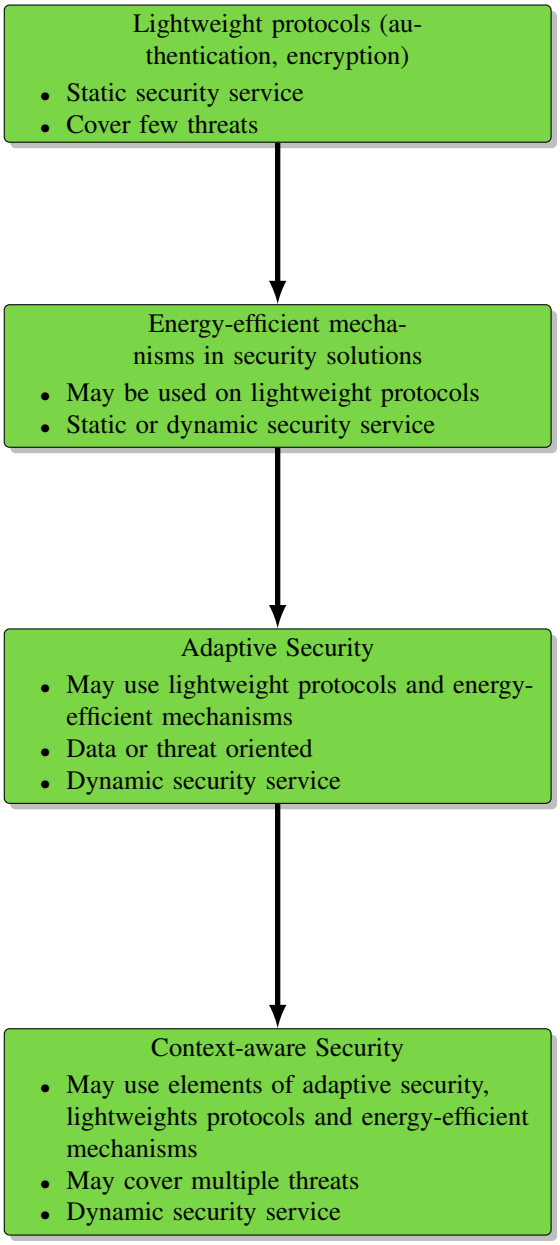

Fig. 5. Characteristics of surveyed IoT security solutions which may save energy while providing an adequate security service. Complexity, flexibility and potential saved energy increase from top to bottom.

Finally, context-aware security methods can cover a variety of threats and provide an adaptive security level by observing the context and taking an appropriate decision. Due to the use of multiple data sources (historical, environmental observations, network traces, trust sources ...), implementing a context-aware security solution is far more complex than using a simple lightweight protocol. The dynamism behind context-aware security solutions make them useful and appropriate for mobile IoT nodes [94], [95]. It may appear natural to merge context-aware security and adaptive security to exploit possible synergies between them.

Security approaches / Energy approaches	Energy-efficient security methods	Adaptive security	Context-aware security
Energy management methods	[78], [85]	X	X
Energy harvesting	[79]–[81]	[87], [88], [91]	X
Wireless charging	X	X	X
No particular mechanism used	[82]–[84], [86]	[89], [90]	[92]–[95]

TABLE VI
CLASSIFICATION OF STUDIED WORKS WITH REGARD TO ENERGY MANAGEMENT OR HARVESTING METHODS THEY USE AND THE SECURITY CLASSES THEY BELONG TO.

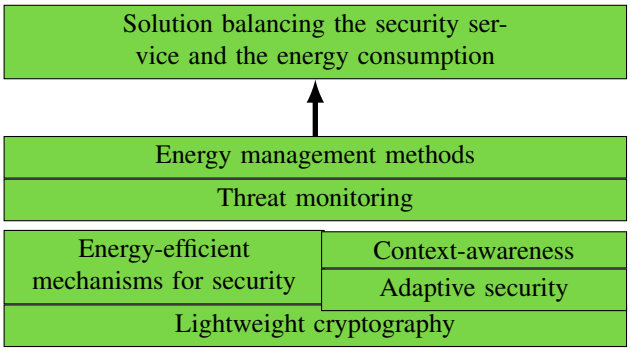

Fig. 6. Elements needed to provide a security solution balancing the provided security level and energy consumption.

