IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 8, 2019, accepted April 8, 2019, date of publication April 15, 2019, date of current version April 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2911424

Energy Depletion Attacks in Low Power Wireless Networks

VAN-LINH NGUYEN, PO-CHING LIN, AND REN-HUNG HWANG
Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 62102, Taiwan

Corresponding author: Van-Linh Nguyen (nvlinh@cs.ccu.edu.tw)

This work was supported in part by the Ministry of Science and Technology of Taiwan, ROC, under Grant MOST 107-2218-E-194-014, and in part by the Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU).

ABSTRACT Low Power Wireless (LPW) networks have recently been emerging as key candidates to offer affordable connectivity for the constrained devices in the Internet of Things (IoT). However, they also raise major security concerns due to the inherent security vulnerabilities of built-in communication protocols. By exploiting these flaws, an adversary can attack sensors or actuators in an LPW network and force them to execute energy-hungry tasks such as verifying unauthenticated garbage messages repeatedly. This attack, namely energy depletion attack (EDA), can drain the batteries of the devices rapidly and lead to soaring network-wide energy expenditure. Consequently, the offense can leave the victims disabled, and even shut down the whole network due to the battery exhaustion of all the devices. In this paper, we investigate existing studies and provide a systematic review of EDAs and defenses in LPW networks. Through this work, we conclude that most existing LPW technologies are vulnerable to EDAs. This paper also indicates the security challenges in LPW networks related to EDAs along with the potential research directions. While LPW technologies have already hit the market with the promising deployment schedules, our attempt can inspire the research community to enhance the security of underlying protocols that will shape the connectivity of billions of devices in the future IoT ecosystem.

INDEX TERMS Energy depletion attacks, IoT security, IoT embedded devices, low power wireless sensor networks.

I. INTRODUCTION

Internet of Things (IoT) technologies are booming and promising to reshape the way of human interaction. According to IHS Statista 2018 [1], the number of IoT devices can soar over 70 billion in 2025, and 70% of them will be low-power and low-cost devices. Low Power Wireless (LPW) technologies appear to offer communications for these devices. We believe that the LPW technologies will have great success shortly due to their promises in shaping the connectivity of billions of IoT devices. However, the biggest challenge of LPW networks is to keep LPW devices in secure communication, while satisfying the lifetime requirement of these devices, e.g., for years. Due to the low cost and limited energy, LPW devices may not come with the state-of-the-art and reliable security mechanisms [2]. This problem potentially opens the door for security vulnerability exploitation, including the energy depletion attacks (EDAs).

EDAs involve a long history of variants that cause severe damage, in which successful cases were practically found in existing networks such as wireless sensor networks (WSN) [3], [4]. The idea of an EDA was first known as a sleep deprivation torture or battery exhaustion attack against handheld devices with a limited power source, e.g., mobile computers [5]. In a formal attack model, an adversary targets to drain the battery of a device, for example, by having the device repeatedly execute an energy-hungry program; once the battery runs out, the attacker can stop and walk away, leaving the victim disabled. Leveraging this kind of attack, an adversary can destabilize the network by depleting the battery of important sensors or a large number of devices in a place. The apparent consequence is to lead high maintenance cost, and sometimes the replacement is prohibitively expensive, such as that for sensors mounted on the body of objects or scattered across a wide range of inaccessible terrain.

With the explosion of low-cost IoT devices, the EDA is a comprehensive approach to destroy the network infrastructure in a wide range or cause massive damage, especially if the sensors are the fundamental parts (e.g., temperature monitoring) of a critical system [2]. Fig. 1 illustrates a potential

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

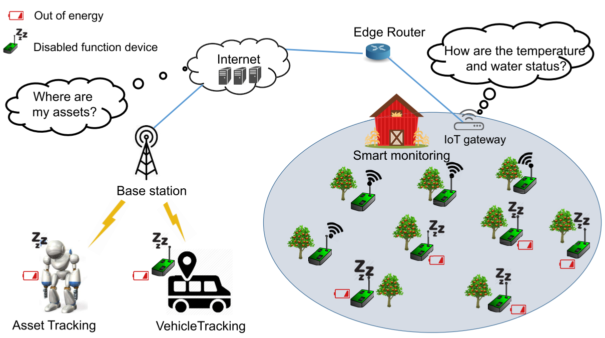

FIGURE 1. The illustration of EDAs and their clear consequences to several business sectors such as asset tracking. In the case of asset tracking, there is no way to track the asset status if the embedded tracking devices are off due to energy exhaustion.

consequence. In this case, the owner may lose the tracks of assets due to no more position updates from out-of-energy devices. There are many efforts, e.g. [6], to counter the EDAs; however, so far, there are few indications that the problem has been entirely solved.

In summary, this article makes the following contributions:

- The first attempt is to cover a systematic approach to address the EDAs in LPW networks, including an overview of current LPW standards, the principle of EDAs and why EDAs are severe problems in such networks. This attempt is driven by the security characteristics of a myriad of LPW communication technologies, which will shape the connectivity of a massive number of IoT devices.
- We provide an extensive overview of prominent EDAs, using the taxonomy as a guideline, and then reinforce the evidence with proof-of-concept literature. We also offer a fine-grained classification by how detection and prevention are performed, which may significantly help the readers to understand the countermeasures against the important classes of EDAs in depth.
- We discuss expectations of the future defense system against EDAs and remarkable open challenges for extensive research.

The remainder of this paper is organized as follows. Section II and Section III cover the related work, the scope of the review, and the main concepts of the LPW networks as well. Section IV, Section V and Section VI then discuss a systematic approach to address EDAs in emerging LPW technologies and the corresponding defense mechanisms. Our vision about a future EDA defense system is presented in Section VII along with the open research directions. To conclude, we discuss the goal of the review in Section VIII.

II. RELATED WORK

EDAs in the context of conventional networks such as WSN appear to be hot topics for a long time. Many studies have covered variants of EDAs in a WSN such as [3], [4], [6]–[15]. For example, Raymond et al. [3] evaluated the denial-of-sleep attacks, a variant of EDA, which targets the MAC layer of WSN sensors. Vasserman et al. [4] primarily focused on Vampire attacks, which try to drain the energy of WSN sensors through several exploitations of WSN multi-hop routing vulnerabilities. Also, the studies [6], [9], [10] addressed EDAs and their defenses in WSNs; however, the information there is outdated, given the latest updates of WSN technologies and security issues.

On the other hand, the authors of [16] focused primarily on mobile devices and exploited many vulnerabilities (e.g., by running malicious multimedia content), including the ones only for operating system-integrated devices. The authors of [17] presented an approach to exploit the vulnerability of IEEE 802.11 Wi-Fi and IEEE 802.15.1 Bluetooth to launch Denial-of-Service (DoS) attacks and accelerate battery depletion of mobile devices. There are also several studies about depletion-of-battery attacks, but the major approaches focused on modeling a specific case of EDAs, e.g., [8].

Meanwhile, several efforts have been made to cover defense methods against EDAs such as encryption-based and intrusion detection-based [18]–[24] approaches, although these methods focus mostly on specific cases of EDAs in short-range wireless sensor networks, e.g., Zigbee. For example, Wood et al. [20] showed frame masking, channel hopping, packet fragmentation, and redundant encoding. Such methods together significantly reduce the probability of a successful jamming attack, a variant of EDAs. Dong et al. [22] covered signature-based broadcast authentication to provide DoS resistance and thus save battery-powered devices. Also with the effort in protecting sensors against DoS-based depletion attacks, the authors of [23] primarily propose an intrusion detection approach based on energy prediction.

However, all the mentioned works have covered the EDAs in traditional networks such as wireless personal (short-range) sensor networks. To the best of our knowledge, so far, there is no work to cover the EDAs in LPW networks, which not only inherit the characteristics of conventional WSNs but also enhance the features to satisfy the tremendous requirements of new applications in the IoT era. Also, the novel (long-range) LPW technologies such as LoRa and NB-IoT have appeared in recent years, but have not been covered yet in prior studies. Therefore, we believe that our work is the enhanced version to cover not only the state-of-the-art EDAs in short-range LPW networks but also the attacks and defenses available or newly specified in the booming network models, e.g., long-range LPW networks. In the future, IoT devices of various technologies, e.g., the ones from both LPW and non-LPW networks, will be probably connected. Therefore, this extensive review also provides the first overview of EDAs and potential security issues that may occur in such interconnected networks.

III. RESEARCH SCOPE AND NETWORK MODEL

In this section, we present the research scope, the LPW network model, and security concerns in LPW networks.

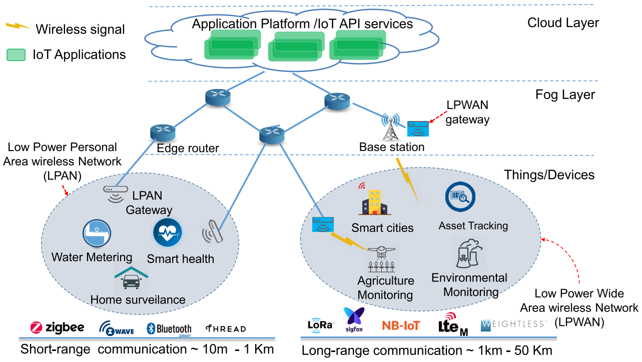

FIGURE 2. **Classification of LPW networks by the coverage and relevant business sectors. LPAN means the short-range communication that is often limited to a few hundred meters at best. LPWAN offers the connectivity to the low-power devices distributed up to a few dozen kilometers.**

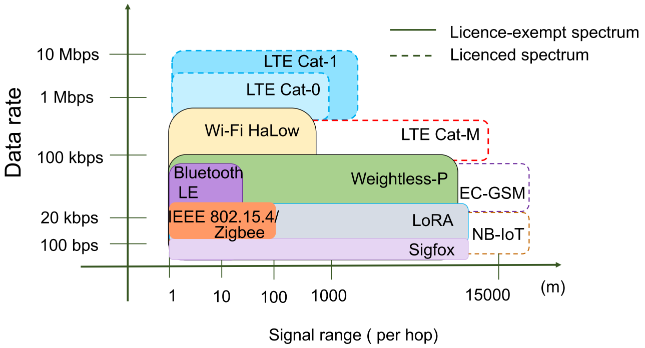

FIGURE 3. **Classification of LPW networks by data rate and signal range [26]. Both the technologies of LPAN and LPWAN offer a diversity of data rates. LPWAN attracts the competitors not only based on the licensed-spectrum but also the licence-exempt frequency.**

A. RESEARCH SCOPE

EDAs are designed to crack down the availability of battery-powered devices primarily through depleting their energy. Due to the lack of abundant energy source attached, by aggressively draining the battery of these connected sensors, EDAs can be a reasonable approach to degrade the function and further disable a battery-powered device (out of energy). The devices in non-LPW networks (e.g., 4G LTE-compatible smartphones) are vulnerable to the EDAs [16]; however, unlike LPW devices, smartphones are constantly improved in features and equipped with powerful security methods [16], [17] and their battery can be easily recharged as well. Therefore, in this work, we lean towards addressing the EDAs in the former case, i.e., LPW networks.

