



A survey on energy-aware security mechanisms



Alessio Merlo^{a,*}, Mauro Migliardi^b, Luca Caviglione^c

^a Computer Security Lab (CSeCLab), DIBRIS - University of Genoa, Via all'Opera Pia, 13, 16145, Genoa, Italy

^b DEI - University of Padua, Italy

^c ISSIA - CNR, Genoa, Italy

ARTICLE INFO

Article history:
Available online 14 May 2015

Keywords:
Security
Energy-aware security
Green networking
Mobile devices

ABSTRACT

The increasing adoption of mobile devices as the preferred tool to access the Internet imposes to deepen the investigation of security aspects. In parallel, their power constrained nature must be explicitly considered in order to analyze security in an effective and comprehensive manner. This aspect, which is often neglected in the literature, allows investigating two important behaviors of mobile devices: (i) evaluate if all the layers accounting for privacy and security can be re-engineered or optimized to save power, and (ii) understand the effectiveness of draining energy to conduct attacks.

In this perspective, this paper surveys and highlights the most recent work on energy-awareness and security. Also, it summarizes the current state of the art on general techniques to save energy, as well as tools to perform measurements. The major contributions of this survey are, thus, a review of past work aimed at minimizing the energy footprint of security mechanisms, and the identification of promising research trends, such as detecting attacks via anomalous power consumption.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

According to [1], the power required to run the most popular ICT infrastructures leads to high economical costs and severe environmental footprints, especially in terms of Green House Gases (GHG) and emissions of CO₂. Therefore, developing some form of energy-awareness has been part of the research agenda on computing [2,3] and networking [4,5] for more than a decade. Such efforts have been defined as *green computing* and *green networking*, respectively. However, they often neglect the security aspect. While it could be acceptable in the past, the actual panorama imposes its explicit consideration, at least for two different aspects: the ubiquitous diffusion of battery-operated devices to access and store a variety of sensitive data [6], and the huge population of Internet users resulting into large-scale hardware deployments.

As a consequence, investigating techniques or solutions dedicated to making security more energy-efficient is a mandatory aspect, even more since in the past there has not been a systematic review of these efforts, while, on the contrary, they have been partially addressed separately in different fields, e.g., networking, computing and hardware/software design. Furthermore, previous surveys dealing with greening aspects were not mentioning security or privacy. For instance, [7,8] review the research done in the field of networks, with emphasis on methodologies ranging from silicon efficiency to dynamic management of the whole network infrastructure (e.g., by shutting down some routes to achieve power savings). Despite the fact that improving the performances of hardware or protocols would also enhance the efficiency of security

* Corresponding author. Tel.: +39 010 353 2344.
E-mail address: alessio.merlo@unige.it (A. Merlo).

frameworks using such facilities, this is never explicitly discussed or evaluated. Ref. [9] deals with cloud computing without mentioning possible improvements by pursuing a more efficient security management, while [10] focuses on general attacks to increase power consumption of large-scale datacenters but without considering countermeasures. Lastly, similar considerations apply to Ref. [11], which analyzes recent data management techniques to reduce energy consumption.

In this perspective, this survey reviews the past work investigating relationships among security and energy. In detail, we considered papers meeting at least one of the following requirements: (i) they offer advancements in understanding the impacts of energy-saving practices and techniques on security; (ii) they introduce novel algorithms, architectures and protocols to reduce the energy consumption; (iii) they consider energy itself as an entity to protect (e.g., against malicious battery drain attacks); (iv) they consider energy as an indicator to reveal threats with a high degree of stealthiness [12].

To summarize, the contributions of this paper are:

1. to review the most recent and effective works on the optimization related to energy costs of security techniques deployed in mobile devices, network nodes and Wireless Sensors Networks (WSN);
2. to analyze studies quantifying the requirements in terms of power and/or energy of the most popular algorithms and protocols used to enforce security in the Internet;
3. to showcase innovative attacks or detection techniques leveraging energy consumption;
4. to evaluate the effectiveness and the accuracy of the most popular tools used to quantify the power used within real-world mobile devices, with emphasis on smartphones.

With regard to the authors' best knowledge, this is the first work surveying energy optimizations and security implications, and it thoroughly extends our previous investigation [13]. In more detail, this paper increases the amount of papers analyzed, enhances the discussion of the background, and also considers practical aspects of tools employed to measure the energy consumption in mobile appliances.

The remainder of the paper is structured as follows: Section 2 portrays the overall architecture of the survey. Section 3 discusses the energy management and the optimization techniques, which can be successfully adopted to optimize security aspects. Section 4 deals with the reduction of energy costs related to security, Section 5 discusses the case of WSN, Section 6 discusses the concept of energy as an asset to be defended and energy as an asset to be leveraged to enhance security. Section 7 reviews the most popular tools to measure consumptions, and, finally, Section 8 concludes the paper by discussing future directions on energy-aware security [14].

2. Survey architecture

To properly discuss related papers, group techniques and possible advancements, we designed the survey in the following manner:

- Section 3 briefly introduces fundamentals of energy management, with emphasis on possible relationships with security mechanisms;
- Section 4 provides an analysis on reduction of energy cost of security aspects. Specifically, it addresses two different kind of entities populating the Internet:
 - end nodes: due to the presence of batteries, mobile nodes are the most important playground where optimizing the impact of security algorithms in terms of energy consumption. Hence, proposals aimed at reducing the footprint of security aspects in end nodes belong to this category;
 - network nodes: modern telecommunication infrastructures must have sophisticated mechanisms to enforce security. Yet, the huge amount of served users requires making optimizations in different layers of the ISO/OSI protocol stack. Thus, here we review papers presenting optimizations/enhancements of network-centric security solutions.
- Section 5 discusses WSN. As energy-awareness is already a mainstream topic in this context, since it has always been considered as a design constraint, here we will only focus on studies explicitly dealing with energy-aware security aspects;
- Section 6 considers energy as an asset to protect, as it already happens for hardware or machineries. Especially, we separately address two different facets:
 - an asset to be protected: limited power availability makes mobile appliances fragile. Hence, many attacks aim at draining power to reduce the lifetime of a device (e.g., via traffic stimulation or by preventing sleep states);
 - an asset for detection: we consider here studies dealing with energy as a metric to detect malicious activities.
- Section 7 analyzes measurement tools. In fact the precise quantification of the energy consumption of algorithms and hardware components is still an open research problem. Besides, without exact measurements, it is difficult to understand what is to be optimized and to fully assess the achieved gains. Accordingly, here we review the most popular tools used to measure consumption with emphasis on solutions used in the surveyed literature.

3. A general overview of energy management and security

This section discusses the general methodologies for energy-efficient computing and networking, with emphasis on solutions that can be used in the perspective of reducing the energy consumption of security protocols or frameworks.