B. Issues and challenges

There is an urgent need to design security solutions covering multiple threats and suited to heterogeneous IoT networks. However, as they are resource-constrained, it is impossible to cover each existing threat. Depending on the application domain, some threats are more present and should be the focus of the security system deployed. Available energy must be considered while designing and implementing security solutions as the induced energy cost is non-negligible [65]. This cost is caused by the use of the radio transceiver and the MCU which consume a lot of energy. Hence, heavy security solutions should not be implemented at the expanse of the applications running in an IoT node, especially when these applications are energy-demanding.

With our classification, we identified the main blocks and concepts to develop energy-efficient and effective security solutions for IoT networks. Firstly, lightweight encryption and authentication methods should be used as the building blocks. Alternatives should be used instead of always considering AES due to the important cost if no dedicated hardware implementations are used [71]. The same remark applies to ECC [65]. Secondly, energy-efficient mechanisms (and energy-awareness) are the second block to consider to reduce the energy consumption of this security solution. Thirdly, adaptive security concepts may prove useful to continuously adapt the security level to a plethora of threats. Then, context-awareness may give additional information from the environment and the users to the security solution in order to fine-tune the choice of a security level. Combining the concepts of adaptive security and context-aware security may improve security while reducing the energy consumption of the security tasks. On one hand, if the environment is safe and fully trusted, a low security level might be applied to save more energy. In another hand, if the environment becomes insecure, the highest security level may be applied. Moreover, network administrators and developers may use threat monitoring systems to improve the choice of a security level, along with the context-aware and adaptive security modules. In figure 6, we summarize the main building blocks to consider in order to have a global security solution minimizing the energy consumption in fully trusted or untrusted environments while providing an adequate security level.

Energy-efficient mechanisms for security solutions are not the only way to have a balance between energy and security. As presented in table VI, some IoT security solutions may use (or be built upon) energy management or harvesting methods. Indeed, energy harvesting and energy saving mechanisms can lead to energy savings when used in security solutions [66], [80]. If hardware constructors design harvesting units with dedicated MCUs for cryptographic operations [101], other MCUs or chips can have more energy and power dedicated to other tasks and balance security with energy consumption. However, according to the authors in [102], asynchronous duty-cycling may negatively impact the energy consumption induced by security solutions. This point requires further research for different duty-cycling protocols.

Mobile chargers [42], [44] may also be considered to extend network lifetime and reduce maintenance costs. However, the use of such robots has a cost, and recharge time relies on antenna efficiency and distances. If there are unreachable nodes or impassable fields, other methods to replenish batteries and operators may be required. These mobile chargers may also be mobile nodes dedicated to heavy computations. Indeed, computation offloading in mobile edge computing nodes (MEC) is a topic of interest in research [103]. Offloading and outsourcing security operations in mobile robots could be an interesting way to manage heavy security operations and thus, nodes with constrained resources may save more energy. However, to the best of our knowledge, no work considered the use of mobile chargers to help securing IoT networks as shown in table VI.

Operators may also use SDN to secure and reduce energy consumption of IoT networks. Authors in [104] surveyed both energy-efficient mechanisms for SDNs and possible security solutions. Authors in [85] proposed an energy-efficient SDN controller along the use of blockchain technology (public and private blockchains) to secure and reduce the energy consumption of all devices in the network. SDN is a promising technology and may be used along 5G networks [84].