B. LPW NETWORK MODEL

An LPW network, as the term suggests, involves a set of wireless communication technologies that interconnects low-cost and low-power sensors/devices. Intuitively, following the definition, LPW networks have covered a wide range of technologies, including the long-standing ones, i.e., WSN, for a dozen years. With the emergence of IoT, LPW networks jump into the race and have been the leading player [25] to provide the connectivity for billions of future IoT devices. In order to clarify the difference and evolution of such technologies, we categorize them, by the radio signal coverage, into two classes: Low power Personal Area wireless Networking (LPAN) and Low Power Wide Area wireless Networking (LPWAN, or another name LPWA), as shown in Fig. 2. The illustration shows a relative difference in the target of two classes: the LPAN offers the connectivity for the applications communicating in a near distance such as smart home, whereas the LPWAN targets the technologies supported in a vast territory, e.g., asset management. The coverage is the clear advantage of the LPWAN technologies compared with the LPAN, although their data rates are sometimes close, as shown in Fig. 3. Moreover, while most LPWAN technologies rely on the licence-exempt spectrum, several vendors, particularly telecommunication providers, have promoted the ones based on the licensed frequency. The latter has significant advantages over the existing network infrastructure, e.g., NB-IoT and LTE-M. However, using which technology depends on the success of each business model the vendors have been promoting and the acceptance of the clients who often require the candidates to satisfy their specific requirements.

The LPAN includes short-range wireless communication technologies, e.g., ZigBee, IEEE 802.11ah (Wi-Fi HaLow), and Bluetooth Low Energy (BLE), in which the coverage is often limited to a few hundred meters at best. For decades, LPAN has been designed for sensors with limited processing capabilities to monitor physical or environmental conditions such as temperature and humidity. The features and connectivity have been gradually extended and now LPAN has been used in a wide range of practical applications of both civil and industrial field such as smart home, telemedicine, and metering systems. The topology of an LPAN network can vary from a star model to a multi-hop mesh. Due to the popularity of the multi-hop model in dispersed and unattended sensors, using a routing protocol is common in LPAN. Also, a typical LPAN network consists of one or many sensors connected to a particular gateway, which supports the connection to the Internet. That gateway must be able to listen to the LPAN channel and decode the sensing data while each sensor can connect to the gateway directly or through its neighbors. An application is also required to process and present the sensing data. The application locates at the gateway or a remote host on the Internet.

Unlike LPAN, LPWAN has shaped a new trend in the IoT communications market by offering affordable connectivity to the low-power devices distributed over a large geographical area, i.e., up to a few dozen kilometers, whereas keeping a battery life up to ten years. LPWAN technologies emerged in late 2012 as long-awaited trends that are well suited to the specific needs of machine-to-machine (M2M) and IoT devices. Nowadays, they are diverse with a crowd of players sharing the market such as LoRa, NB-IoT, Sigfox and LTM Cat-M [25], [26]. Meanwhile, rising ones such as Weightless-P also start debuting. These technologies are mostly at the early stage of commercial deployment, but appear to be promising. They have significant advantages of a nationwide rollout, i.e., boosted by the signal coverage and longevity. However, each vendor is wrestling to promote their solutions and convince the clients that their technologies, particularly the ones under proprietary class and licence-exempt spectrum, are entirely reliable and reasonable with the deployment cost. As a result, LPWAN technologies also have different approaches to building the network model and protocol stack (proposed by the vendors). In a typical model, an LPWAN network consists of an LPWAN sensor, a gateway and a remote application server on the Internet.

In a nutshell, the market of LPAN and LPWAN technologies is expected to be huge in the IoT era, since both of them are designed to satisfy the specific communication requirements of a wide variety of IoT use cases such as smart metering.

C. OVERVIEW OF LPW PROTOCOL STACK

The characteristics of a protocol stack significantly unveil the supporting features and connectivity ability of a communication model. Due to the low cost, LPW devices cannot accommodate communication protocols which often consume much energy such as advanced packet loss/congestion management [27]. Another critical factor is that the data per request in LPW networks are typically quite small, just 10-12 bytes long in the application payloads and rarely exceeding 200 bytes. Thus, there is no doubt that using a bulky protocol stack such for wired networks is too wasteful in this case, i.e., to carry small packets. Also, the duty-cycle for transmitting data in LPW is often only a few times per minute, even per day or per week. Thus, it is reasonable that the protocol stacks of the LPW technologies must be restructured and simplified. Fig. 4 illustrates such changes. Most protocols of the LPW protocol stacks are different from those of the Internet domain. For example, the energy-hungry protocols (e.g., IEEE 802.11) are replaced by the lightweight and energy-efficient ones (e.g., IEEE 802.15.4), or even the routing in the LPWAN domain is gone.

Intuitively, the protocol stacks vary for LPAN and LPWAN. The first difference is the PHY/MAC layers. LPWAN often offers proprietary RF modulation and custom MAC protocol. The single-hop communication model, i.e., the LPW sensors will transmit directly to an LPWAN gateway, is also popular in LPWAN, whereas LPAN devices may support either single-hop or multi-hop communications. With the support of the multi-hop communication model, LPAN requires a routing protocol such as 6LoWPAN in the network layer to handle the packet forwarding. Typically, an LPWAN/LPAN application can be located merely right at the local gateways or further, a remote cloud server. In the latter case, the connection between the gateways and the application server is over the IP-based protocols.

The difference in the protocols and network model of each LPW plays a significant role to address EDAs and learn the key points in attack techniques. We cover these characteristics in the next sections.

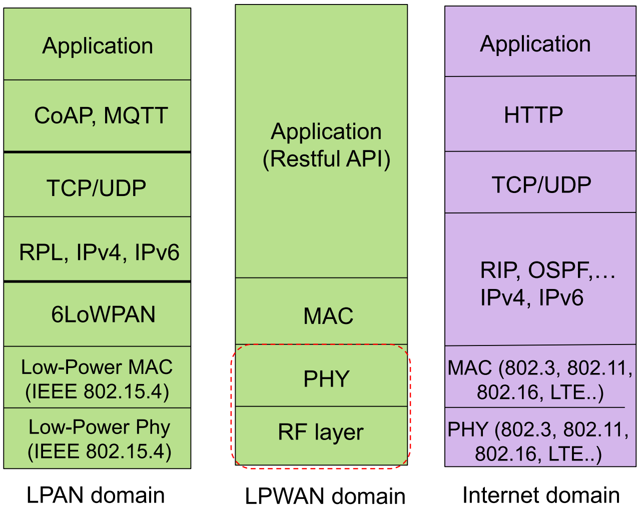
Application
CoAP, MQTT
TCP/UDP
RPL, IPv4, IPv6
6LoWPAN
Low-Power MAC (IEEE 802.15.4)
Low-Power Phy (IEEE 802.15.4)
LPAN domain
Application (Restful API)
MAC
PHY
RF layer
LPWAN domain
Application
HTTP
TCP/UDP
RIP, OSPF,… IPv4, IPv6
MAC (802.3, 802.11, 802.16, LTE..)
PHY (802.3, 802.11, 802.16, LTE..)
Internet domain

FIGURE 4. Classification of LPW protocol stacks in relation to the IP-based protocol stack. Most protocols of both LPAN and LPWAN domain are changed to satisfy the energy consumption requirement and the simplicity of LPW devices.

D. IOT NETWORK MODEL

Until 2012, LPAN was the solo player in the IoT market. However, taking only a few years in the evolution, LPWAN has found its sustainable position for IoT applications, especially in the smart city and industrial sectors that do not require comparable speed and bandwidth of consumer cellular devices but still prefer long-range transmission. LPAN along with LPWAN can meet the requirements of IoT applications in terms of cost, battery life, coverage, and network capacity, but both have been designed for different targets, at least in terms of signal coverage. In the future, more players in LPAN and LPWAN may appear, but for sure, no single technology of them can cover every IoT application, although there is probably a competition among them in IoT applications, e.g., smart metering.

A typical IoT network model can help to structure the layers and the protocol that the attacker often targets. Fig. 2 illustrates such a model. The model is made up of three layers [28], [29]. Most communications of LPW sensors are in the first layer, so-called Things/Devices. The second (edge) and third (cloud) layers are the network and application layers. We also use this model in reviewing the EDAs and relevant countermeasures. The detail can be found in Section IV-D.

E. WHY EDAS ARE POSSIBLE IN LPW NETWORKS

The security concerns that lead to EDAs in the LPW devices and relevant communication technologies can be summarized as follows:

1) In the profit-driven business, security is often an afterthought of most manufacturers, i.e., not given

TABLE 1. Security modes in IEEE 802.15.4 [8].

Cryptography schemes	Description	Confid-entiality	Inte-grity
None	No security	-	-
AES-CBC-MAC-32	32-bit MAC	-	✓
AES-CBC-MAC-64	64-bit MAC	-	✓
AES-CBC-MAC-128	128-bit MAC	-	✓
AES-CTR	Encryption only	✓	-
AES-CCM-32	Encryption & 32-bit MAC	✓	✓
AES-CCM-64	Encryption & 64-bit MAC	✓	✓
AES-CCM-128	Encryption & 128-bit MAC	✓	✓

priority over functionality [2]. Notably, data of some devices conveyed over the air interface are not encrypted [25], [30]–[32] or secured with weak cryptography schemes. For example, Table 1 illustrates the security schemes defined in the IEEE 802.15.4 Standard for the LPW networks, where the bottom cryptography schemes mean more secure. Unfortunately, implementations of any security practice are heavy in terms of resource usage, and an LPW device may be so constrained to gain all security recommendations. To keep the cost of the device to a minimum [28], the manufacturers may not prefer the most reliable security scheme. That means the sensors and their network are potentially vulnerable to security attacks.

2) Due to the priority in producing low-cost devices, most manufacturers may cut off the security maintenance (such as never issue a security patch for the devices in their lifetime). Unfortunately, this bad behavior is not uncommon [2], [29]. Lacking regular protection measures makes the sensors weakened to resist EDAs, even those derived from well-known vulnerabilities.
3) The attached energy source of LPW devices is limited and sometimes not easy to replace (e.g., mounted in the body of objects or scattered across a wide range of inaccessible terrain). Any damage to the battery may require a long time and high cost to maintain.
4) The nature of open medium access (wireless) makes the LPW networks susceptible to security attacks, e.g., jamming or gathering information via sniffing by unauthorized devices in range.

In conclusion, lacking reliable security mechanisms in LPW communication protocols and maintenance ability is the top concern of why an LPW network is extremely vulnerable to security attacks, including EDAs.

IV. PRINCIPLE OF EDAS

Before covering the state-of-the-art EDAs and defenses, we first clarify the EDAs in terms of the concept, their consequences, and measurement. The classification in this part is essential for the systematic reviews in the next sections.

A. THE EDA DEFINITION

Although there are many types of research about EDAs such as [3], [5], [8], [10], [11], at this moment, there has been no consensus on the concept of an EDA. To best fit the research scope in this paper, we define that an EDA is a kind of security attack in which the energy of a device is depleted in processing unexpected/illegal operations. The purpose of attackers is to force sensors to waste computing time on energy-consuming tasks, e.g., processing garbage data, and thus vastly deplete the power of victim nodes without the device owner's expectation/permission. Meanwhile, a conventional low-power sensor means that it can wake up at least a few times each day to transmit data, but its battery life is still up to years without recharging.