Moreover, a particular attention will be put on considering wireless technologies, which account for a relevant fraction of power drains in modern mobile devices. From the perspective of developing energy awareness, the following *three* main complexity drivers of the Internet play a major role:

1. *architectural*: the diffusion of wireless access networks, especially those based on the IEEE 802.11 and Long Term Evolution (LTE), increase the heterogeneity of the overall deployment. Besides, wireless loops are power consuming, both from the viewpoint of devices and the carrier (see, e.g., Ref. [15] and references therein);
2. *functional*: ubiquitous access to Online Social Networks (OSNs) like Facebook and Google+, Web 2.0 and highly interactive services increase the traffic and the operations to be performed within the device (e.g., the usage of AJAX-like paradigms). Additionally, the vast amount of sensitive data augments the need of proper security/privacy layers eventually boosting energy consumption [16];
3. *entities*: the plethora of devices (smartphones, network appliances and gaming consoles), jointly with the Internet of Things (IoT) paradigm, lead to very composite set of entities, also with very mixed requirements, e.g., in terms of battery capacity, CPU power, bandwidth and storage. This should motivate the introduction of proper coherency layers, both for managing energy and the access to/control of network/physical resources. For instance, a cutting edge research deals with the development of energy management techniques built in the inner layer of mobile Operating Systems (OS), e.g., energy-aware schedulers (see, Ref. [17] for a recent survey on the topic).

As a consequence, the development of energy-aware mechanisms must be pursued both in end nodes and in the network. While the field of research called green networking is now very mature, the wide variety of mobile nodes still needs a deep investigation [17]. Concerning security, features (1)–(3) have twofold implications: (i) more people demanding for increased privacy/security guarantees lead to relevant energy consumption, and (ii) for battery operated devices, or sensors deployed in unattended areas, power is a resource to be secured, for instance, by avoiding an attacker to maliciously deplete batteries.

Therefore, in the remainder of the section we showcase techniques and papers dealing with optimizations that could be also beneficial in the perspective of taming energy consumption of security algorithms. We point out that enforcing security of always-connected devices, sensors or appliances, mainly involves the constant exchange of data over the Internet. Hence, we will also review basic methodologies used for the reduction of energy footprints within the network infrastructure.

3.1. Energy optimization for mobile nodes

Nowadays, mobile devices and sensors are equipped with powerful hardware and employ very complex software layers. Yet, despite the growth of their “brute force”, battery technology has not experienced the same trend of evolution. Even with the adoption of lithium-ion batteries, devices such as handsets still have in energy consumption the most severe limitation [17]. Put briefly, the main methods suitable to reduce the energy costs of security are:

1. *silicon-efficiency*: are practices rooted within the advancements in microprocessor design. Among the others, those aiming at reducing static currents of Integrated Circuits (ICs) are the most promising [18];
2. *smart hardware management*: contains techniques ranging from smart sleeping, to the selective idling of unused components like storage units [19];
3. *energy-aware operating systems/software*: embraces all the software components explicitly engineered for battery-operated devices such as smartphones and tablets. In detail, this contains ad-hoc operating systems [20], or middleware aiming at reducing the energy drains of applications, while guaranteeing high performances;
4. *energy-efficient air interfaces and protocols*: are those methods aiming at reducing wastes due to an inefficient usage of the transmission power (see, e.g., Ref. [21] for a survey of optimizations for the IEEE 802.11);
5. *device offloading*: consists in shifting into network-centric or cloud-like facilities the most energy-consuming operations [22].

Surely, implementing methods (1)–(4) reduce the energy consumption of security mechanisms, even if in a “for free” fashion. Yet, they require a major re-engineering of the device or the protocols resulting in a long phase-in.

According to the high ferment of the actual research panorama on cloud computing, the methodology presented in (5) appears as one of the most promising technique in the field of developing solutions explicitly aiming at reducing energy consumption of security. As explained in [23], a recent trend is to use a lightweight local agent running on the phone delegating tasks like virus detection to a remote facility. This approach uses an order of magnitude less CPU and memory, also leading to reduced energy consumption when compared with existing on-device antivirus software. In a similar manner, having applications to be installed through application stores (at least for the case of smartphones and tablets) could lead to a potential reduction of power depletion in devices, since checking software offline before the delivery to customers would reduce the need of power demanding online tests [24].

3.2. Energy optimization for network infrastructure

The more pervasive and complex characteristics of Internet services lead to scenarios where many resources and applications are mixed together. The intrinsic distributed nature of this “diffuse” architecture imposes to deploy proper protocols to guarantee the secure exchange of information among the involved entities. For instance, personal details

Table 1

Summary of enhancements and issues when optimizing energy consumption of security mechanisms with the most popular greening techniques.

Devices	Enhancements	Security issues
Silicon efficiency	Especially suited for computational intensive tasks (e.g., cryptography)	New HW is needed
Smart HW	Especially suited for intermittent tasks (e.g., key generation)	New HW is needed
Energy-aware OS	Overall enhancement to SW	Potential new exploits
Energy-aware L2	Improvements for network traffic carrying security data	Possible new attacks preventing sleep
Device offloading	Shift the complexity from the device	Single point of failure
		Sensitive data centralized
Network		
Architectural	New ad-hoc entities to handle security in optimized manners	New target for attacks
		E2E semantic issues
Traffic	Especially for chatty protocols such as key exchange	No realistic models
		New forging attacks
Protocols	Possibility of re-design to consider 4G and intermittent connectivity	Time to get standard
		New vulnerabilities

are constantly delivered among several devices and appliances for syncing purposes. Hence, the presence of security mechanisms heavily impacts on their energy consumption, and can clash with green requirements [24]. Alas, optimizing the enforcement of security over the Internet relies upon a very composite “problem space”, specifically [14]:

1. some security mechanisms may require proper architectural elements to be placed in the network, e.g., key distribution servers, or Authentication Authorization and Accounting (AAA) machineries;
2. to secure communications additional traffic could be needed, e.g., to exchange keys, or because of the overhead required for signaling and encrypted information or credentials;
3. security needs additional protocols and software layers, which increase energy consumption through CPU usage. At the same time, if they are implemented via ICs, they still require proper power;
4. users access the Internet both via wireless and wired access networks. Thus, security mechanisms could be deployed at different layers, according to the specific technology used at the physical level.

Therefore, items (1)–(4) affect the power efficiency of the network deployment, and could benefit from many green-based techniques. In this perspective, the network could implement some smart sleeping methods. Especially, devices such as routers or authentication/keys distribution servers can react to particular traffic or security criteria via dynamically adjusting their idle periods, reducing the voltage of their CPUs, or activate/deactivate in real-time portion of the hardware/network link to meet some performance criteria.

Another possible solution is to have protocols scaling according to the features provided by the lower layers of the stack. One of the most adopted workaround is to shift the complexity at the border of the network by using proxy-based architectures [24], where end-nodes are masqueraded via ad-hoc techniques enabling them to dynamically change their energy profiles, e.g., via smart sleeping or other power saving mechanisms.

At the same time, having “intelligence” in the network to optimize energy consumption (despite being for traffic or security purposes) or additional machineries (e.g., middle-boxes to prevent propagation of wastage) raises a security issue “by design”, since: (i) the entity running the optimization software in charge of managing devices or computing strategies to dynamically reconfigure the network could be perceived as a target for an attack (see, e.g., Ref. [25] for an example of a centralized decision maker). In this sense, without proper countermeasures the overall architecture will be more fragile; (ii) proxies and middleboxes could break the end-to-end semantic of many security mechanisms, enabling new attacks (à la Man In the Middle); (iii) more devices imply more hardware/software having additional insecurities or exploitable bugs.

Table 1 offers a condensed comparison of enhancements and issues when optimizing energy consumption of security mechanisms with the most popular greening techniques. As it can be noticed, the trade-off among energy efficiency, security and energy-efficient security must be carefully investigated, and such aspect has been considered to survey the papers found in the reference literature. Even if definitely outside the scope of this work, understanding the security implications of greening techniques must become a relevant part of the future research agenda.