Another possible method to optimize both security and energy consumption is the use of learning methods. Authors

considered this approach in [90] to optimize QoS, security, privacy and energy consumption for 5G IoT networks. Conceição in [88] used reinforcement learning to dynamically attribute security levels along the use of energy harvesting in 5G IoT networks. On the contrary, authors in [91] favored an approach based on optimization to find the best security suite for a given time cycle. However, using learning methods such as reinforcement learning or deep learning may incur an additional complexity and sometimes, these solutions may not scale well. Some solutions we surveyed in section IV may scale well, others may be not practical in real IoT environments. Moreover, some solutions consider real-time and constrained environments (such as UAV networks [60]), but no practical information on the feasibility is given. In table VII, we sum up the characteristics of each security solution using a learning method.

We believe that researchers should pursue further research in this field to improve network lifetime along securing IoT devices. Moreover, combining adaptive security and context-aware security may improve network protection against advanced threats. In addition, such solutions may consider energy constraints, user needs, security requirements, and other attributes to continuously adapt the security services with regard to the available resources. There is research in the field of green IoT, energy-efficient IoT, security for IoT, energy-efficient security, but research tackling both green IoT and energy-efficient security in IoT is scarce. Authors in [105] advocate the need of research in the field of sustainable security for IoT. We also think that more research needs to be done in this field. The energy cost of security solutions cannot be ignored anymore.

VII. Conclusion

Security is needed due to the increasing number of threats and sensitive data but this will increase energy consumption and deplete batteries. Thus, there is a need to design security solutions that can efficiently protect IoT networks with a controlled energy consumption to maximize network lifetime.

Toward this end, we have taken a different approach in this survey compared to the majority of existing surveys on IoT security which were only focused on the security of IoT networks. We studied both energy management methods and recent security solutions and showed the limits of those solutions. Then, we discussed the cost associated with security primitives. After that, we presented classes of recent security solutions which can have a decreased energy consumption while providing appropriate security service in a static or dynamic manner. We classified these security solutions into four classes, namely lightweight protocols, energy-efficient methods, adaptive security methods, and context-aware security methods. We also proposed a set of elements needed to design an energy-efficient and secure IoT solution based on the classification we provided. New approaches based on artificial intelligence or software-defined networking may reduce energy consumption while securing IoT networks. This survey proposes new research challenges linked to the balance of security and energy consumption and we hope that it will inspire researchers and industries to further develop energy-efficient security solutions for IoT networks.

Our future work will focus on intelligent and energy-aware security solutions for large-scale IoT networks. Learning approaches, along optimization, may provide the keys needed to balance energy and security. Moreover, the use of particular technologies such as SDN and energy-harvesting, may further improve the network lifetime and provide more tools for security.

References

[1] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A Survey on Internet of Things From Industrial Market Perspective," *IEEE Access*, vol. 2, pp. 1660–1679, 2014.

[2] H. F. Atlam, R. Walters, and G. Wills, "Internet of Things: State-of-the-art, challenges, applications, and open issues," *International Journal of Intelligent Computing Research (IJICR)*, vol. 9, no. 3, pp. 928–938, Sep. 2018.

[3] S. Balaji, K. Nathani, and R. Santhakumar, "IoT Technology, Applications and Challenges: A Contemporary Survey," *Wireless Personal Communications*, vol. 108, no. 1, pp. 363–388, Sep. 2019.

[4] M. Raj, S. Gupta, V. Chamola, A. Elhence, T. Garg, M. Atiquzzaman, and D. Niyato, "A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0," *Journal of Network and Computer Applications*, vol. 187, p. 103107, Aug. 2021.

[5] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, Jul. 2015.

[6] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, "Internet of Things (IoT) and the Energy Sector," *Energies*, vol. 13, no. 2, p. 494, Jan. 2020.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[8] F. Javed, M. K. Afzal, M. Sharif, and B.-S. Kim, "Internet of Things (IoT) Operating Systems Support, Networking Technologies, Applications, and Challenges: A Comparative Review," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2062–2100, 2018.

[9] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? a Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[10] S. H. Alsamhi, O. Ma, M. S. Ansari, and Q. Meng, "Greening internet of things for greener and smarter cities: A survey and future prospects," *Telecommunication Systems*, vol. 72, no. 4, pp. 609–632, Dec. 2019.