TABLE 2. Average energy consumption of Zigbee-based node per request [8].

Working mode	Average consumption (mA)
Idle	11
Pure data processing	18
Receiving and processing unsecured packets	32
Receiving and processing secured packets	40

B. POTENTIAL CONSEQUENCES OF AN EDA

EDAs may severely affect several fields in the civil and public services. First, EDAs potentially cause severe damage to critical services such as healthcare, e.g., by interrupting the monitoring status of patients [33]. Second, for the management services and business sectors of smart cities such as traffic flow and predictive maintenance services, a large number of disabled sensors by EDAs can dramatically degrade the quality of service (QoS) or cause chaos in sensing data. Particularly, in smart monitoring services such as transportation tracking and pollution monitoring, EDAs can incur high maintenance cost due to the replacement of out-of-battery devices and therefore cast doubt on the efficiency of IoT deployment or further, the manufacturer's reputation. For industry, the risk of EDAs will cost the manufacturers more resources (e.g., for hiring labor) in releasing the patches, especially, if their vulnerable products have been widely deployed. Note that the critical infrastructure can also be affected if the LPW disabled devices act as sensors for collecting information.

For personal use of IoT, EDAs can be a practical approach that helps the attacker deliberately sabotage a specific target such as the monitoring system in a smart home.

C. THE MOST ENERGY CONSUMING TASKS

Knowing which tasks heavily consume the device batteries can help to reveal the potential target of each attack type. As illustrated in Table 2, the communication and processing of secured packets are the champions in such tasks. The energy estimation is based on the work of a Zigbee node [8] that has an ATmega128L processor operating with 8MHz frequency, 128kB in-system programmable flash, and a CC2420 RF transceiver compliant with the 2.4GHz IEEE 802.15.4 standard. The values can vary with different LPW technologies, but the trend for each mode should remain [34].

Besides the highly effective methods of using bogus secured packets, deliberately transmitting superfluous

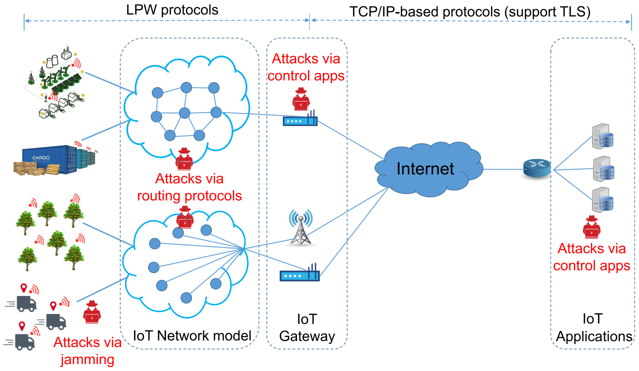

FIGURE 5. A typical architecture of LPW networks and related EDAs (in red text). Internet connectivity and the interconnection of LPW devices extend the attack surface.

meaningless packets (pure data processing in the second row) can degrade the sensor batteries gradually. In this way, adjusting the duty-cycle and data size in each transmission can significantly affect the battery life. However, each exploitation techniques are heavily tailored to the available vulnerabilities of each protocol. In comparison with the similarities in the target of the attacks, we can know why the attackers are consistently interested in attacking against the protocols in a specific layer.

D. EDA CLASSIFICATION METHOD

EDAs target the availability of LPW devices and can disable such devices by draining their battery. However, EDAs vary in protocol layers. In this study, we categorize an EDA by its target in the four layers: the physical layer, the MAC layer, the network layer, and the application layer. The location of the attacks is illustrated in Fig. 5, in which Internet connectivity and the interconnection of LPW devices can extend the attack surface. This model is compatible with the three-layer IoT model in Fig. 2. The detail of each attack in these layers is fully addressed in Section V.

Besides the above classification from the attack position and attacker's ability, internal or external attacks can be also a factor to assess the threat level, e.g., easy or hard to launch the attack. An external (or outsider) attack such as jamming refers to an attack type against LPW devices without any special privilege (possessing no secret key) to access the network/device. In contrast, an internal (also namely insider) attack implies that a device is compromised and allowed to freely access the network or communicate with other devices with genuine keys. Note that external attacks such as physical attacks [8], [35] can be used to gain necessary access for internal attacks.

The way to launch an EDA can also be either passive or active. The goal of passive attacks is to obtain transmitted information by eavesdropping or monitoring of transmission. Active attacks are the attempts to break into the security protection to illegally access the components of the LPW networks (e.g., devices, control applications). We believe that the EDAs are mostly tailored to the latter case.

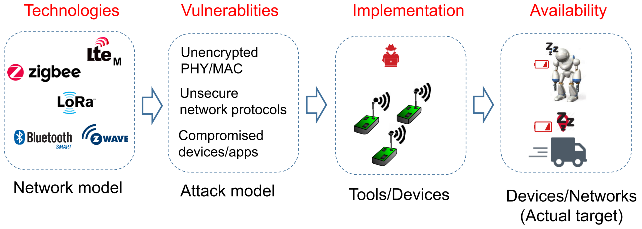

FIGURE 6. A typical approach of EDAs in LPW networks. From left to right, the attack stages may vary with different networks but often start with a task of gathering information about the network model and vulnerabilities.

E. ATTACK STAGES

Like generic IoT security attacks, an EDA probably requires several pre-conditions to be launched successfully. The more information about the target is collected, the more options of the attack methods can be selected. Typically, starting with a target technology, e.g., Bluetooth LE, the attacker can gather as much information about the network model as possible (e.g., multi-hop), find a list of available vulnerabilities and then implement a tool to launch. Fig. 6 illustrates such steps, although amateur attackers such as script kiddies may prefer the tools directly to attack the network.

Intuitively, the useful information can be collected via penetration [36], public documents such as technical papers (e.g. [37]) or open specification [38]–[40]. This step is called the pre-attack phase. The target of this pre-attack phase is to obtain critical information such as radio frequency, network model, the device type and the firmware version. Based on found vulnerabilities, the attacker can develop an exploit or use a suitable scenario in available tools such as [41], [42] to attack. Note that the vulnerabilities may not sometime appear in the latest/enhanced version of the technology, but they will if the attacker can downgrade the security mode of a protocol to its older version that has the flaws. Typical examples of this tactic are the attacks that target Bluetooth LE and Z-Wave [35], [43].

The cost to launch an EDA varies with the required equipment and the complexity of exploiting the vulnerabilities. With several hundreds of dollars, finding a killer tool in the online market to launch EDAs is not uncommon, e.g., the tool to support an attack against Zigbee-based devices [41], [42], LoRa jamming, or even the libraries to build a powerful exploitation and attack tool [36], [43], [44]. To launch an effective EDA, the attacker may adjust these tools according to specific cases.

F. EDA DAMAGE MEASUREMENT

Quantifying the damage can confirm the claim whether EDAs cause serious matters. For this purpose, we prefer the measurement of potential damage by reviewing the energy reduction rate of the individual sensors or the whole network in two scenarios: the EDAs absent and present. The energy reduction can be evaluated by the shortage of battery lifetime (e.g., years to days) or the higher energy usage level (e.g., joule or mA) in the presence of the attack than the relative energy usage of the same device following the setup environment recommendations from the manufacturers. The former metric is suitable to measure whether the testing can be launched on real devices, whereas the latter is preferable for the evaluation in a simulated environment. To clarify the comparison of the EDAs, we follow [8] in reviewing the average energy consumed per message and the number of messages that the attacker should send to deplete the energy of the victim node successfully. Moreover, we also consider the cost to pay for launching an EDA if any, i.e., how difficult to initialize an attack. The assessment for each EDA will be detailed in the summary of Section V.

V. STATE-OF-THE-ART ENERGY DEPLETION ATTACKS

Following the attack classification in Section IV-D, in this section, we discuss existing EDAs in four layers: physical (PHY), datalink (MAC), network, and application. Note that a smart attacker can combine the attacks to maximize the damage to the victim.

A. EDA IN THE PHYSICAL LAYER

Jamming is a severe threat for either LPAN or LPWAN in this layer. An adversary can easily launch this attack by sending abundant signals to deny legitimate LPW device access to the channel resource. Meanwhile, jamming can rapidly drain sensor batteries [20]. For example, LPW devices must wait longer to finish transmitting data due to the effect of jamming. However, jamming can be ineffective for the ultra-narrow band and unidirectional technology, e.g., Sigfox, in which the wake-up or transmission period in these LPW devices is predefined and cannot be changed without re-activation [25].

The most straightforward jamming approach in LPW networks is by using a constant jammer, which continually emits radio signals, and a waveform generator with this ability [45] can help. In a wireless network, if no channel is idle, legitimate traffic cannot be sent and a device must awake and ''wait longer'' for potential re-transmission; thus, valuable energy is wasted for this unexpected non-sleeping. There are also variants of advanced jamming. For example, a deceptive jammer injects regular packets into the channel without any gaps between subsequent packet transmissions, and thus a normal communicator will be deceived into the receive state. Also, a random jammer is another advanced PHY-layer EDA, in which the jammer turns off its radio and enters a ''sleeping'' mode after jamming in random periods to complicate the detection efforts of an anti-jammer. Another serious attack is a reactive jammer, which often stays quiet when the channel is idle, but immediately transmits signal if it finds an activity on the channel. The detail of jamming attacks in sensor networks can be found in [45].

Also, an attacker of a PHY-layer EDA can deplete the energy of an LPW sensor by launching much communication in the hidden channel or occupying the whole available channels of the devices. Moreover, the attacker can use electromagnetic emissions to create noise that will cause high error rates, and hence force the sensors to take a corrective action such as packet retransmissions that increases energy consumption [46]. Covert timing channel attacks or stealthy communication [47] in part can be seen as an indirect agent to cause degradation to the device energy. In this case, such attacks force a device to waste its energy for covertly transferring trash data in the gaps between transmitted packets. This transfer is not supposed to be allowed in a normal case. However, this kind of attack may target a small group of high-end LPW devices, e.g., those supporting an operating system.

B. EDA IN THE MAC LAYER

Most existing EDAs are launched in the MAC layer. A common attack strategy is that the attacker deliberately broadcasts forged packets, e.g., including encrypted junk data, to force the receivers to perform unnecessary processing such as signature verification [22] and a large number of authentications. For example, the frame counter within the nonce field in the IEEE 802.15.4 MAC frames [48] is used to prevent replay attacks [8]. However, the entire nonce field in the sending frame is unencrypted [8], [37], [49]. Leveraging this flaw, an adversary can construct bogus messages by increasing this frame counter in every frame [8]. According to the standard, the receiver will extract the frame counter value from an incoming packet and compare it with the largest value stored in its memory. If the extracted value is larger than the stored one, the message is accepted for further processing and the stored one will be updated with a new value (e.g., plus 1); otherwise, the message is rejected. Nevertheless, the bogus messages will not pass the integrity check (i.e., message integrity code verification) for sure, but the recipient node has wasted a valuable amount of energy accepting and processing those forged messages. This kind of attack is also called garbage data verification. Note that an adversary can launch the attack without knowing the network keys [8], [37]. That is why this approach is one of the most effective EDAs. To avoid the suspicion of the detection engine if any, the attacker can choose to gradually drain the battery of the recipient, instead of doing in a short time.