4. Reducing energy costs of security

While the energetic cost of security techniques has been investigated in past work, as it has been summarized in [26], there has been only a very limited amount of studies dedicated to analyzing if and how it is possible to leverage security to save energy. The rationale of the works belonging to this field of research is: *any operation concerning security reasons has to be done as soon as possible in order to avoid waste of energy due to malicious activities*. More specifically, this allows reducing the waste of resources consumed by activities that have to be stopped before completion in any case. Thus, by making an aggressive use of security mechanisms, it should be possible to save energy. In past works, this approach has been tested only in the case of Intrusion Detection Systems (IDS) as to limit the amount of resources squandered by traffic generated by malware and intrusion attempts.

As previously discussed, green networking has been a very hot topic for quite a few years now and has reached a significant level of maturity proposing several solutions to have a more energy-aware behavior both for core routers and appliances placed at the border of the network. In more detail, many studies demonstrated how to move from energy-agnostic networking devices, e.g., devices that are either off or have maximum consumption, toward fully energy-aware network devices capable of energy consumption proportional to their load [27]. However, the majority of the approaches does not take into account the costs of security. For instance, many works dealing with greening mechanisms allow to reduce the energy costs of Protocol Data Units (PDUs) on a per-byte basis, but ignore that a relevant volume of PDUs may be malicious. Thus, this requires security solutions, for instance, to analyze such unwanted data. Additionally, the energy for the needed security analysis may overcome the costs of routing the PDU itself. Therefore, strategies to reduce the energy cost of security must be taken into account on large-scale Internet Service Providers (ISPs) or in core networks.

Moreover, security also impacts on energy consumption within end-nodes, which are the source/destination of the Internet traffic. This is a relevant concern for mobile entities since they are battery operated and with tight privacy constraints. Hence, also in this case, mitigating the required power to accomplish security tasks would be beneficial.

In the remaining part of this section we will survey the main results achieved in reducing and measuring the aforementioned energy costs.

4.1. Network security savings

At the network level, it is important to notice that, independently from the amount of malicious traffic, the “*bad packets*” have to be identified and discarded. Thus, the amount of energy needed for the traffic sanitization is an unavoidable cost and the savings due to aggressive analysis and early elimination of these packets is a net gain in terms of consumption.

An early model for the energy balance of the delivery process of a PDU in a network can be found in [28], while an extended version of the same model is defined in [14,12]. The model allows calculating the energy costs due to the routing of malicious PDUs to their destinations (as it is the case when identification of network attacks is delegated to the target itself) and, by comparison to the former, it also allows calculating the possible energy savings. Nevertheless, in [29,30] the effects of aggressive identification and discard of these malicious packets have been simulated to have some quantitative metrics. More specifically, in [29] the model is applied for the assessment of the energy cost of different intrusion detection approaches. Experimental results show that there is not an optimal strategy to preserve energy in IDSs, but, on the contrary, optimality of a strategy strongly depends on a set of network and security parameters such as: throughput, actual percentage of malicious PDUs, and availability of energy for their inspection. Therefore, the paper suggests to periodically change the IDS strategy according to the actual network state, in order to improve the energy efficiency of IDSs.

On the other hand, in [30] the attention is focused on a set of network parameters contributing to the global consumption of the network, like the average throughput, the percentage of unwanted PDUs and the underlying routing strategies. In detail, the paper experimentally assesses the impact of each parameter on the global energy saving, pointing out the set of the most important ones to take into account when evaluating an IDS strategy switch. From a general point of view, [30] demonstrates that the aggressive behavior may lead to significant energy savings. However, current literature suffers from some limitations: (i) none of the above works analyze the impact of the technique on the latency of PDUs, (ii) no works establish a clear and direct relation between the possibility of saving energy and the additional costs in terms of delays and jitters. Thus, as a part of future research, we argue that a model capable of taking into account not only the energy aspects, but also the Quality of Service (QoS) is needed to make this kind of techniques deployable in a real, carrier-grade network environment.

4.2. Mobile security savings

The energy consumption of security mechanisms in mobile devices has started to be considered an issue from the advent of PalmOS-enabled devices. The rise of the early Personal Digital Assistant (PDA) leads to the implementation of cryptographic libraries to encrypt local storage and support Transport Layer Security (TLS) and the Secure Socket Layer (SSL). To this aim, in [31] the implementation of native cryptographic functions in PalmOS has been extensively tested. Experimental results show that there are relevant differences in terms of resource consumption among block ciphers (e.g., DES uses more than 4 times the resources used by AES). Similar considerations can be formulated for hash functions where MD5 results to be the more efficient method. All in all, this work has the merit to draw the attention on the potential impact of security on mobile, albeit it does not deal directly with energy consumption.

An early work that tries to relate the performance of mobile crypto libraries with the energy consumption is [32], where the impact of four block ciphers (i.e., RC2, AES, XTEA and Blowfish) on the batteries of three PDAs is discussed. The empirical assessment shows that they consume the same amount of energy in a given period of time. For this reason, authors conclude that faster algorithms necessary lead to save more energy than slower ones.

A similar study has been carried out recently on the Bouncy Castle crypto Application Programming Interface (API) [33]. In this work, authors empirically evaluate the energy consumption of symmetric and asymmetric crypto algorithms, confirming the results of [32]. Furthermore, authors propose a trade-off model between the crypto API throughput and the energy saving. Other optimizations of mentioned Bouncy Castle crypto library have been described in [34].

In [35], the energy cost of watermarking algorithms on mobile is discussed. In more detail, the paper empirically analyzes the energy consumption required by the state-of-the-art algorithms and concludes that they are too energy-hungry in their original form for mobile devices. Hence, authors propose a solution based on an external proxy to mitigate the impact of watermarking on the energy consumption, by moving most of the computational effort on the proxy server itself.

Beyond cryptography, other studies focus on analyzing the energy impact of security protocols on mobile. For instance, in [36] using the Circuit Switched Domain instead of the Packet Switched Domain for secure video communication is tested and results in lower energy costs because of reduced keep-alive activity. In [37] an empirical study on the energy costs of TLS protocol on 3G and Wi-Fi is discussed. Surprisingly, the experimental results show that the consumption related to the I/O operations during the handshake and the record protocol greatly overcomes the cost of cryptographic API used to cipher the transmitted PDUs. Previous work shows that basic security mechanisms have a strong impact on the consumption of the mobile device but it lacks in providing an intuition on the energy consumption of a mobile application as a whole. Instead, a global picture is provided in [38] where the energy costs to secure video communications on handheld devices is discussed. Authors show that the energy impact can be very high and they propose a set of tradeoffs between video quality and security that can be taken into account. Since most of the power needed to secure the video is due to the encoding and decoding algorithms, similar considerations may hold for current smartphones and modern mobile OSes, albeit a complete assessment is still missing.

5. Wireless sensor networks

The impact of security on energy-saving/consumption and vice versa has been a very hot topic in research on WSN for years. The intrinsically limited energy sources available to sensors makes them an ideal target for battery drain attacks. In fact, it may force the shutdown of one or more node, cripple the WSN communication capabilities, require additional power to be spent in communication activities by other nodes and finally escalate into a significant reduction of the life-span of the whole deployment. This makes the whole WSN critically dependent from power consumption levels of every single node. At the same time, the prominent features of WSN, i.e., their distributedness, wirelessness and openness, make them easier targets for several kinds of security attacks as it has been portrayed in [39].