[11] D. K. Sah and T. Amgoth, "Renewable energy harvesting schemes in wireless sensor networks: A Survey," *Information Fusion*, vol. 63, pp. 223–247, Nov. 2020.

[12] T. Sanislav, G. D. Mois, S. Zeadally, and S. C. Folea, "Energy Harvesting Techniques for Internet of Things (IoT)," *IEEE Access*, vol. 9, pp. 39 530–39 549, 2021.

[13] 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. 82 721–82 743, 2019.

[14] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, Aug. 2018.

[15] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications*, vol. 161, p. 102630, Jul. 2020.

[16] M. binti Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, Jan. 2019.

[17] R. Yugha and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," *Journal of Network and Computer Applications*, vol. 169, p. 102763, Nov. 2020.

[18] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2702–2733, thirdquarter 2019.

Articles	Application domain(s)	Algorithm(s)	Real-time	Scalable	Reduced energy consumption of security?
[56]	Smart home	Best results: Random forests + PCA	Yes	No	No
[58]	Generic WSNs	MLP	Yes	Yes	No
[59]	Generic IoT	Variational autoencoders	Not studied	Not studied	No
[60]	UAV networks	Deep Belief Networks	Not studied	Not studied	No
[61]	Fog-based IoT	Q-learning	Yes	Yes	No
[84]	Wireless SDNs	Statistical learning (contrastive pessimistic likelihood estimation)	Yes	Yes	Yes
[88]	5G-based IoT	SARSA, Q-learning, Double Q-learning, Actor-critic (Deep-RL)	Yes	Yes	Yes
[92]	Smart home	Contextual bandits (RL)	Yes	No	Yes

TABLE VII
SECURITY SOLUTIONS BASED ON LEARNING METHODS SURVEYED IN THIS ARTICLE.

[19] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 616–644, Firstquarter 2020.

[20] 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, Nov. 2017.

[21] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, "Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review," *Journal of Network and Computer Applications*, vol. 190, p. 103118, Sep. 2021.

[22] P. Tedeschi, S. Sciancalepore, and R. D. Pietro, "Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges," *IEEE Communications Surveys Tutorials*, vol. 22, no. 4, pp. 2658–2693, Fourthquarter 2020.

[23] R. Arshad, S. Zahoor, M. A. Shah, A. Wahid, and H. Yu, "Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond," *IEEE Access*, vol. 5, pp. 15 667–15 681, 2017.

[24] S. F. Abedin, M. G. R. Alam, R. Haw, and C. S. Hong, "A system model for energy efficient green-IoT network," in *2015 International Conference on Information Networking (ICOIN)*, Jan. 2015, pp. 177–182.

[25] G. Jaber, R. Kacimi, L. A. Grieco, and T. Gayraud, "An adaptive duty-cycle mechanism for energy efficient wireless sensor networks, based on information centric networking design," *Wireless Networks*, vol. 26, no. 2, pp. 791–805, Feb. 2020.

[26] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, Oct. 2002.

[27] A. Rashid, F. Khan, T. Gul, S. Ali, S. Khan, and F. K. Khalil, "Improving Energy Conservation in Wireless Sensor Networks using Energy Harvesting System," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, p. 8, 2018.

[28] C. Wang, J. Li, Y. Yang, and F. Ye, "Combining Solar Energy Harvesting with Wireless Charging for Hybrid Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 17, no. 3, pp. 560–576, Mar. 2018.

[29] J. Huang, Y. Meng, X. Gong, Y. Liu, and Q. Duan, "A Novel Deployment Scheme for Green Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 196–205, Apr. 2014.

[30] K. Wang, Y. Wang, Y. Sun, S. Guo, and J. Wu, "Green Industrial Internet of Things Architecture: An Energy-Efficient Perspective," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 48–54, Dec. 2016.