1) PROOF-OF-CONCEPT ATTACKS

Several studies have demonstrated a successful EDA of garbage data verification. For example, the authors of [8] present a ghost attack in ZigBee networks, which can reduce the lifetime of Zigbee nodes from years to days (as shown in Fig. 7). The results illustrate the average energy reduction rate for various security suites (as listed in Table 1). Specifically, the descending level varies with the cryptography algorithms, in which, the energy degradation will be increased if the payload data are encrypted with more XOR operations (e.g., AES-CCM). In other studies [50], [51], this higher consumption is proven because more data bytes are involved in the processing or because of misbehaving MAC activities. Another case targeting Implantable Medical Devices (IMD) is presented in [33], in which the lifetime of an IMD could be reduced from several years to a few weeks. An example

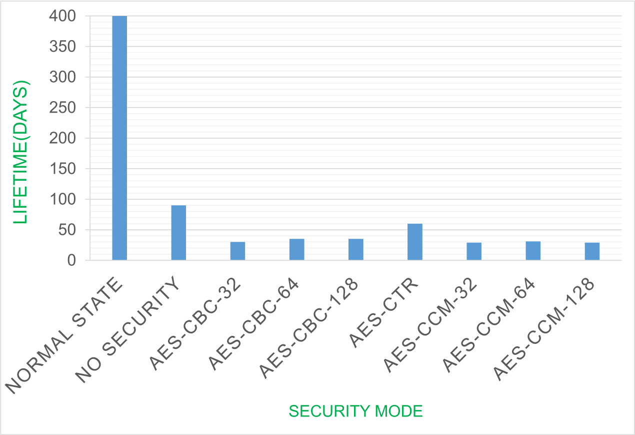

FIGURE 7. Amount of time (in days) needed to deplete the energy, where the attacking rate is 10 packets/s [8].

of unauthenticated traffic flooding attack targeting heavy computation at the victim can be found in [52].

Another effective EDA in the MAC layer is duty-cycling manipulation. As shown in Table 2, the sources of most energy loss in LPW networks are communication-related tasks such as sending, receiving data and listening to the channel. According to the work [34], adjusting several parameters such as longer time-on-air, higher data rate, and larger packet size has a significant adverse effect to the energy consumption of wireless devices, including those of LPW networks. With a wide range of subtle exploitation techniques [24], [53] in the MAC layer, an adversary can intentionally broadcast control requests, e.g., synchronization or beacon messages [11] to the victim nodes to make them forgo their sleep cycles, so that they are completely exhausted and hence stop working. Notably, a smart attacker can manipulate their MAC protocol parameters, e.g., contention window size [8], and send packets to create more collisions to ongoing transmission [52], which can cause the victim nodes to overhear. On the other hand, the attacker can try to attain enormous disruption by dropping small, payloadless frame headers to its victim radio receiver, depriving the latter of bandwidth and sleep time. This attack is a variant of denial-of-sleep attacks or sleep deprivation. The details of such attacks and their impacts on the MAC protocols (SMAC, T-MAC, B-MAC, and G-MAC) are described in [11], [53].

2) PROOF-OF-CONCEPT ATTACKS

Several tests by the authors [15], [53] show that the most efficient duty-cycling manipulation attack can keep a cluster of nodes awake up to 100% of the time. In a typical example [53], each time of waking up can cost the device up to 0.16% duty cycle and a lifetime of 1287 days. In a similar case, the researchers have successfully drained the battery of Bluetooth LE-based sensors (with a lifetime of days) up to 93% [15] in approximately 6 hours.

Although most of the attacks mentioned above target LPAN, several ones are also suitable for the LPWAN in terms of general ideas, i.e., manipulating duty-cycle. However, the MAC protocol stack of LPWAN relies heavily on the proprietary technology of different vendors; thus, the exploitation is tailored to specific technologies. For example, LoRa uses lightweight crypto algorithms in communication protocols and even have no clear protection mechanism addressed in their specification [38]. A fake gateway (controlled by the attacker) can request the change to the reporting cycle of the sensors (e.g., specified by the beacons broadcast), even to adjust their sleep period. Consequently, the device must wake up frequently, thereby increasing the power consumption of the sensor. Note that the support of bi-directional communication model, such as LoRa Class B devices [54], NB-IoT [26], and the inconsistency of default security setting in each technology [55], [56] can unveil potential vulnerabilities for EDAs, including the indirect attack approaches such as denial of services [57]. The faster bi-directional communication and more features in the MAC layer the devices support, the higher the probability to be the targets of EDAs is.

C. EDA IN THE NETWORK LAYER

For mesh-based networks such as LPAN, the routing mechanisms raise major security concerns. For example, in the source routing protocols such as Dynamic Source Routing (DSR), the source node specifies the route to the destination; thus, intermediaries forward packets based on a route specified by the source rather than their forwarding decisions. Exploiting this limitation, an attacker sends a packet with a route in a loop [4], [19], and forces that packet to traverse the same set of nodes repeatedly. As a result, packet processing is forced to trigger in the nodes that would not normally receive at all, leading to network-wide energy expenditure.

The stretch forwarding attack, also so-called carousel attack, is another EDA targeting source routing but does not create loops. In this attack, an adversary constructs artificially long source routes [4], [19], potentially traversing longer network path by some nodes than the shortest path to the packet destination. The impact of this attack can be amplified, up to an order of magnitude, by increasing the number of adversarial nodes in the network or merely sending more packets. Another special attack of this kind is selective forwarding [58], in which a misbehaving forwarding node just forwards a subset of the packets it receives but drops the others. That may cause the source, which has not yet transmitted data successfully, to waste energy on waking for retransmitting the data.

For stateful routing protocols such as Optimized Link State Routing Protocol (OLSR) and Ad hoc On-Demand Distance Vector (AODV), collusion attacks in routing are also big threats. Usually, stateful routing protocols are built dynamically from independent forwarding decisions; thus, the effect of loop routing or stretch forwarding attack is dramatically reduced. However, an intelligent attacker can design cooperating malicious nodes (also so-called collusion) along the packet paths to manipulate forwarding actions, for example, by just depositing a packet in arbitrary parts of the network or non-optimal next hops, whereas still forwarding the packet to nodes as in the original route. The nodes on the extra route must spend the energy processing the data while they do not need. A variant of this attack is spurious route discovery [4]. In most protocols, every node will forward route discovery packets (and sometimes route responses as well), and that means we can initiate a flood by sending a single route request(RREQ)/route reply(RREP). Systems that perform as-needed route discovery, such as AODV and DSR, are particularly vulnerable to the attack since any node can send an initial discovery at any time, not just during a topology change. A malicious node has some ways to induce a perceived topology change: it may merely claim that a link is down, or declare a new link to a non-existent node. The collusion of several compromised nodes (targeting the false claims) can make the surrounding nodes to trust that the route has been changed. As a result, these nodes consume their valuable energy to process the state change or restore it (e.g., after a failure to send a packet along that route) while it does not at all.

RPL (IPv6 Routing Protocol for Low and Lossy networks) or 6LowPAN are also vulnerable to EDAs. 6LowPAN is a proactive protocol, a rival of Zigbee, optimized for multi-hop and many-to-one communication, and also supports secure communication protocols such as IPSec [30], [59]. However, the high-end requirement of computation and energy to satisfy the end-to-end security protocol like IPSec may be only feasible for the network-to-network model (gateway to gateway or gateway to the Internet) instead of the host-to-host model of low-cost devices in LPW. That means the routing implementation based on the route-under mechanism for low-power devices such as [30], [60] are probably vulnerable to routing-based EDAs, e.g., stretch forwarding.

1) PROOF-OF-CONCEPT LITERATURE

Vampire attacks [4] are typical examples of routing-based EDAs in mesh-based networks, e.g., loop routing and stretch forwarding attack. Geographic and beacon routing protocols, as well as a logical ID-based sensor network routing protocol all, are also vulnerable to Vampire attacks. According to the evaluation [4], several individual nodes in the path lose almost up to 10 percent of their total energy for each sent message from the attacker that significantly leads to the network-wide energy degradation. Notable, Bluetooth LE and Z-Wave [61] are vulnerable to this attack type.

Recently, there are also several interesting studies on the multi-hop routing in LPWAN networks such as LoRa [62], [63], but we argue that the one-hop network model of long-range communication technologies may gain more advantages, e.g., keeping the simplicity in the design (according to the original specifications), than the multi-hop model. Therefore, we do not consider the routing-based EDAs against LPWAN networks in detail.

D. EDA IN THE APPLICATION LAYER

In this layer, there are various approaches to EDAs in LPAN and LPWAN. Many LPWAN devices may not have an advanced operating system (OS) but purely send the sensing data to the application server, which could be placed at the gateway, a server farm or the cloud. The final case is popular due to the convenience for remote access. Like most applications in IoT devices [64], [65], this application shares severe security problems. For example, by exploiting the application-level bugs such as buffer overflow, security vulnerabilities of the Web APIs of the control application and IoT application frameworks (e.g., The Things Network [66]), it is possible that an attacker can obtain the full access privilege to the system function, and then compromise the application. In practice, it is common that there is no command to turn off the sensors of a network directly, but the control application can request the sensors to report more frequently than the original setting (duty-cycle manipulation). When the sensors actively work more than the standard setting, the network energy expenditure can be significantly degraded in a short time. For LPAN, the attacker can inject the malicious code or activate a program and run it in the background [18] if the OS (e.g., Contiki and WearOS) is available in such devices.

E. SABOTAGE EXPANSION

From the attacker's perspective, maximizing the damage through EDAs, i.e., shortening the life of the sensors in an LPW network, is the nature of mind. We believe, in the real world, this tactic is entirely possible by combining multiple EDAs. For example, the attack can broadcast unauthenticated traffic to the victims while keeping them waking up as long as possible (i.e., the combination of EDA garbage data verification and EDA duty cycling manipulation), and even applies several amplification methods [67]. In mesh-based networks, the attacker can also amplify the magnitude of the EDAs by several options such as increasing the source path as long as possible and using more collusion nodes. However, due to the intrinsic characteristic of the routing protocols, the intermediate forwarding nodes do not often involve in processing the data (i.e., packet payload). As a result, the individual nodes may have a different energy degradation rate from each other due to its availability in receiving the packet from the attacker (e.g., sleeping during the attack time).

F. SUMMARY

EDAs in LPAN and LPWAN have several slight differences in the method. In LPAN, the attacker can exploit the flaws of the one-hop or multihop transmission model. By contrast, the bidirectional end devices in LPWAN connect to the gateway directly, and thus exploiting the flaw of the former model is common. Note that several already-in-the-market LPWAN devices support only uplink transmission. For such devices, the attacker may face a stonewall to launch most EDAs, except the jamming. Another potential intervention may happen only in the bootstrapping period of the devices (activation).

TABLE 3. Summary of state-of-the-art EDAs in prominent LPW technologies.