A first type of energy draining attack is described in [40], and it is called *denial-of-sleep*. It leverages the fact that a node in a WSN tries to spend as much time as possible in a power-saving mode (called a sleep mode) in order to prolong its life-span. However, a node may be forced to get out of the power-save mode by a malicious node in a sleep-deprivation attack that reduces the life-span of the nodes in terms of orders of magnitude. In [40], the authors first analyze different kinds of MAC implementations specific for WSN. More in detail, the implementation analyzed are Sensor MAC, Timeout MAC, Berkeley MAC, and Gateway MAC. Then, they evaluate the vulnerability to denial-of-sleep attacks of these implementations and show that, because of the fact that they try to concentrate communication in limited periods, they are generally vulnerable to rogue nodes maliciously injecting de-synchronizing traffic. Furthermore, the authors define a “subtle” attack as one that does not encroach the normal traffic of the WSN and thus is not easily detected. Through its comprehensive analysis with different level of knowledge of the network (i.e., from no knowledge to trust of other nodes), the authors show that a rogue node that has penetrated the network may keep the WSN awake all the time and drain their energy two order of magnitude faster than expected. The authors conclude that to become resilient to denial-of-sleep attacks, a WSN needs to implement link-layer authentication since application-layer security is ineffective against this threat. The authors in [41] acknowledge the importance and inherent threat posed by denial-of-sleep attacks, but they perform an analysis of proposed solutions and suggest that authentication mechanisms are themselves too expensive in terms of energy to provide an efficient protection. Instead, they introduce a cross-layer approach that leverages routing and, more in general, network-layer information to secure the nodes from link-layer attacks. The general idea can be summarized as (i) checking routing tables and disregard messages from nodes that are not neighbors and (ii) checking perceived transmission power to identify replay attacks. These mechanisms are tested on nodes implementing the S-MAC protocol and show a very good level of resilience to many denial-of-sleep attack, in fact simulation shows that they double the life-span of nodes subject to denial-of-sleep attack in comparison to nodes using plain, unsecured S-MAC protocol. Nonetheless, the proposed solution is not capable of protecting neighbors from the action of a compromised node, and the lack of authentication leaves the WSN prone to attacks from rogue nodes that act cooperatively as good nodes at the time of topology discovery and routing tables creation.

The authors in [42] tackle the problem of protecting routing tables from malicious tampering. Indeed, routing table tampering is a significant threat in WSN, even if cross-layer solutions such as the ones described in [41] are adopted, and may lead to total disruption of the functional capabilities of the WSN as a whole. The authors claim to be able to guarantee secure routing using only symmetric cryptography and they also claim that it is not necessary for every node to know the key of every other node. However, to achieve that result they assume a topology discovery process performed according to the process described in [43], that can be completed with no interference. Thus their results are valid if and only if no malicious node was present at the time of the topology discovery process and thus no rogue node has had the capability to infiltrate the topology on top of which routing is built. Furthermore, pre-loaded keys are generally vulnerable to node capture.

In [44] the authors describe a set of attacks targeted at the routing algorithms used in WSN. They define these attacks “Vampire Attacks” as they do not directly disrupt the network working but they inexorably drain resources until they obtain a full shutdown. Furthermore, they use the term to identify a characteristic of this kind of attack that authors in [40] called

“subtlety”, i.e., the capability to mount the attack while using only behaviors that are legitimate according to the protocol rules. The actual definition provided by the authors is as such: an attack that construes a mutation of a legitimate packet that forces the network into consuming more energy than the original, benign version of the same message would have required. A very important implication of this definition is the fact that the source of a “Vampire Attack” must be a full fledged insider, an entity that is trusted and has the same knowledge of the network that legitimate nodes have.

The authors distinguish between attacks to source-routing based protocols and to packet-forwarding based protocols. In the first case, they suggest as a mitigation measure to have intermediate nodes check if the source-defined route is optimal. Yet, this completely negates the usefulness of source routing as all the intermediate nodes need to perform a routing decision to hunt for vampires. In the second case, the authors suggest to enhance the routing protocols with check of progress toward the destination at each hop, this would allow dropping mis-routed packet and, eventually, identify the vampires.

The authors in [45] evaluate on the StrongARM platform the different schemes for establishing cryptographically secured channel in terms of energy expenditures. They start with a taxonomy of key distribution mechanisms and they actually evaluate the energy costs of a lightweight variant of Kerberos and of the Elliptic Curve Menezes–Qu–Vanstone (ECMQV) protocol, an Elliptic Curve Diffie–Hellman scheme. They find that, contrarily to the experience of early 2000 studies, the energy cost of asymmetric cryptography, mainly because of the enormous progress that has been made in the efficient implementation of elliptic curve cryptography, is not orders of magnitude higher than the one of symmetric cryptography. Furthermore, even if the base cost of the Kerberos scheme is still lower, the scalability characteristics of ECMQV make it strongly preferable and more energy-efficient in large WSN.

In [46] the authors compare the energy costs of two public key schemes, namely Elliptic Curve Cryptography (ECC) and RSA. The evaluation is done on a simpler and less performing platform than the one adopted in the previous study, namely a platform based on the Atmel ATmega128L 8-bit micro-controller. Once again, their experiments indicate that recent implementations of the elliptic curve cryptography have a high level of efficiency and may be viable even on severely constrained platforms such as one based on 8-bit micro-controllers. Then, the authors evaluate what is the energy impact of exchanging keys using asymmetric cryptography compared with the costs of communication in a real-world WSN scenario. They conclude that if the key can be used for exchanging 64KB of data, the cost of the initial key exchange contributes only for 1/50 of the global communication (both key exchange and the following message exchange) energy expenditure. Obviously, a larger life-span of the key could lead to an even smaller fraction, but it reduces the level of security.

All in all, the authors of both [45,46] infer that the recent progresses in the efficient implementation of ECC make it a viable solution to authentication problems in WSN.

As a final remark, we highlight that while energy-drain attacks are not limited to WSN but are, on the contrary, a first-class threat for mobile devices in general, many of the threats and solution devised for WSN (e.g. threats related to routing algorithms or attack targeted at the MAC layer) are specific of WSN and do not simply translate into viable attacks for smartphones. Nonetheless, many of the concepts and ideas devised and tested in the WSN field may be adopted as the source from which both new solutions and new threats specific for the field of mobile devices may be derived.

6. Energy as an asset

As discussed, reducing the consumption of security is of primary importance. In this section, we consider energy as an asset to protect and constantly measure. This leads to: (i) preventing attacks aiming at depleting power of devices and (ii) using the energetic behavior as an indicator to monitor possible malicious activities.

6.1. Energy as an asset to be protected

While the importance of protecting nodes from energy drain attacks has been a hot topic in WSN for quite a while, energy drain attacks in mobile devices are a rather lightly trodden path. Even if the concept that an energy-drain attack equals to a denial-of-device attack is not new, most of the work dealing with mobile security concerns privacy and information stealing. The emphasis on the importance of availability for mobile devices, however, is rapidly growing, fueled by the explosive increase in their market share and daily usage.