[31] O. Said, Z. Al-Makhadmeh, and A. Tolba, "EMS: An Energy Management Scheme for Green IoT Environments," *IEEE Access*, vol. 8, pp. 44 983–44 998, 2020.

[32] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan, and M. Jo, "Efficient Energy Management for the Internet of Things in Smart Cities," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 84–91, Jan. 2017.

[33] J. Curry and N. Harris, "Powering the Environmental Internet of Things," *Sensors*, vol. 19, no. 8, p. 1940, Jan. 2019.

[34] A. S. Adila, A. Husam, and G. Husi, "Towards the self-powered Internet of Things (IoT) by energy harvesting: Trends and technologies for green IoT," in *2018 2nd International Symposium on Small-Scale Intelligent Manufacturing Systems (SIMS)*, Apr. 2018, pp. 1–5.

[35] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the Internet of Things," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102–108, Jun. 2015.

[36] S. Bi, C. K. Ho, and R. Zhang, "Wireless powered communication: Opportunities and challenges," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 117–125, Apr. 2015.

[37] D. Mishra, S. De, S. Jana, S. Basagni, K. Chowdhury, and W. Heinzelman, "Smart RF energy harvesting communications: Challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 70–78, Apr. 2015.

[38] A. Kansal, J. Hsu, M. Srivastava, and V. Raqhunathan, "Harvesting aware power management for sensor networks," in *2006 43rd ACM/IEEE Design Automation Conference*, Jul. 2006, pp. 651–656.

[39] A. Cammarano, C. Petrioli, and D. Spenza, "Pro-Energy: A novel energy prediction model for solar and wind energy-harvesting wireless sensor networks," in *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, Oct. 2012, pp. 75–83.

[40] J. R. Piorno, C. Bergonzini, D. Atienza, and T. S. Rosing, "Prediction and management in energy harvested wireless sensor nodes," in *2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology*, May 2009, pp. 6–10.

[41] S. Kosunalp, "A New Energy Prediction Algorithm for Energy-Harvesting Wireless Sensor Networks With Q-Learning," *IEEE Access*, vol. 4, pp. 5755–5763, 2016.

[42] K. Abid, G. Jaber, H. Lakhlef, A. Lounis, and A. Bouabdallah, "An Energy Efficient Architecture of self-sustainable WSN based on Energy Harvesting and Wireless Charging with Consideration of Deployment Cost," in *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet '20. New York, NY, USA: Association for Computing Machinery, Nov. 2020, pp. 109–114.

[43] W. Na, J. Park, C. Lee, K. Park, J. Kim, and S. Cho, "Energy-Efficient Mobile Charging for Wireless Power Transfer in Internet of Things Networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 79–92, Feb. 2018.

[44] N. Gharaei, Y. D. Al-Otaibi, S. A. Butt, S. J. Malebary, S. Rahim, and G. Sahar, "Energy-Efficient Tour Optimization of Wireless Mobile Chargers for Rechargeable Sensor Networks," *IEEE Systems Journal*, vol. 15, no. 1, pp. 27–36, Mar. 2021.

[45] A. Hameed and A. Alomary, "Security Issues in IoT: A Survey," in *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sep. 2019, pp. 1–5.

[46] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, "ECCbAP: A secure ECC-based authentication protocol for IoT edge devices," *Pervasive and Mobile Computing*, vol. 67, p. 101194, Sep. 2020.

[47] M. Ghahramani, R. Javidan, M. Shojafar, R. Taheri, M. Alazab, and R. Tafazolli, "RSS: An Energy-Efficient Approach for Securing IoT Service Protocols Against the DoS Attack," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3619–3635, Mar. 2021.

[48] D. Chen, W. Yang, J. Hu, Y. Cai, and X. Tang, "Energy-Efficient Secure Transmission Design for the Internet of Things With an Untrusted Relay," *IEEE Access*, vol. 6, pp. 11 862–11 870, 2018.