Attack to layer	Paper	LPAN				LPWAN			Attack type		Attacker Presence	Threat Assessment	Implement-ation	Limitation
		BLE	Zigbee	WiFi Halow	Z-Wave	LoRa	NB-IoT	LTE-M	Internal	External				
Physical layer														
Jamming	[20], [45]	✓	✓	✓	✓	✓	✓	✓		✓	✓	High	R	- Require a jamming device
Communication in hidden channels	[46], [47]	✓	✓			✓			✓			Medium	S	- Infeasible if no hidden channel
MAC layer														
Garbage data verification	[8], [17], [50], [51]	✓	✓	✓	✓					✓		High	S	- Attack only on unencrypted MAC header
Duty-cycle manipulation (sleep of depletion)	[33], [31], [52], [53]	✓	✓		✓	✓	✓		✓	✓		High	S	- Duty-cycle of the victim is modifiable
Network Layer														
Loop forwarding	[4], [19]	✓	✓		△				✓		✓	Medium	S	- Attack only in the multi-hop communication
Stretch forwarding	[4], [19], [58]	✓	✓		△							Medium	S	- Attack only in the multi-hop communication
Application Layer														
Duty-cycle manipulation	[7], [8], [18]	✓	✓		✓	△	△	△	✓	✓		Medium	S	- The control app is compromised
Malformed App	[6], [32]	✓	✓				◇	◇	✓	✓		Low	OS	- Attack only on the OS-integrated devices

✓It is possible to launch an EDA: proof-of-concept in practice or research papers.
△ It is only possible to launch an EDA if the end-devices satisfy several pre-conditions such as the support of changing the device duty cycle via the control messages (i.e., bidirectional communication).
◇ Few devices are available on the market and the protocol information is primarily briefed in the specification or research prototypes.
S(Simulator, e.g., NS2, NS3), R (Real sensors), OS (Operating System, e.g., Contiki)

Table 3 summarizes our assessment about typical EDA variants in the range of suffered LPW technologies and research gap. Intuitively, most of the EDAs are found on LPAN and fewer in LPWAN such as NB-IoT. These technologies start debuting and thus a wide real-life usage may not come soon. Therefore, this limits the EDA cases and the evaluations on them.

For the threat assessment, the most threatening attack types are in the physical and the MAC layers. Also, jamming is still the most popular attack method without an effective defense mechanism to defeat (high threat), although the attacker's presence near the victim could risk himself to the detection. In addition, it is quite hard to perform the loop/stretch forwarding in a wide range if there are few compromised nodes (medium threat). Usually, the EDAs using collusion techniques are limited in scope, and therefore the attackers are in favor of targeting specific nodes in critical infrastructure such as metering sensors. Finally, each attack type has its limitation in spreading the damage in a diversity of LPW devices and this leaves a path for enforcing effective defenses. The last remarkable point can be the threat of the central architecture of the LPW remote control applications. The damage could be very high if an attacker can obtain the control privilege of these remote applications and then replace an irregular reporting cycle to IoT devices (i.e., duty-cycle manipulation).

VI. STATE-OF-THE-ART EDA DEFENSE MECHANISMS

This section begins with an overview of the scope of EDA defense, and then state-of-the-art anti-EDA approaches. These methods are predominately proposed in literature or specifically described as security improvements in the protocol specification. We group the defenses into four classes, similar to the classification approach in Section V.

A. SCOPE OF DEFENSES

Protecting the availability of the LPW networks, including the LPW sensors, fundamentally relies on the protection ability of the intrinsic security designs of each technology and extensive security enforcement methods. These architectures can broadly be categorized into proactive and reactive mechanisms. Proactive defenses aim to prevent potential attackers from system access, whereas reactive approaches assume that attack activity can be present within the system, e.g., compromised sensors.

More specifically, proactive defenses refer to the mechanisms that enforce a security policy or communication protocols. This category includes many mechanisms: security scheme (e.g., AES-CCM), authentication, message integrity check (MIC) verification, access control mechanisms and so on. These methods target to make the outside attacker/unauthorized entities (mentioned in Section IV-D) more difficult to access the system if not possess valid credentials and thus mitigate the risk of a potential attack and the number of EDA vectors.

Reactive defenses consist of a diversity of approaches to defeat the attacks that are not prevented by proactive security. This kind of defense has a long history in traditional networks with several key techniques such as intrusion detection/prevention systems (IDSs/IPSs).

However, to match the above attack classification, in this review, we first describe the EDA defenses in the four layers: the physical layer, the MAC layer, the network layer and the application layer. In the summary of the section, we discuss the relation of the proactive and reactive methods.

B. EDA DEFENSES IN THE PHYSICAL LAYER

Detecting physical EDAs on LPW networks, particularly LPAN, has already got significant efforts from the security community over decades. The hardest problem to prevent this kind of attack is the complexity of discriminating between legitimate and adversarial causes of poor connectivity [45]. In particular, it is difficult to differentiate legitimate scenarios for poor connectivity such as congestion and device failures from the network condition under well-designed jamming tactics, e.g., adaptive jamming [68]. The most popular approach to defeat the jamming attacks is to use statistical techniques with the parameters such as signal strength, carrier sensing time and packet delivery ratio. For example, the authors of [45], [68] used two approaches to detect jamming using the signal strength. One compares the average signal magnitude, and the other compares a threshold calculated from the ambient noise levels. Both then classify the shape of a window of signal samples.

Another promising approach is the multimodal tactic [45], which evaluates the combination of several parameters such as packet delivery ratio (PDR) with signal strength readings. In the normal case of no signal interference, a high received signal strength indication (RSSI) means a high PDR. If the signal strength is low compared with noise levels, the PDR will also be low. In contrast, a low PDR does not imply low signal strength, but that the node could be under jamming. The key observation here is to confirm the attack by the low PDR in the case of high signal strength (should be high as that in the normal case).

Besides the above extensive defenses, several evasion strategies to the jamming attacks are proposed to be integrated into the frequency modulation techniques of the technologies such as multiple channel hopping and spatial retreats [45]. The goal of these strategies is to evade the interferer, in either the spectral or physical sense. Multiple channel hopping is motivated by frequency hopping modulation. In this scheme, changing the frequencies in a channel is on demand and operates in the link layer. When a node finds anomaly such as under jamming, it immediately switches channels and sends beacons to announce its presence on the new channel. The nodes that are not jammed but are neighbors of jammed nodes will detect the absence of their neighbors on the original channel and probe the next channel to see if their neighbors are still nearby. If a node detects beacons on the new channel, it will switch back to the original channel and transmit a broadcast message informing the entire network to switch to the new channel. Spatial retreats mean jammed nodes try to evacuate from jammed regions and thus are suitable for LPW mobility networks. How to escape the jammed area and secure a safe-zone for connecting to the network are the key of this method. The details of these techniques are discussed in [45]. Note that the above defense techniques may cost more energy of the devices and that explains why few of them are applied in practice.

An alternative method is to directly compete against the jammer in terms of the adjustable ability of the coding and power of their communications in the physical layer. This requires that, if a node detects it is jammed, it will ignore the fact that it is jammed, and transmit its packet anyway. However, the reliability may not be guaranteed if the attacker is well equipped. We argue that bringing a low-cost and low-power device to beat a powerful and well-equipped device of the attacker is unlikely a wise decision.

In addition, several proposals to implement the encryption mechanisms in the physical layer such as [69], [70] have also gained the attention recently. So far, most of the security methods are provided by upper-layer encryption schemes, e.g., MAC and application layer. The encryption in the physical layer also has significant benefits, e.g., help to mitigate the attacks targeting unencrypted data simultaneously and reduce the computations in the upper layers. The encryption is also hardware efficient for acceleration. It also significantly improves the lifetime of a node in the presence of a ghost attacker by preventing the legitimate node from processing the bogus messages and hence combats against EDAs. In short, this approach appears to be promising, but there is a cost. That is, the protocols in the upper layers (e.g., routing) may need to be adjusted, whereas neither legacy nor low-cost LPW devices are ready for.

So far, we conclude that an effective and holistic anti-jamming method to defeat all mentioned jamming attacks is far away to be reached. There are more efforts towards the goal [20], [45], [68].

C. EDA DEFENSES IN THE MAC LAYER

EDAs in this layer are quite diverse, as mentioned in Section V-B, but there is not a one-for-all solution to defeat all such attacks. However, the defenses can focus primarily on the efforts for: (1) mitigating secure data to be processed unexpectedly or abused (i.e., rejecting unauthenticated garbage data); (2) preventing the potential intervention if any to the normal flow of the sensor duty-cycle.

Enhancing MAC security schemes and authentication mechanisms is the most straightforward defense method. The enhancement can be applying the suitable security schemes (as classified in Table 1) and optimize the underlying cryptography models for the security schemes such as

Elliptic Curve Cryptography (ECC) and lightweight block ciphers [22], [24]. In another example, Hsueh et al. [71] propose the Two-Tier Energy-Efficient Secure Scheme to protect sensor networks against power exhausting attacks, especially the denial-of-sleep attacks. In that scheme, they use the hash-chain to generate the dynamic session key, which can be used for mutual authentication and the symmetric encryption key. As they claim, using the hash model (MD5 or SHA-1) and symmetric in authentication has significant benefits in computation and time, and thus can reduce the authentication process as short as possible. The model can help to mitigate the effect of the power exhausting attacks; however, it also raises the questions how to generate the keys for a large-scale distributed sensors effectively and manage them safely.

On the other hand, securing the frame header and building strong link-layer authentication [8] can help to guarantee both confidentiality and integrity in data exchange, and thus thoroughly prevent the eavesdropping exploitation in the pre-attack phase of the EDA garbage data verification. The most noticeable benefit of mentioned methods is that the devices are remarkably reinforced with reliable security schemes to prevent the external attacks. However, in several cases, it is infeasible to deploy the implementations, particularly, the proposals which require a firmware/hardware update because most LPW devices may not support (due to the cost).

Besides authentication-based schemes to defeat the MAC-layer EDAs, an alternative approach is to use a challenge-response scheme, in which the node [8] – after observing a certain number of bogus messages from a specific address or when the communications are re-initiated – will challenge the attacker with a random number. To correctly respond, the attacker needs to know the secret key, which is available only to the legitimate parties and is securely stored in the node. On the restoration of energy, as part of the challenge-response scheme, the devices need to establish new keys so that they do not reuse the same nonce twice with the same key.

Unlike the prior approach, detection and filtering abnormal (malicious) MAC messages are the most favorable methods. For example, the work in [8] proposes to deploy a trusted monitoring model, which detects the attacker by the measurements of collision probabilities. Similarly, Dong et al. [22] propose to apply pre-authentication signature-based filters to remove bogus MAC messages before the signature verification is performed. Specifically, they develop two more filters, a group-based filter and a keychain-based filter to help sensor nodes avoid performing unnecessary signature verifications. The former filter is used to organize the neighbor nodes of a sensor sender into the groups, which are protected by secure communication and thus isolate compromised nodes that launch EDAs. Unfortunately, the group-based filter cannot prevent the compromised nodes from sending forged messages before they are isolated. Therefore, the latter filter aims to prevent compromised neighbor nodes from affecting benign ones completely.