In [47] the authors put the identity between battery-drain and denial-of-device as the foundation of their study. Then, they describe three different methodologies to perform an energy-drain attack targeting a mobile device. More in detail, they distinguish between a *service request power attack*, a *benign power attack*, and a *malignant power attack*.

The first typology of attack includes all the situations in which repeated requests of a legitimate service request keep the device out of power save state, as such, they represent a variation of the *denial-of-sleep* attack described in Section 5. At first glance, a personal mobile device might appear as an unlikely target for a “service request”, but, it is important to notice, though, that the type of applications typically running on a personal mobile device change the way in which a “service request” has to be envisioned. While it will be rather absurd (at least at present) to imagine a smartphone hosting a website, it is to be intended as a request for service an event such as the delivery of a notification from an OSN.

The second typology of attack includes all the situations in which a mobile device is forced into repeatedly performing a legitimate but intrinsically energy hungry activity. This type of attack does not need to introduce any additional software into the attacked device, it just leverages legitimate, already installed software making it execute a pathological number of times the normal activity.

The third typology describes a case in which a mobile device is forced into repeatedly executing a piece of code that has been maliciously hacked with the goal to make it more energy hungry than the original version. It is obvious that it requires penetrating the device to make a specific piece of malicious software executable from the inside. Yet, it is very important to notice that this requirement does not equate this attack to any other traditional virus, worm or trojan; in fact, all the security mechanisms currently adopted (e.g., static and dynamic analysis of app uploaded to app markets, anti-virus softwares, etc.) do not consider the energy costs of activity and they only hunt for more traditional security threats such as information stealing. Thus, an application containing a *malignant power attack* could easily slip through the current generation of security mechanisms and end into a large number of mobile devices undisturbed.

As a possible remedy, the authors in [47] suggest a *Power Secure Architecture*, i.e., an architecture capable of guaranteeing that the battery life will be no less than a given fraction of the expected value for normal use even in the presence of energy drain attacks. A first characteristic is its capability to enforce an authentication before investing a significant amount of energy into serving a request. Alas, this is rather unrealistic and provides very little protection, in fact the authentication itself could be exploited as the service to be attacked. The second characteristic of the architecture is its capability to profile the energy consumption of normal execution of activities and to monitor the current energy expenditure in order to spot both benign and malignant power attacks.

The eDoctor tool described in [48] is dedicated to the identification of Anomalous Battery Drain (ABD), which is not a form of attack, at least in the canonical sense. For instance, an ABD may be easily caused by buggy software. Yet, eDoctor may be considered a significant security tool because it is capable to identify with a high rate of success (94% as stated by the authors) the culprit of an ABD. The methodology adopted to evaluate the applications is described in Section 7, once the applications have been divided in phases according to their resource usage, eDoctor associates those phases to the battery consumption measurements provided by the operating system to associate a significant change in app behavior to what they call a *Suspicious New Phase*. The main limitations of eDoctor as a security tool are: (i) alarms are only triggered by changes in the power behavior, and (ii) the time scale of eDoctor is measured in several recharge cycle (one week) thus it can be used mainly as a post-mortem tool to identify an ABD.

The authors in [49] describe a battery-drain attack that can be mounted by exploiting a security hole in the Packet Data Protocol (PDP) context, the point of inter-operation between cellular networks and the Internet. More in detail, the authors show that the mechanism for Multimedia Messaging Service (MMS) delivery and the PDP context retention contain several security holes due to the fact that the architecture was devised to only deal with heavily protected infrastructure nodes (such as the ones in voice networks) while MMS traffic travel over the public Internet. We point out that this is a mobile-phone oriented version of the *denial-of-sleep* attack described in Section 5, since it makes possible to keep a handset in a power-hungry data-exchange-ready state. Also this vulnerability allows building hit-lists to attack several devices at the same time. Its main weakness is the dependency on the MMS delivery network, which is becoming a legacy service in many countries. Furthermore, the authors clearly identify a battery drain attack as the one with the most convenient (from the attacker point of view) ratio between damage dealt and likelihood of early discovery. Finally, to mitigate its dangerousness, the authors propose some changes to the MMS delivery. It is important to notice, though, that while the authors fully acknowledge the level of danger posed by an energy-drain attack, they are not capable of suggesting any form of mitigation active on the terminal and they rely only on removal of attack surfaces at network level. Another possible option to securely use legacy services is presented in [50], where authors do present a power efficient architecture to securely send encrypted data within a burst of SMS. Despite the contribution in the design of a novel service, the main point is the adoption of “energy-aware profiles” to optimally select compression algorithms, as to avoid excessive power depletions.

The authors in [51] describe what, according to [47] is a *benign power attack*. They propose to build a legitimate Web-page containing a multimedia content capable of putting a heavy burden on the multimedia subsystem of the device. Leveraging the new HTML5 tags, it is possible to specify the most energy inefficient codec available on the platform and to keep the multimedia content from showing explicitly (e.g., specifying a 0x0 display size for a video) to avoid being caught by the user. The authors compare several audio and video codec available on the Android platform and measure the energy consumption they extol. The attack is extremely difficult to detect as it does not represent any form of intrusion as a traditional security system may envision it. Only a next-generation energy-aware security system such as the ones described in [52] may detect such an attack. Although the extensive comparison performed by the authors provides a novel way to evaluate the efficiency of the attack-vector, the study in [51] has two drawbacks: (i) the tool adopted for the measurements of consumption is PowerTutor [53], which is not accurate enough [54]; (ii) authors do not describe how it would be possible to guarantee that the victim will stay on the Web-page for a period of time long enough to induce a significant battery drain.

As a concluding remark, we may say that the fact that energy is an important asset that needs to be defended has already reached a significant level of recognition in the field of mobile security. However, the continuous and very fast evolution of mobile devices has not allowed the formulation of any kind of stable and general purpose solution.

6.2. Energy as an asset to ease detection

We reviewed the work that shows how energy is a major asset in mobile devices and may be the target for very dangerous attacks, here we consider energy as an asset to be leveraged to ease detection. More in detail, we use energy consumption as a bio-marker capable of discriminating among legitimate and malicious activities. This concept is still far from reaching full maturity, in fact very few works have tried to classify malicious behaviors in Android in terms of their energetic footprints.

A first attempt at defining a Battery-Based Intrusion Detection System is described in [55]. The authors acknowledge the high level of danger that battery drain attack pose to mobile devices and propose to use energy consumption monitoring techniques to try achieving an early detection of this kind of threats. They also advocate the need for a Host Intrusion Detection Engine (HIDE) because the widespread diffusion of wireless networks makes traditional network security choke-points ineffective. To achieve their goal, they devise a hybrid combination of traditional intrusion detection techniques that are triggered when energy-consumption monitoring detects an unexpected energy consumption level. Also, they compare the energy consumed by the HIDE system with the one saved by it and they, rather obviously, conclude that security is not free and while a situation in which no attack has taken place makes HIDE only a loss, the amount of power saved by detecting four different attacks is larger than the one consumed by the security system.