[49] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A Software Defined Networking architecture for the Internet-of-Things," in *2014 IEEE Network Operations and Management Symposium (NOMS)*, May 2014, pp. 1–9.

[50] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A

Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[51] T. H. Szymanski, "Security and Privacy for a Green Internet of Things," *IT Professional*, vol. 19, no. 5, pp. 34–41, 2017.

[52] Z. Li, M. Shahidehpour, and X. Liu, "Cyber-secure decentralized energy management for IoT-enabled active distribution networks," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 900–917, Sep. 2018.

[53] L. Yang, X.-Y. Liu, and W. Gong, "Secure Smart Home Systems: A Blockchain Perspective," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 1003–1008.

[54] M. M. Hasan and H. T. Mouftah, "Optimal Trust System Placement in Smart Grid SCADA Networks," *IEEE Access*, vol. 4, pp. 2907–2919, 2016.

[55] S. Boudko and H. Abie, "Adaptive Cybersecurity Framework for Healthcare Internet of Things," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, May 2019, pp. 1–6.

[56] Y. Wan, K. Xu, G. Xue, and F. Wang, "IoTArgos: A Multi-Layer Security Monitoring System for Internet-of-Things in Smart Homes," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, Jul. 2020, pp. 874–883.

[57] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1646–1685, thirdquarter 2020.

[58] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in *2009 International Joint Conference on Neural Networks*, Jun. 2009, pp. 1680–1687.

[59] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the Classification Effectiveness of Intrusion Detection by Using Improved Conditional Variational AutoEncoder and Deep Neural Network," *Sensors*, vol. 19, no. 11, p. 2528, Jan. 2019.

[60] X. Tan, S. Su, Z. Zuo, X. Guo, and X. Sun, "Intrusion Detection of UAVs Based on the Deep Belief Network Optimized by PSO," *Sensors*, vol. 19, no. 24, p. 5529, Jan. 2019.

[61] S. Tu, M. Waqas, S. U. Rehman, M. Aamir, O. U. Rehman, Z. Jianbiao, and C. Chang, "Security in Fog Computing: A Novel Technique to Tackle an Impersonation Attack," *IEEE Access*, vol. 6, pp. 74 993–75 001, 2018.

[62] A. Uprety and D. B. Rawat, "Reinforcement Learning for IoT Security: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8693–8706, Jun. 2021.

[63] S. Alharby, N. Harris, A. Weddell, and J. Reeve, "The Security Trade-Offs in Resource Constrained Nodes for IoT Application," *International Journal of Electronics and Communication Engineering*, vol. 12, no. 1, p. 9, 2018.

[64] G. de Meulenaer, F. Gosset, F. Standaert, and O. Pereira, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Oct. 2008, pp. 580–585.

[65] P. Schaumont, B. Yuce, K. Pabbuleti, and D. Mane, "Secure authentication with energy-harvesting: A multi-dimensional balancing act," *Sustainable Computing: Informatics and Systems*, vol. 12, pp. 83–95, Dec. 2016.

[66] P. Schaumont, "Security in the Internet of Things: A challenge of scale," in *Design, Automation Test in Europe Conference Exhibition (DATE), 2017*, Mar. 2017, pp. 674–679.

[67] L. M. Vračar, M. D. Stojanović, A. S. Stanimirović, and Z. D. Prijić, "Influence of Encryption Algorithms on Power Consumption in Energy Harvesting Systems," https://www.hindawi.com/journals/js/2019/8520562/, p. e8520562, Apr. 2019.

[68] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm," in *Fast Software Encryption*. Springer, Berlin, Heidelberg, Dec. 1994, pp. 363–366.

[69] R. M. Needham and D. J. Wheeler, "Tea extensions," *Report, Cambridge University*, 1997.

[70] E. F. Brickell, D. E. Denning, S. T. Kent, D. P. Maher, and W. Tuchman, "SKIPJACK review," *Interim Report: The Skipjack Algorithm*, 1993.