Also, there are the methods to adapt the similar approach, i.e., detection-based scheme, but require the support of an additional system. Typically, the authors of [33] propose to use the Support Vector Machine (SVM) based scheme to monitor the behavior of sensors, e.g., wakeup and sending data period, and then classify whether those devices are running unexpectedly compared with the patterns in a pre-trained dataset of the normal network state. Their architecture is originally designed for Implantable Medical Devices (IMDs). Like LPW devices, these typical IMDs also have a very limited resource in terms of energy and computation. Predicting the impossibility of using the SVM-based system on these sensors, they propose an additional device, e.g., cellphone to perform the monitoring and classification, and the IMDs are required to connect to the phone. In addition, the authors of [22], [51] propose neighbor monitoring based techniques to detect the existence and location of attack nodes. However, the neighbor-based detection can be inefficient if a timely report from the neighbor nodes about the existence of the attacker is blocked due to the busy channel of the network under flooding bogus messages. To overcome that limitation, Cao et al. [8] propose to use the cluster head nodes which are trusted and serve as data fusion centers. In practice, e.g., for LPWAN, the cluster nodes can be the gateways or repeaters. Note that, for the detection-based methods, an isolation procedure, e.g., a blacklist of misbehaving nodes, can be activated (after the attacker found) to prevent the spreading of forge messages and thus significantly mitigate the magnitude of the attacks. In another solution, the authors of [58] propose a channel aware detection (CAD) system at the forwarding routers through channel estimation and traffic monitoring. If the monitored loss rate at certain hops exceeds the estimated normal loss rate, those involved nodes will be identified as attackers.

For EDAs using unencrypted frame counters in the MAC layer, storing the counter values in nonvolatile or flash memory [38] is worthwhile; so that even if the energy is lost, the state of the node can be restored and therefore this method can frustrate the attacker efforts. Nevertheless, slow access to flash memory, even with the requirement of additional hardware, may limit its use specifically for legacy and constrained devices. Improving duty-cycle communication, so-called duty-cycle optimization [72]–[75], can be the right way to mitigate unexpected energy consumption.

D. EDA DEFENSES IN THE NETWORK LAYER

Most concerns in the network layer are routing-based EDAs. Fortunately, there are also remarkable countermeasures to defeat them. One of the most recommended methods is to secure routing protocols. For example, the authors of [4] propose PLGPa, a protocol for the forwarding nodes to check the source routes by using a verifiable path in every packet with a non-replayable attestation (signature). The existence of the signature in every packet allows any node receiving it to validate the path. Every forwarding node can also verify the attestation chain to ensure that a packet has never traveled away from its route and thus enforce the packet to consistently move toward the destination. However, this method requires a modification to the original protocol and a potential firmware update that may not be suitable for LPW devices, particularly, the deployed ones. An alternate solution is to alter how intermediate nodes process the source route. To forward a message, a node must determine the next hop by locating itself in the source route. If a node searches for itself from the destination backward rather than from the source forward, any loop that includes the current node will be automatically truncated.

Trust mechanisms and avoidance approaches are also promising to prevent routing-based EDAs. In such mechanisms, each sensor monitors it neighbors, evaluates their trustworthiness, classifies them as either trustworthy or untrustworthy, and then discards untrustworthy sensors from the network. However, the attacker who is initially a legitimate member of the network can easily evade the detection by imitating the behavior of the legitimate sensors in the network. To prevent this evasion, the authors of [19] proposed a complementary defensive mechanism based on an entropy trust model to identify the attacker and a prevention-routing algorithm to proactively prevent the reroute behavior if any. The constraint is that this approach fails to detect highly cooperating (collusion) attacks as described in Section V-C.

Intrusion detection-based methods are quite popular and effective approaches to defeat EDAs [12], including the ones in the network layer. In our case, any kind of unauthorized or unapproved activities is called intrusions. An intrusion detection system (IDS) is a collection of the tools, methods, and resources to help identify, assess, and report intrusions. There are tremendous intrusion detection-based approaches for sensor networks [12], and several of them are effective for LPW networks such as statistical anomaly detection or the clustering approach. For example, IDSEP [23] is designed to detect malicious nodes based on energy consumption statistics of sensor nodes. If the battery of a node consumes in a given time over the estimated threshold, it is identified as a manipulated one. The parameters such as packet dropping rate due to false route updating and percentage of the changed routes can be added to the detection criteria to improve the accuracy of IDSs. However, the IDS-based approaches sometimes face certain challenges in balancing the trade-off among key factors such as the accuracy, detection time, energy-efficient usage or false-positive rate.

Rate limiting (limiting malicious sending rate) [8], [53] is likely another good defense to prevent EDAs in this layer but also potentially punishes honest nodes that may transmit large amounts of time-critical data.

With the support of only one-hop communication, there is probably no network layer in LPWAN networks (as shown in Fig. 4). A potential case is that LPWAN gateways connect to the LPWAN application server via IP-based protocols. However, we argue that the pair connection (gateway-cloud) in this case is out of range of LPW devices and often protected by secure protocols such as TLS. Therefore, the attack cases for LPWAN network layer may not happen in practice. Recently, there are several ideas to propose multi-hop communication in LPWAN [62], [63], and a source routing protocol is likely used. If those cases are applied to future business models, the mentioned defense methods still play a critical role to prevent the threats from routing-based EDAs.

E. EDA DEFENSES IN THE APPLICATION LAYER

Security vulnerabilities in the application layer can come from various sources, and they can be the inherent problem of software (the application code), from the cloud infrastructure, or even from the framework on which the control application runs. To counter such threats, it is required to propose a continuous protection mechanism across multiple classes, i.e., bug-free in software, secured APIs, safe code-execution in OS and so on. Due to the advantage of using the good facilities, e.g., well-protected networks and powerful servers, there are options to enforce the security to protect the LPW devices against both the insiders (internal attacks) and outsiders (external attacks) in the application layer. For example, TLS can be used to create an end-to-end security model between the LPW gateway and application server, and thus mitigate the exploitation of unauthorized access.

Similar to the other layers, the IDSs also appear to be promising to defeat the EDAs in this layer [28]. For the LPW devices with an OS, the power consumption distribution of each component/running task is the key criterion for the detection. Following the shape of consumption samples, it is not hard to figure out an abnormal running task, e.g., by comparing with the points of its working history or the shape of other sensors. Specifically, this model is also effective for the EDAs targeting computation on the sensors. For the simple sensors, i.e., without an OS, a similar IDS can be used but located at the LPW gateway or extensive systems such as cluster head nodes. To best defend the EDAs, the approach of an end-to-end solution or multiple protection layers such as [76] are ideal, although it is uncertain whether it is widely deployed.

F. SUMMARY

From the analysis of the defenses presented above, it is shown that the protection methods are specifically tailored to the EDA type, the layer where the EDA triggers and the LPW network model. Table 4 summarizes typically mentioned methods with our comments on the advantages and disadvantages for each.

The most selective approaches are IDSs and security scheme enhancement (secure content and route). This is consistent with the reality that they are also the most popular and comprehensive approaches in terms of reactive and proactive protection (as mentioned above). For the LPW devices, a delay of several seconds in responding to the request may not be a big problem but the accuracy of report data. Thus the security scheme enhancement (energy-efficient) is always the priority, and the second is the reactive protection. However,

TABLE 4. Summary of state-of-the-art EDA defense methods.

Mechanism	Attack target				Purpose				Target LPW		Implement-ation	Pros	Cons
	PHY	MAC	NET	APP	IDS	Secure content	Secure channel	Secure route	LPAN	LPWAN			
Statistical techniques [20], [45], [68]	✓	✓	✓	✓	✓				✓	✓	S	Simplicity and high accuracy	Tailored to specific attack cases
Multimodal statistics [45]	✓	✓			✓				✓	✓	S	High accuracy	Designed only for anti-jamming
Multiple channel hopping [20]	✓	✓					✓		✓	✓	R	Highly efficient	Consume much energy
Physical layer encryption [69], [70]	✓						✓				S	Hardware acceleration	Must modify the upper layers
Enhancing security scheme [8], [22], [24]		✓				✓			✓	✓	R	High accuracy	Complexity
Mutual authentication [7], [8]		✓							✓		C	Highly secure	Complexity
Intrusion detection [12], [22], [24], [51], [58]	✓	✓	✓	✓	✓				✓		S	Flexible design and detect many attack types	False positive rate, insuitable for in-sensor integration
Security Routing [3], [19]			✓					✓	✓		S	Build a list of trusted routes	Potential modification to the protocol
Trust mechanisms and avoidance [14]			✓			✓		✓	✓		S	Build a safe and trusted network	Vulnerable to bad mouthing attack
Rate limiting [53]		✓	✓				✓				S	Minimize the effect of the high rate attack	Potentially punish the legitimate nodes
Challenge-Response [7], [8]		✓				✓	✓	✓	✓	✓	S	Simplicity	Must wait the attack to happen first
End-to-end security [76]	✓	✓	✓	✓		✓	✓	✓	✓	✓	S	Highly secure	Expensive to deploy and require a good infrastructure

PHY(Physical), MAC(Medium Access Control), NET(Network), APP(Application)
S(Simulator: e.g., NS2, NS3, C++), R(Real sensors: e.g., Mica Mote)

satisfying the security requirements of the system/application in such approaches should be tailored to specific networks and layers (PHY/MAC/NET/APP).

Similarly, the location and flexibility of the system deployment are often different in EDA defenses. The security scheme enhancement has been integrated into the protocol or a firmware update, e.g., secure routing, whereas the detection-based methods do not require a modification like that but additional equipment. To judge which one is better, we may need to consider the effectiveness of investment (cost) on the real protection requirement of the networks. For example, an LPWAN network may not need routing-based EDA defenses. In fact, the best scenario is: proactive mechanisms should be complemented by reactive security. This complement is absolutely useful in the case of the basic security schemes that cannot cover the whole EDAs, particularly from the compromised sensors or IoT control applications. In that case, the defense such a reactive system can help to shield the remaining weak links of the system (i.e., against the attacks of the insiders). Also, while the researchers are in favor of proposing the IDS-based approaches and locating such protection systems in the gateway, they do not prefer the idea of an anti-EDA deployment inside the LPW sensors due to the inherent limitation of the LPW devices in terms of computation and energy.

Finally, due to the lack of facilities, the evaluation of existing studies heavily relies on simulation, instead of using real sensors. In such a model, due to the complexity of guaranteeing the reliability of the experiment, e.g., energy and error/noise model, implementing the solution on simulation frameworks such as NS2/NS3 should be preferred.

VII. ANALYSIS & OPEN RESEARCH

This section provides an overview of the expectations of the future anti-EDA systems, followed by our conclusion about state-of-the-art defense methods. Also, we discuss remarkable open challenges for future research. We believe that the following discussion may also be correct with other IoT enabling technologies.