Another attempt to enhance threat detection by means of energy consumption measurements is described in [56]. The authors describe what they define a Battery-Sensing Intrusion Prevention System (B-SIPS), that is, as the authors say, a “non-conventional” intrusion detection system capable of detecting threats that are not visible to standard anti-malware systems. They focus on network-centric groups of mobile devices and on attacks adopting as a vector either IEEE 802.11 (Wi-Fi) or IEEE 802.15.1 (Bluetooth). The contribution that differentiates this work from the others in this group is the fact that the mobile devices on top of which the B-SIPS is running are not considered as stand-alone devices to be defended, but they are, instead, the sensors of a distributed intrusion detection system dedicated to the discovery of attacks taking place in the network the nodes are inserted into. They call this system *Canary-Net* [57]. The authors show that, adopting a Dynamic Threshold Calculation to devise the expected current delivered by the battery and comparing it with the actual sampled value, the sensors grouped into the *Canary-Net* system allow identifying flooding and DoS attacks. The authors also provide one of the earliest definition of *Energy Consumption Signature* both with regard to attacks and with regard to normal activities as they are used in Dynamic Threshold Calculation.

Even if these works are still in early stage and require further development to provide fully conclusive results, their finding clearly show that it is possible both to adopt energy consumption as a parameter to detect anomalies and to devise *Energy Consumption Signatures*. Obviously, the rapid growth in the capability of mobile devices that has taken place in the recent years makes the generation of *Energy Consumption Signatures* a task of growing complexity, especially in terms of general analytical models [58]. Nonetheless, as we will analyze in the next section the tools available for measuring energy consumption have experienced a significant evolution too.

7. Measurement tools

To effectively profile the energy consumption of devices, the power drained by each hardware component (e.g., CPU, GPS and air interfaces) must be quantified with a sufficient precision. In this sense, the reference literature already provides different viable options, even if with different degrees of granularity. To the best of our knowledge, a standard classification of the various approaches has never been proposed, thus, we introduce the following taxonomy:

- *probe source*: measurements can be collected using internal hardware (e.g., relying on the onboard device instrumentation) or external (e.g., ad-hoc hardware connected to the device or added to it). Internal measurements are generally less precise than external ones. Yet, external hardware severely reduces the usability of the device; for this reason they can be used only for laboratory trials but not in everyday use;
- *invasiveness of measurement*: methods can get information provided by different layers in the OS stack. For instance, information on energy consumption can be obtained from the application (high level) by invoking a proper API, or by querying directly the device driver handling the battery or the Linux kernel (low level). As a consequence, high-level measurements have a *low invasiveness* and are more coarse-grained, less precise and often estimated, yet they do not require a strong customization of the mobile OS. On the other hand, low-level measurements have a *high invasiveness* and require proper modifications within the device driver or the kernel, but provide more reliable and precise consumption values;
- *processing of collected data*: collected data can be processed *on-device*, i.e., directly on the device, or delivered to an external server (*off-device*) for offline analysis. On-device analysis is performed by specific applications (e.g., an energy-saving daemon) and does not generally overtake the boundary of the single device. External servers often perform off-device analysis by collecting data from several devices.

We point out that the proposed taxonomy is well suited to describe the current state-of-the-art implementation of tools used to measure energy consumption in smartphones. However, it is quite impossible to find a model falling uniquely in one class. For this reason Table 2 precisely classifies tools and approaches according to the defined metrics.

In more detail, an early energy measurement approach is proposed in [59], where authors empirically evaluate if it is possible to predict the discharge curve of the battery, according to the load generated by running programs. More specifically, authors define four benchmarks (i.e., IReg, IMem, FReg and FPMem), each one suited for a particular kind of program instruction (i.e., integer or floating point mathematic and load/store operations). Benchmarks results are then combined to predict the discharge curve caused by a specific application.

In [60] an approach to profile activities on Symbian phones for anomaly detection purposes is proposed. Albeit it does not directly deal with energy consumption, the set of features considered (e.g., CPU usage, user inactivity, etc.) can be indirectly related to the energy consumed by the device as a whole. Specifically, this method can recognize deviations from the normal

Table 2

Measurement tools surveyed in this work and its classification according to the used functional taxonomy.

Name/reference	Probing	Invasiveness	Usage of data
IReg, IMem, FPRReg, FPMem/[59]	Int.	Low	On-device
E61 Monitoring Client/[60]	Int.	High	Off-device
TailEnde/[61]	Int.	Low	On-device
Carrol and Heiser/[62]	Ext.	High	On-device
Rice and Hay/[63]	Ext.	Low	Off-device
PowerTutor/[64]	Int.	Low	On and off-device
Xiao, et al./[65]	Int.	Low	On-device
Sesame/[66]	Int.	Low	On-device
AppScope/[67]	Int.	High	On-device
eLens/[68]	Ext.	Low	Off-device
MPower/[69]	Int.	Low	Off-device
eDoctor/[48]	Int.	High	On-device
Curti, et al./[52]	Int.	High	On-device
Merlo, et al./[54]	Int.	Low	On-device

usage during the execution of malware. Due to its high precision and the limitations of mid-2000s mobile hardware, the analysis has been executed by an external server running an anomaly-based IDS.

In [61], authors propose a methodology to measure the power drained by 2G and 3G communication protocols, noticing that there is a relevant waste of energy after the completion of a data transfer phase. As a workaround, the same authors propose TailEnde, which reduces the waste of energy at the expenses of increased delays, even if bounded. The performance evaluation has been done on a Nokia device, using the embedded Nokia measurement tool (NEP) (i.e., without any modification of the underlying OS nor any use of external HW) and analyzed onboard. While TailEnde is limited to 3G and IEEE 802.11, Ref. [62] offers a complete low-level profiling of energy consumption of a smartphone in its entirety. The proposed methodology is precise but very invasive, since it measures the current by injecting sense resistors in the rails of each component. Albeit this approach is hardly portable on different hardware, it provides an important contribution to understand the consumption ratio between the different smartphone components.

A different approach to low-level measurement is proposed in [63]. Here, authors provide a method to build fine-grained energy traces of power consumption in Android smartphones by using external hardware placed between the phone and the battery. The proposed methodology is empirically evaluated by profiling two handsets connected to the smartphone. The main result is to show how implementation choices made by developers may impact the global energy consumption in a very pronounced manner.

PowerTutor [64] is an Android application performing an estimation of the actual consumption of the device. The key idea is to measure well-accessible values (e.g., the bytes sent by the air interfaces) to feed a quasi real-time model performing an estimation, primarily by using the breakdown introduced in [52]. Since it has been used in many research papers as well as a basis for a new-wave of tools, it will be discussed in detail. PowerTutor adopts a simple energy model for each considered hardware component. Besides, the power drained by the device screen is estimated as a constant base consumption summed to a value linearly multiplied by the brightness level of the screen. This may provide rather accurate results in the case of LCD screens, but it is not adequate for AMOLED technology where, as clearly shown in [70,71] the consumption depends on the colors displayed. In fact, while a totally dark LCD screen is obtained by masking the backlighting, a dark AMOLED screen actually avoids emitting light. In the case of the audio device, the consumption is simply an on–off value with no dependency on the actual amplifier level. To model the power consumption of the CPU, PowerTutor assumes a linear relation between its utilization level and the used clock frequency. Alas, this introduces a large estimation error since: (i) it does not consider the hysteresis present in modern CPU schedulers, and (ii) it uses only the most expensive power state (C0). However, this latter factor has a minor impact on the accuracy since the profiling daemon of PowerTutor prevents the CPU switching to deeper power saving state. As regards the IEEE 802.11 interface, PowerTutor considers the channel speed, the data rate of the uplink and the number of PDUs sent in a second. Hence, such parameters are combined to obtain a linear interpolation of minimum/maximum power consumption bounds. A similar approach is done for the 3G, but in a more refined manner. In fact, the tools also considers the presence/absence of connectivity, its type (UMTS or HSDPA), its state (idle, fch and dch), and the number of bytes transmitted. Lastly, the GPS is modeled by using a simple three-state model, i.e., considering off, on and sleep.