[71] S. Maitra and K. Yelamarthi, "Rapidly Deployable IoT Architecture with Data Security: Implementation and Experimental Evaluation," *Sensors*, vol. 19, no. 11, p. 2484, Jan. 2019.

[72] L. E. Kane, J. J. Chen, R. Thomas, V. Liu, and M. Mckague, "Security and Performance in IoT: A Balancing Act," *IEEE Access*, vol. 8, pp. 121 969–121 986, 2020.

[73] E. Aerabi, M. Bohlouli, M. H. A. Livany, M. Fazeli, A. Papadimitriou, and D. Hely, "Design Space Exploration for Ultra-Low-Energy and Secure IoT MCUs," *ACM Transactions on Embedded Computing Systems*, vol. 19, no. 3, pp. 19:1–19:34, May 2020.

[74] B. Girgenti, P. Perazzo, C. Vallati, F. Righetti, G. Dini, and G. Anastasi, "On the Feasibility of Attribute-Based Encryption on Constrained IoT Devices for Smart Systems," in *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*, Jun. 2019, pp. 225–232.

[75] F. Conceição, N. Oualha, and D. Zeghlache, "An Energy Model for the IoT: Secure Networking Perspective," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2018, pp. 1–5.

[76] D.-H. Lee and I.-Y. Lee, "A Lightweight Authentication and Key Agreement Schemes for IoT Environments," *Sensors*, vol. 20, no. 18, p. 5350, Jan. 2020.

[77] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, "Secure D2D Communication for 5G IoT Network Based on Lightweight Cryptography," *Applied Sciences*, vol. 10, no. 1, p. 217, Jan. 2020.

[78] K. J. S. R. Kommuru, K. K. Y. Kadari, and B. K. R. Alluri, "A Novel Approach to Balance the Trade-Off between Security and Energy Consumption in WSN," in *2018 2nd International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, Sep. 2018, pp. 85–90.

[79] G. Ateniese, G. Bianchi, A. T. Capossele, C. Petrioli, and D. Spenza, "HELIOS: Outsourcing of Security Operations in Green Wireless Sensor Networks," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Jun. 2017, pp. 1–7.

[80] C. Suslowicz, A. S. Krishnan, and P. Schaumont, "Optimizing Cryptography in Energy Harvesting Applications," in *Proceedings of the 2017 Workshop on Attacks and Solutions in Hardware Security*, ser. ASHES '17. New York, NY, USA: Association for Computing Machinery, Nov. 2017, pp. 17–26.

[81] X. Fang, M. Yang, and W. Wu, "Security Cost Aware Data Communication in Low-Power IoT Sensors with Energy Harvesting," *Sensors*, vol. 18, no. 12, p. 4400, Dec. 2018.

[82] F. De Rango, G. Potrino, M. Tropea, and P. Fazio, "Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks," *Pervasive and Mobile Computing*, vol. 61, p. 101105, Jan. 2020.

[83] B. J. Mohd, K. M. A. Yousef, A. AlMajali, and T. Hayajneh, "Power-Aware Adaptive Encryption," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Apr. 2019, pp. 711–716.

[84] B. Wang, Y. Sun, and X. Xu, "A Scalable and Energy-Efficient Anomaly Detection Scheme in Wireless SDN-Based mMTC Networks for IoT," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1388–1405, Feb. 2021.

[85] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625–638, Jul. 2020.

[86] U. Farooq, N. Ul Hasan, I. Baig, and N. Shehzad, "Efficient adaptive framework for securing the Internet of Things devices," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 210, Aug. 2019.

[87] A. D. Mauro, "On the Impact of Energy Harvesting on Wireless Sensor Network Security," 2015.

[88] F. Conceicao, "Network survival with energy harvesting : Secure cooperation and device assisted networking," Ph.D. dissertation, Université Paris Saclay (COmUE), Nov. 2019.

[89] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy Efficiency in Security of 5G-Based IoT: An End-to-End Adaptive Approach," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6589–6602, Jul. 2020.