A. EXPECTATIONS FOR THE FUTURE EDA DEFENSES

Most of the proposed defense mechanisms are typically tailored to a specific protocol, primarily in LPAN devices. For example, researchers have proposed to enhance the MAC security schemes to prevent the EDAs, but these approaches may require a fundamental modification to the networking layer or physical layer. Unfortunately, these could be infeasible to implement on massive IoT devices in practice. Following the above review of state-of-the-art defense methods, we conclude that the following guideline should be seriously considered in building the future EDA defenses:

- An EDA defense itself should not consume significant energy. The battery consumption of an anti-EDA system in sensors (if any) thus should be quantified carefully in the evaluation.
- Low-cost IoT devices, including LPW ones, are constrained to integrate a defense engine, even impossible [77]. In such cases, the top approach is to implement the security schemes and the changes in the PHY/MAC layer.
- The complexity and interoperability in multi-access networks, i.e., IoT connected world, incur difficulties in a holistic defense system, in which the security issues should be scrutinized by the application requirement and individual use cases.
- Most LPW packet headers are not encrypted; thus, unencrypted data become the most sources of security concerns. This flaw should be considered in all security designs; otherwise, they can be leveraged for the potential EDAs.
- Producing IoT devices now is no longer the exclusive match of well-established players such as flagship and leading vendors but also that of small manufacturers that target affordable accessories. This shift will raise the question of whether or not all these devices can be correctly implemented with the latest security standards. Also, the capability of small manufacturers for long-term services (e.g., publishing security patches) is questionable.
- The clients may have few motivations to pay for an enhancement on the security of their network side if the cost of the changes exceeds the need of the network. Updates to the core system if any, e.g., protocol stack, should be minimized.

Taking the above into account, a new comprehensive anti-EDA system should satisfy the following requirements:

- Energy-efficient usage is the priority and the high accuracy detection/prevention and effectiveness of deployment cost are so crucial.
- The ability to detect EDAs in as many layers as possible (e.g., the physical layer and above), but should prioritize the defenses against the threats to applications due to the probably limited resources on the devices.
- The system should cover a vast number of IoT enabling technologies and attack scenarios, while also balancing between the protection coverage and the deployment/replacement cost.
- For IDSs, the self-protection ability must be conducted to avoid several attacks target the defense system itself (e.g., flooding the attack data to overload the defense's computation ability and thus diminish the security protection).
- The system should be flexible to interact with assistive platforms such as a firewall or be deployed in the future network platform such as mobile edge computing servers and software-defined networks (SDN) for IoT.
- Each technology may have multiple legacy instances (i.e., with old firmware versions) already deployed on commercial products [2], [8]. The existence of the legacy implementations urges the developers and manufacturers to propose the protection mechanisms that not only deal with new applications but also consider the compatibility with old devices, including the available ones on the market.
- The defense architecture should be well specified to specific applications, but also be modular and thus permit a wide variety of technology types and features in an extensible manner (e.g., add-ons).

So far, it is quite hard to find in existing solutions that satisfy all the above requirements. However, from our perspective, the defense should balance the trade-off between the above factors and support as many features as possible, including the efficiency (e.g., performance) and the cost. Pursuing an ideal solution to satisfy every requirement is unlikely a right way to go. Depending on the LPW applications and their specific protection requirement, the designer should prioritize proper factors, e.g., the efficiency vs. the cost or secure channel vs. secure content.

B. OPEN RESEARCH

Even though specific aspects of EDAs and defenses have been addressed, there are still a number of interesting open research directions. We list the following research issues by their priority to deal with, e.g., the urgency of the remaining fundamental security issues of the emerging technologies, however, each issue could be independently conducted in depth.

As summarized in Table 3 and Table 4, various EDA patterns are common to LPW technologies, in which each of the technology is vulnerable to at least one of the variants of EDAs. Besides the lack of strong security schemes and a holistic defense tactic, a diversity of available exploitation tools and vulnerabilities also make the system easily attacked by EDAs. However, the aforementioned attacks and defenses on new and dominant LPW technologies such as NB-IoT have not yet thoroughly been addressed, e.g., potential influence of the vulnerabilities inherit from conventional LTE networks, and therefore this is also a potential topic of concern for further study. Moreover, the EDAs in the PHY/MAC layers are the most effective and proven to bring serious damage in LPW technologies (mentioned in Section V-A, V-B). Therefore, thorough research on these layers for dominant LPW technologies, even only through the technical specification and protocol standards, can reveal unknown issues. Continuing on this topic, using the standard Dolev-Yao attacker model [78] and tools such as ProVerif [79] to verify the vulnerabilities of security protocols in such technologies can be also another promising approach.

Conducting EDAs and exploiting relevant vulnerabilities in IoT heterogeneous networks are also another exciting direction. In the future, heterogeneous implementations for various technologies, including LPW devices from various providers, may introduce potential vulnerabilities such as bugs of firmware, defects of hardware and flaws in the protocol design. Potentially valuable work is to assess commercial LPW products, including IoT platforms and firmware, to get a clearer view of the security weaknesses and whether or not the vulnerabilities as mentioned earlier have been fixed. The quantifiable results are preferred in all cases. The assessment results may reveal many interesting results, e.g., whether all products are updated with the highest security standards, or the manufacturers may pull out several required security features due to the cost or are incredibly careless in initializing the default values for the security setting of their products.

Also, network key generation, storage, and management are still gaps in LPW networks. The implementation of generating and storing keys can introduce vulnerabilities. For example, a compromise in the keys of an IoT device may bypass the security of communications between other devices. Leveraging this compromise, the attacker can spoof messages and abuse to launch EDAs, e.g., routing-based attacks. Therefore, an investigation on this issue is worthwhile, especially, for the legacy devices on the market or deployed in the industrial/critical infrastructure.

For EDA defense solutions, prior proposals have simulated promising results, mainly, in specific contexts but that does not mean they are deployed in practice for certain reasons, e.g., infeasible to upgrade LPW deployed devices' firmware. Therefore, we conclude that IDS is a comprehensive and highly effective approach to mitigate and defeat EDAs. In such a system, the approach of on-demand anti-EDA services in the fog layer is promising. However, for the IDS-based solutions, particularly, those relying on traffic analysis, the difficulties in collecting a massive IoT available data incur the major obstacles to improve the detection accuracy. Thus, generating/collecting a qualified IoT security dataset (e.g., energy usage, attack log), no matter where it comes – a particular IoT industry (critical infrastructures such as a smart city) or a generic source – will be beneficial for the research community.

For EDA evaluation, the preferable scenario is to use real devices and a large topology as possible. However, there may be obstacles to do that (e.g., due to a limited budget on the project). In this context, simulation is a natural selection. Although simulation/emulation has significant benefits (e.g., easy to deploy a large-scale network model), the main obstacle is the lack of the implementations of fundamental components such as the energy and error model in the physical and MAC layers of LPWAN technologies, e.g., NB-IoT. Therefore, we believe that a simulation implementation for new technologies (e.g., an NB-IoT module for NS3 [80]) relying on a reliable power consumption/error model will potentially be a significant contribution to the community.

Finally, the future of the Internet may rely on the connectivity of both LPW networks and next-generation networks such as 5G [81]. In a connected world, EDAs can be initiated from not only equipment connected to LPW networks but also traditional network devices. Hence, a promising approach is to exploit vulnerabilities of interoperability communication schemes or weak links in the network to launch attacks, including EDAs. For example, inter-operable IoT gateways may be controlled from a remote application (e.g., at home). An attacker can find an indirect approach to obtain the privilege to control these gateways by exploiting known vulnerabilities of the computer that installed the remote program. For LPWAN networks such as LoRa, massive devices connected with a centralized server prove the feasibility of this approach. If the adversary can compromise the application server, he can easily adjust the duty-cycle of the whole end-devices in the network. Although a strong and secure communication method may solve the problem; however, such a mechanism for interoperability communication among network technologies with various characteristics are under development and unlikely to be done soon. A MEC-based defense accommodates with traffic filtering features for IoT devices at 5G mMTC slice could be a starting point.

VIII. CONCLUSION

The explosion of low-cost IoT devices raises major security concerns, including EDAs. In this review, we have discussed the impacts of EDAs on LPW networks and present the insights into featured EDA types as well. In this moment, or even in the future, there is no indication that the whole network and IoT devices will be updated with the latest security patches to resist EDAs for certain reasons such as the extra cost. Therefore, EDAs will continue to be the security threats in LPW networks and IoT infrastructure. To mitigate EDAs, we highlight several proposed defenses, but none of them are perfect. Some require an infeasible adjustment in a large-scale network while others assume that any device may easily get a firmware update for new designs such as a new authentication scheme. However, this update is unlikely an easy task for most legacy and low-cost devices. We hope that our assessment can inspire the manufacturers to improve their next generation products or urge the standard organizations to fix the flaws and the poor security design if any in the future specifications. Particularly, the open research directions may motivate other researchers to continue our work and significantly contribute to deal with the addressed issues. At last, depleting energy is an extremely effective method to take down a sensor network or disable a battery-based device. This is a clear warning to the developers and the research community that EDAs are still real threats they must take care of, particularly in the sensor networks connected to critical infrastructures.

REFERENCES

[1] (Nov. 13, 2018). *Statista*. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018.

[3] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 367–380, Jan. 2009.

[4] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless Ad Hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 318–332, Feb. 2013.

[5] D. C. Nash, T. L. Martin, D. S. Ha, and M. S. Hsiao, "Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices," in *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2005, pp. 141–145.

[6] N. Geethanjali and E. Gayathri, "A survey on energy depletion attacks in wireless sensor networks," *Int. J. Sci. Res.*, vol. 3, no. 9, Sep. 2014.

[7] Z. He and T. Voigt, "Droplet: A new denial-of-service attack on low power wireless sensor networks," in *Proc. IEEE 10th Int. Conf. Mobile Ad-Hoc Sensor Syst.*, Oct. 2013, pp. 542–550.

[8] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy depletion attack on ZigBee-based wireless networks," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 816–829, Oct. 2016.

[9] R. P. Muthu and M. Suseela, "Effect and defense of resource depletion attacks in wireless Adhoc sensor networks," *Int. J. Inf. Technol. Syst.*, vol. 3, no. 1, pp. 1–7, Jun. 2014.

[10] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep deprivation attack detection in wireless sensor network," *Int. J. Comput. Appl.*, vol. 40, no. 15, pp. 19–25, Jan. 2012.

[11] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," *Int. J. Distrib. Sensor Netw.*, vol. 2, no. 3, pp. 267–287, Jul. 2006.

[12] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart. 2014.

[13] V. Shakhov, I. Koo, and A. Rodionov, "Energy exhaustion attacks in wireless networks," in *Proc. Int. Multi-Conf, Eng., Comput. Inf. Sci. (SIBIRCON)*, Sep. 2017, pp. 1–3.

[14] V. Shakhov and I. Koo, "Depletion-of-battery attack: Specificity, modelling and analysis," *Sensors*, vol. 18, p. 1849, Jun. 2018.

[15] J. Uher, R. G. Mennecke, and B. S. Farroha, "Denial of sleep attacks in bluetooth low energy wireless sensor networks," in *Proc. IEEE Military Commun. Conf.*, Nov. 2016, pp. 1231–1236.

[16] U. Fiore, A. Castiglione, A. De Santis, and F. Palmieri, "Exploiting battery-drain vulnerabilities in mobile smart devices," *IEEE Trans. Sustain. Comput.*, vol. 2, no. 2, pp. 90–99, Apr./Jun. 2017.

[17] B. R. Moyers, J. P. Dunning, R. C. Marchany, and J. G. Tront, "Effects of Wi-Fi and bluetooth battery exhaustion attacks on mobile devices," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, Jan. 2010, pp. 1–9.

[18] K.-F. Krentz, C. Meinel, and H. Graupner, "Countering three denial-of-sleep attacks on ContikiMAC," in *Proc. Int. Conf. Embedded Wireless Syst. Netw. (EWSN)*, Feb. 2017, pp. 108–119.