As it can be noticed, PowerTutor uses high-level data, thus being a low-invasive tool. Alas, this leads to particularly coarse-grained measurements [52], thus preventing its use to study (or detect) security-related aspects having a reduced energy footprint. A tool similar to PowerTutor is presented in [65] but it considers also I/O operations, the Wi-Fi downlink rate and the IEEE 802.11 power saving mode for a more precise estimation. Besides, [62,63] exploit the same philosophy even if using more detailed breakdowns.

Sesame [66] proposes the usage of mobile devices to perform self-modeling to automatically generate own consumption profiles. This task is done by collecting data at low level (i.e., directly from the device driver of the battery) and by means of on-device analysis. To achieve a good level of accuracy, it is necessary to calibrate the models. Besides, the paper also

describes some techniques to reduce errors due to the Coulomb counter embedded within batteries of many popular devices.

The AppScope tool [67] provides detailed low-level energy consumption measurements. Unfortunately, it works only on the Google Nexus One, and its closed-source nature prevents evaluating the correctness of the measurements.

A completely different approach is offered by eLens [68]. This tool analyzes how the applications has been developed, rather than its behavior while running. Thus, it used a code-level estimation of the energy that will be consumed by at runtime. Also, it annotates the source code with “consumption tags”, providing the developers guidelines to optimize their code. The performance evaluation provided by the authors demonstrate the effectiveness of the tool.

Many of the discussed solutions have been designed from a green computing perspective rather than from an energy-aware security one, thus they are useful to evaluate energy drains but cannot be used to recognize malicious activities from their energy footprints. An earlier proposal dealing also with security aspects, is MPower [69]. In more detail, it profiles the normal usage of the device and rise a warning in case of the energy consumption deviates from an expected behavior. The main drawback of the approach concerns the usage of an external server centralizing the detection.

eDoctor [48] is a tool dedicated to the detection of ABD, and it is based on high level measurements, performed without external hardware and evaluated on-device. Its main contribution is to use “phases”, i.e., clustered execution intervals according to used hardware resources. Therefore, phases can be leveraged to identify the vector of both benign and malignant power attacks as described in Section 6.

More recently, the sensitivity toward energy aspects of security has stimulated the idea of using energy footprints for the detection of malware [52]. Alas, the main issues it to have correct “energy signatures” both of licit and malware applications. In this vein, the work proposed in [52] is promising but very invasive (low-level) and hardly portable. An alternative is proposed in [54] where the reliability provided in [52] is coupled with a less invasive measurement approach granting portability. Both solutions still require a proper validation on a significant number of malware and devices and are limited to WiFi profiling only. We argue that a future extension of these works should focus on profiling GSM/3G energy consumption to detect *zombie* devices inadvertently driven by malware to carry out *denial-of-service* attacks to the cellular infrastructure (e.g. [72,73]).

To conclude, two additional remarks could be made. Firstly, the very energy cost of the measurements themselves has to be taken into account. Secondly, offline measurements are not functional as security support, since the collection of data may be denied by the attack itself.

8. Conclusions and future directions

Energy awareness and security are two hot topics in several fields of research. However, the notion that they need to be taken into account simultaneously has only recently become a standpoint for further research. In this paper we surveyed the most recent work dedicated to the merging of energy-awareness and security aspects into a seamless research fabric. As a preliminary step, we introduced the most relevant techniques used for “greening” purposes both in computing and in networking. Then, we reviewed studies aiming at the minimization of the energy footprint of security mechanisms and we analyzed how energy awareness and security have been a major concern in the field of WSNs for years. With such a basis, we also analyzed the recent, but increasingly growing, trend that explicitly considers energy as an asset to be protected from targeted attacks instead of considering energy consumption merely as a by-product of attacks targeted to different system's assets. Symmetrically, we then reviewed a number of papers that suggest leveraging energy consumption measurements to ease the detection of attacks even in situation where traditional threat sensors fail to deliver any alarm. Finally, we analyzed the evolution of energy consumption measurements tools that can be used in all the above described scenarios.

On the basis of our analysis, the major lessons learned are:

- an important topic to be addressed by academic and developers concerns the optimization of algorithms for cryptography used by mobile devices. In fact, recent developments in the field of WSN security show that Elliptic Curve Cryptography (ECC) has a very low energy footprint and might thus be adopted in situations where more energetically expensive crypto-security solutions were out of range. Furthermore, the experimental evidence is that the reduced energy footprint of ECC is due to reduced computational requirements, thus it is not tied to any specific computing architecture and will hold in general;
- to increase the effectiveness of security frameworks a proper kind of energetic scalability must be introduced. In this vein, part of the ongoing research dealing with energy-aware software is also starting to consider the trade-off between the level of security and the consumption of related mechanisms;
- at present, there is not any model able to predict if and how the performance degradation due to the implementation of energy-efficient strategies (e.g., the introduction of additional delays or the relaxation of the constraints on QoS) could impact security mechanisms. To deal with this problem, the resilience of security mechanisms to any form of energy-related performance degradation should be proved. Symmetrically, the effect of security measures on the down-scaling of the amount of unwanted traffic has been studied in terms of energy-savings only in an extremely limited number of cases;
- as a consequence of their nature (constrained both in computational and in energy resources) WSNs have been the archetypal field where security and energy efficiency are jointly studied. Alas, many of the reference literature cannot be

easily ported to the more popular smartphone case, this is due mainly to the rapid growing gap in terms of computational power between sensor nodes and smartphones and to the adoption in WSNs of special purpose networking stacks instead of the standard Internet Suite. However, many ideas concerning their architectural blueprint can be borrowed and properly adapted to protect wireless networks or IoT nodes or mobile appliances with limited capabilities;

- the development of precise tools to measure energy is quite an active research field; however, the closed-source nature of many devices/OS has the effect to concentrate the efforts almost exclusively on the Android platform; furthermore, it is important to notice that, while many tools achieve a level of precision that is reasonable if applied to the problem of warning users that they are burning their batteries too fast, the problem of detecting malware and threats needs a much higher level of precision;
- energy draining attacks have already captured some attention from the research community. Yet, their thorough understanding, especially the one of the instances targeting large-scale deployments, is still incomplete as most work in this topic focus on targeting a single device.

At the same time, the survey described in this paper allowed us to identify some very innovative trends for future research. Among these we want to cite:

- investigating the use of energy as a metric to detect hazards, worms and threats in general. For instance, this can be the case of data exfiltration attacks using steganography, which leaks data in such a slow manner as to stay hidden from traditional threats detection software. In this sense, some proposals are emerging, albeit the possibility to detect attacks in terms of their energy footprint is still a work-in-progress.
- studying, designing and implementing a new-generation of devices and protocols able to scale their security requirements according to the power availability and vice versa;
- optimize security algorithms and mechanism by exploiting all the techniques already available from green networking and computing (for instance device offloading). This process should start with a through re-thinking of security protocols with energy-awareness as a rule of thumb;
- in the specific case of large-scale networks, where energy consumption is magnified by scale factor, an important research topic concerns the early detection of security risks. In fact, preventing security issues or promptly dropping unwanted traffic (e.g., malware signaling) would lead to relevant energy savings;
- the engineering of future mobile devices, which will have their end-to-end transparency restored by IPv6, should always take into account energy as an asset to protect from the very start. This process should work the same way as it works today in the case of data;
- the recent developments in the mobile operating systems (e.g. Android) have made available novel solutions to the problem of energy consumption measurements. Hence, a study of the trade-off between the precision of measurement and the invasiveness of the approach needs to be further investigated to improve both the reliability of energy footprints and the energetic costs of measurements themselves.