[90] T. Mohammed, A. Albeshri, I. Katib, and R. Mehmood, "UbiPriSEQ—Deep Reinforcement Learning to Manage Privacy, Security, Energy, and QoS in 5G IoT HetNets," *Applied Sciences*, vol. 10, no. 20, p. 7120, Jan. 2020.

[91] B. Mao, Y. Kawamoto, J. Liu, and N. Kato, "Harvesting and Threat Aware Security Configuration Strategy for IEEE 802.15.4 Based IoT Networks," *IEEE Communications Letters*, vol. 23, no. 11, pp. 2130–2134, Nov. 2019.

[92] P. Zhou, G. Zhong, M. Hu, R. Li, Q. Yan, K. Wang, S. Ji, and D. Wu, "Privacy-Preserving and Residential Context-Aware Online Learning for IoT-Enabled Energy Saving With Big Data Support in Smart Home Environment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7450–7468, Oct. 2019.

[93] M. A. Massad and B. A. Alsaify, "MQTTSec Based on Context-Aware Cryptographic Selection Algorithm (CASA) for Resource-Constrained IoT Devices," in *2020 11th International Conference on Information and Communication Systems (ICICS)*, Apr. 2020, pp. 349–354.

[94] S. Roy, S. Sankaran, P. Singh, and R. Sridhar, "Modeling Context-Adaptive Energy-Aware Security in Mobile Devices," in *2018 IEEE 43rd Conference on Local Computer Networks Workshops (LCN Workshops)*, Oct. 2018, pp. 105–109.

[95] A. Asaithambi, A. Dutta, C. Rao, and S. Roy, "Online Context-Adaptive Energy-Aware Security Allocation in Mobile Devices: A Tale of Two Algorithms," in *Distributed Computing and Internet Technology*, D. V. Hung and M. D´Souza, Eds. Cham: Springer International Publishing, 2020, pp. 281–295.

[96] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28 177–28 193, 2021.

[97] B. Chatterjee, N. Cao, A. Raychowdhury, and S. Sen, "Context-Aware Intelligence in Resource-Constrained IoT Nodes: Opportunities and Challenges," *IEEE Design Test*, vol. 36, no. 2, pp. 7–40, Apr. 2019.

[98] M. Loske, L. Rothe, and D. G. Gertler, "Context-Aware Authentication: State-of-the-Art Evaluation and Adaption to the IIoT," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Apr. 2019, pp. 64–69.

[99] A. K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac, "Aegis: A context-aware security framework for smart home systems," in *Proceedings of the 35th Annual Computer Security Applications Conference*, ser. ACSAC '19. New York, NY, USA: Association for Computing Machinery, Dec. 2019, pp. 28–41.

[100] Y. Hussain, H. Zhiqiu, M. A. Akbar, A. Alsanad, A. A. Alsanad, A. Nawaz, I. A. Khan, and Z. U. Khan, "Context-Aware Trust and Reputation Model for Fog-Based IoT," *IEEE Access*, vol. 8, pp. 31 622–31 632, 2020.

[101] J. Li, J. H. Hyun, and D. SamHa, "A Multi-Source Energy Harvesting System to Power Microcontrollers for Cryptography," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2018, pp. 901–906.

[102] S. Alharby, N. Harris, A. Weddell, and J. Reeve, "Impact of duty cycle protocols on security cost of IoT," in *2018 9th International Conference on Information and Communication Systems (ICICS)*, Apr. 2018, pp. 25–30.

[103] M. Min, L. Xiao, Y. Chen, P. Cheng, D. Wu, and W. Zhuang, "Learning-Based Computation Offloading for IoT Devices With Energy Harvesting," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1930–1941, Feb. 2019.

[104] D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 325–346, 2017.

[105] M. De Donno, K. M. Malarski, X. Fafoutis, N. Dragoni, M. N. Petersen, M. S. Berger, and S. Ruepp, "Sustainable Security for Internet of Things," in *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*, Dec. 2019, pp. 1–4.