[19] Y. Cho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, Aug. 2013.

[20] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *Proc. 4th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, Jun. 2007, pp. 60–69.

[21] H. Kim, K. G. Shin, and P. Pillai, "MODELZ: Monitoring, detection, and analysis of energy-greedy anomalies in mobile handsets," *IEEE Trans. Mobile Comput.*, vol. 10, no. 7, pp. 968–981, Jul. 2011.

[22] Q. Dong, D. Liu, and P. Ning, "Providing DoS resistance for signature-based broadcast authentication in sensor networks," *ACM Trans. Embedded Comput. Syst. (TECS)*, vol. 12, no. 3, Mar. 2013, Art. no. 73.

[23] G. Han, J. Jiang, W. Shen, L. Shu, and J. Rodrigues, "IDSEP: A novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," *IET Inf. Secur.*, vol. 7, no. 2, pp. 97–105, Jun. 2013.

[24] A. T. Capossele, V. Cervo, C. Petrioli, and D. Spenza, "Counteracting denial-of-sleep attacks in wake-up-radio-based sensing systems," in *Proc. 13th Annu. IEEE Int. Conf. Sensing, Commun., Netw. (SECON)*, Jun. 2016, pp. 1–9.

[25] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.

[26] F. Rayal, "Mobile and wide-area IoT: LPWA and LTE connectivity," Xona Partners, Silicon Valley, CA, USA, White Paper 1, Jan. 2016.

[27] K. Cengiz and T. Dag, "A review on the recent energy-efficient approaches for the Internet protocol stack," in *EURASIP Journal on Wireless Communications and Networking*. Cham, Switzerland: Springer, 2015.

[28] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3496–3509, 4th Quart. 2018.

[29] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[30] C. Hennebert and J. D. Santos, "Security protocols and privacy issues into 6LoWPAN Stack: A synthesis," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 384–398, Oct. 2014.

[31] J. H. Kong, L.-M. Ang, and K. P. Seng, "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments," *J. Netw. Comput. Appl.*, vol. 49, pp. 15–50, Mar. 2015.

[32] J. Granjal, E. Monteiro, and J. S. Silva, "Security in the integration of low-power wireless sensor networks with the Internet: A survey," *Ad Hoc Netw.*, vol. 24, pp. 264–287, Jan. 2015.

[33] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proc. IEEE GLOBECOM*, Dec. 2010, pp. 1–5.

[34] R. Min and A. Chandrakasan, "Top five myths about the energy consumption of wireless communication," *ACM SIGMOBILE*, Jan. 2003, pp. 1–2.

[35] *Bluetooth Low Energy Attack Tool*. Accessed: Jan. 4, 2018. [Online]. Available: https://gattack.io/

[36] *Radio Frequency Communication Protocol Hacktools*. Accessed: Sep. 12, 2017. [Online]. Available: https://github.com/cn0xroot/RFSec-ToolKit

[37] R. Miller, "LoRa security building a secure LoRa solution," MWR Labs, London, U.K., MWR Labs White Paper 1, 2016.

[38] *LoRa Specification 1. 1*, LoRa Alliance, Inc, 2017.

[39] "Make things come alive in a secure way," Sigfox White paper Security, Jan. 2017.

[40] P. Cope, J. Campbell, and T. Hayajneh, "An investigation of bluetooth security vulnerabilities," in *Proc. IEEE 7th Annu Comput. Commun. Workshop Conf. (CCWC)*, Mar. 2017, pp. 1–7.

[41] *Zigbee Exploitation*. Accessed: Jun. 2018. [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

[42] *Zigbee Attack Tool*. Accessed: Jun. 26, 2018. [Online]. Available: https://github.com/riverloopsec/killerbee

[43] *Bluetooth Low Energy Attack Tool*. Accessed: Jan. 4, 2018. [Online]. Available: https://github.com/DigitalSecurity/btlejuice

[44] *Z-Wave Security Testing Tool*. Accessed: Dec. 4, 2017. [Online]. Available: https://github.com/appzer/openhab/wiki/ZWave-Security-Testing

[45] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May./Jun. 2006.

[46] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proc. IEEE INFOCOM-26th IEEE Int. Conf. Comput. Commun.*, May 2007, pp. 1307–1315.

[47] Y.-A. Tan, X. Zhang, K. Sharif, C. Liang, Q. Zhang, and Y. Li, "Covert timing channels for IoT over mobile networks," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 38–44, Dec. 2018.

[48] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proc. 3rd ACM Workshop Wireless Secur.*, Oct. 2004, pp. 32–42.

[49] A. K. Nain, J. Bandaru, M. A. Zubair, and R. Pachamuthu, "A secure phase-encrypted IEEE 802.15.4 transceiver design," *IEEE Trans. Comput.*, vol. 66, no. 8, pp. 1421–1427, Aug. 2017.

[50] A. Ali, A. G. Shah, and J. Arshad, "Energy efficient techniques for M2M communication: A survey," *J. Netw. Comput. Appl.*, vol. 68, pp. 42–55, Jun. 2016.

[51] M. Li, S. Salinas, P. Li, J. Sun, and X. Huang, "MAC-layer selfish misbehavior in IEEE 802.11 ad hoc networks: Detection and defense," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1203–1217, Jun. 2015.

[52] D. E. Boubiche and A. Bilami, "A defense strategy against energy exhausting attacks in wireless sensor networks," *J. Emerg. Technol. Web Intell.*, vol. 5, no. 1, pp. 18–27, Feb. 2013.

[53] D. R. Raymond and S. F. Midkiff, "Clustered adaptive rate limiting: Defeating denial-of-sleep attacks in wireless sensor networks," in *Proc. MILCOM-IEEE Military Commun. Conf.*, Oct. 2007, pp. 1–7.

[54] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of LoRa," in *Proc. 3rd IEEE Int. Conf. Cybern. (CYBCONF)*, Jul. 2017, pp. 1–6.

[55] *Huawei IoT Security White Paper*. Accessed: Nov. 13, 2018. [Online]. Available: https://www.huawei.com/minisite/iot/img/hw_iot_secutity_white_paper_2017_en_v2.pdf

[56] "LPWA technology security comparison," Franklin Heath Ltd, Huawei, China, White Paper 2, May 2017.

[57] E. V. Es, H. Vranken, and A. Hommersom, "Denial-of-service attacks on LoRaWAN," in *Proc. 13th Int. Conf. Availability, Rel. Secur. (ARES)*, Aug. 2018, p. 17.

[58] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNs," *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1661–1675, May 2010.

[59] *6LoWPAN Overview*. Accessed: Jan. 12, 2019. [Online]. Available: https://en.
wikipedia.org/wiki/6LoWPAN

[60] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *Proc. Int. Conf. Pervasive Comput. (ICPC)*, Jan. 2015, pp. 1–6.

[61] B. Fouladi and S. Ghanoun, "Security evaluation of the Z-wave wireless protocol," Blackhat, 2013.

[62] M. Bor, J. Vidler, and U. Roedig, "LoRa for the Internet of Things," in *Proc. Int. Conf. Embedded Wireless Syst. Netw. (EWSN)*, Feb. 2016, pp. 361–366.

[63] C.-H. Liao, G. Zhu, D. Kuwabara, M. Suzuki, and H. Morikawa, "Multi-Hop LoRa networks enabled by concurrent transmission," *IEEE Access*, vol. 5, pp. 21430–21446, 2017.

[64] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015.

[65] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct./Dec. 2017.

[66] *LoraWAN Solution Providers*. Accessed: Jan. 2019. [Online]. Available: https://www.thethingsnetwork.org/

[67] M. H. R. Khouzani and S. Sarkar, "Maximum damage battery depletion attack in mobile sensor networks," *IEEE Trans. Autom. Control*, vol. 56, no. 10, pp. 2358–2368, Oct. 2011.

[68] O. Osanaiye, S. A. Alfa, and G. P. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 18, no. 6, p. 1691, May 2018.

[69] H. Jeon, J. Choi, W. S. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 619–625, Apr. 2013.

[70] J. Zhu, Y. Zou, and B. Zheng, "Physical-Layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 5313–5320, 2017.

[71] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 6, pp. 3590–3602, Jun. 2015.

[72] B. Djamaa and M. A. Richardson, "Improved broadcast communication in radio duty-cycled networks," Centre Electron. Warfare, Cranfield Univ., Shrivenham, U.K., Tech. Rep. 1, 2015.

[73] P. Park, S. C. Ergen, C. Fischione, and A. Sangiovanni-Vincentelli, "Duty-cycle optimization for IEEE 802.15.4 wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 10, no. 1, p. 12, Nov. 2013.

[74] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy-efficient mechanisms in security of the Internet of Things: A survey," *Comput. Netw.*, vol. 127, pp. 173–189, Nov. 2017.

[75] Y. Zhang, S. He, and J. Chen, "Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1632–1646, Jun. 2016.

[76] G. Zheng, R. Shankaran, A. M. Orgun, L. Qiao, and K. Saleem, "Ideas and challenges for securing wireless implantable medical Devices: A review," *IEEE Sensors J.*, vol. 17, no. 3, pp. 562–576, Feb. 2017.

[77] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, and N. M. Khan, "A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 39–95, 1st Quart. 2018.

[78] S. Schneider and P. Ryan, *The Modelling and Analysis of Security Protocols: The CSP Approach*. London, U.K.: Pearson Education.

[79] *Automatic Cryptographic Protocol Verifier*. Accessed: Jan. 2019. [Online]. Available: http://prosecco.gforge.inria.fr/personal/bblanche/proverif/

[80] *Network Simulator Software*. Accessed: Jan. 4, 2018. [Online]. Available: https://www.nsnam.org/

[81] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of LoRaWAN and 4G/5G for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 60–67, Feb. 2018.

VAN-LINH NGUYEN received the B.E. and M.Sc. degrees in data communication and networking from the University of Information and Communication Technology and the University of Engineering and Technology, Vietnam National University, in 2011 and 2015, respectively. He is currently pursuing the Ph.D. degree in computer science and information engineering with National Chung Cheng University (CCU), Taiwan. His research interests include network security, the Internet of Things, edge computing, and software-defined networks.

PO-CHING LIN received the Ph.D. degree in computer science from National Chiao Tung University, Hsinchu, Taiwan, in 2008. He joined the faculty of the Department of Computer and Information Science, National Chung Cheng University, in 2009, where he is currently an Associate Professor. His research interests include network security, network traffic analysis, and performance evaluation of network systems.

REN-HUNG HWANG received the Ph.D. degree in computer science from the University of Massachusetts, Amherst, MA, USA. He joined the Department of Computer Science and Information Engineering, National Chung Cheng University (CCU), in 1993, where he is currently a Distinguished Professor. He has published over 200 international journal and conference papers. He has served as the Dean of the College of Engineering (2014–2017). He received the IEEE Best Paper Award from the IEEE Ubi-Media 2018, the IEEE SC2 2017, the IEEE IUCC 2014, and the IEEE Outstanding Paper Award from the IEEE UIC 2012. His current research interests are the Internet of Things, network security, cloud/edge/fog computing, and software-defined networks.