To conclude, we may state that the field of study of energy-aware security mechanisms has seen many recent developments, but is still far from full maturity. However, the increasing importance of both security and energy awareness are making it more and more critical and will surely boost its future development.

References

- [1] M. Gupta, S. Singh, Greening of the internet, in: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '03, ACM, New York, NY, USA, 2003, pp. 19–26. <http://dx.doi.org/10.1145/863955.863959>.
- [2] A. Sinha, A. Chandrakasan, Energy aware software, in: Thirteenth International Conference on VLSI Design, 2000, 2000, pp. 50–55. <http://dx.doi.org/10.1109/ICVD.2000.812584>.
- [3] S. Ricciardi, D. Careglio, G. Santos-Boada, J. Solé-Pareta, U. Fiore, F. Palmieri, Saving energy in data center infrastructures, in: 2011 First International Conference on Data Compression, Communications and Processing (CCP), 2011, pp. 265–270. <http://dx.doi.org/10.1109/CCP.2011.9>.
- [4] L. Feeney, M. Nilsson, Investigating the energy consumption of a wireless network interface in an ad hoc networking environment, in: Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings, Vol. 3, INFOCOM 2001, IEEE, 2001, pp. 1548–1557. <http://dx.doi.org/10.1109/INFCOM.2001.916651>.
- [5] S. Ricciardi, F. Palmieri, U. Fiore, D. Careglio, G. Santos-Boada, J. Solé-Pareta, An energy-aware dynamic {RWA} framework for next-generation wavelength-routed networks, *Comput. Netw.* 56 (10) (2012) 2420–2442. <http://dx.doi.org/10.1016/j.comnet.2012.03.016>. Green communication networks. URL <http://www.sciencedirect.com/science/article/pii/S1389128612001156>.
- [6] L. Cavaglione, Can satellites face trends? the case of web 2.0, in: International Workshop on Satellite and Space Communications, 2009, IWSSC 2009, 2009, pp. 446–450. <http://dx.doi.org/10.1109/IWSSC.2009.5286305>.
- [7] R. Bolla, R. Bruschi, F. Davoli, F. Cucchietti, Energy efficiency in the future internet: A survey of existing approaches and trends in energy-aware fixed network infrastructures, *IEEE Commun. Surv. Tutor.* 13 (2) (2011) 223–244. <http://dx.doi.org/10.1109/SURV.2011.071410.00073>.
- [8] A. Bianzino, C. Chaudet, D. Rossi, J. Rougier, A survey of green networking research, *IEEE Commun. Surv. Tutor.* 14 (1) (2012) 3–20. <http://dx.doi.org/10.1109/SURV.2011.113010.00106>.
- [9] Q. Li, M. Zhou, The survey and future evolution of green computing, in: 2011 IEEE/ACM International Conference on Green Computing and Communications (GreenCom), 2011, pp. 230–233. <http://dx.doi.org/10.1109/GreenCom.2011.47>.
- [10] F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco, A. Castiglione, Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures, *J. Supercomput.* (2013) 1–22.
- [11] J. Wang, L. Feng, W. Xue, Z. Song, A survey on energy-efficient data management, *SIGMOD Rec.* 40 (2) (2011) 17–23. <http://dx.doi.org/10.1145/2034863.2034867>.
- [12] L. Cavaglione, A. Merlo, The energy impact of security mechanisms in modern mobile devices, *Netw. Secur.* 2012 (2) (2012) 11–14. [http://dx.doi.org/10.1016/S1353-4858\(12\)70015-6](http://dx.doi.org/10.1016/S1353-4858(12)70015-6).

- [13] M. Migliardi, A. Merlo, L. Caviglione, A survey of green, energy-aware security and some of its recent development in networking and mobile computing, in: Proc. of the 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2014, pp. 297–304.
- [14] L. Caviglione, A. Merlo, M. Migliardi, What is green security?, in: 2011 7th International Conference on Information Assurance and Security (IAS), 2011, pp. 366–371. <http://dx.doi.org/10.1109/ISIAS.2011.6122781>.
- [15] N. Balasubramanian, A. Balasubramanian, A. Venkataramani, Energy consumption in mobile phones: a measurement study and implications for network applications, in: Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference, ACM, 2009, pp. 280–293.
- [16] L. Caviglione, M. Coccoli, Privacy problems with web 2.0, *Comput. Fraud Secur.* 2011 (10) (2011) 16–19.
- [17] N. Vallina-Rodriguez, J. Crowcroft, Energy management techniques in modern mobile handsets, *IEEE Commun. Surv. Tutor.* 15 (1) (2013) 179–198. <http://dx.doi.org/10.1109/SURV.2012.021312.00045>.
- [18] N. Kim, T. Austin, D. Baauw, T. Mudge, K. Flautner, J. Hu, M. Irwin, M. Kandemir, V. Narayanan, Leakage current: Moore's law meets static power, *Computer* 36 (12) (2003) 68–75. <http://dx.doi.org/10.1109/MC.2003.1250885>.
- [19] H. Kim, N. Agrawal, C. Ungureanu, Revisiting storage for smartphones, *Trans. Storage* 8 (4) (2012) 14:1–14:25. <http://dx.doi.org/10.1145/2385603.2385607>.
- [20] N. Vallina-Rodriguez, J. Crowcroft, Erdos: Achieving energy savings in mobile os, in: Proceedings of the Sixth International Workshop on MobiArch, MobiArch '11, ACM, New York, NY, USA, 2011, pp. 37–42. <http://dx.doi.org/10.1145/1999916.1999926>.
- [21] S.-L. Tsao, C.-H. Huang, A survey of energy efficient {MAC} protocols for [IEEE] 802.11 {WLAN}, *Comput. Commun.* 34 (1) (2011) 54–67. <http://dx.doi.org/10.1016/j.comcom.2010.09.008>.
- [22] K. Kumar, Y.-H. Lu, Cloud computing for mobile users: Can offloading computation save energy? *Computer* 43 (4) (2010) 51–56. <http://dx.doi.org/10.1109/MC.2010.98>.
- [23] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, F. Jahanian, Virtualized in-cloud security services for mobile devices, in: Proceedings of the First Workshop on Virtualization in Mobile Computing, MobiVirt '08, ACM, New York, NY, USA, 2008, pp. 31–35. <http://dx.doi.org/10.1145/1622103.1629656>.
- [24] P. Gilbert, B.-G. Chun, L.P. Cox, J. Jung, Vision: Automated security validation of mobile apps at app markets, in: Proceedings of the Second International Workshop on Mobile Cloud Computing and Services, MCS '11, ACM, New York, NY, USA, 2011, pp. 21–26. <http://dx.doi.org/10.1145/1999732.1999740>.
- [25] L. Caviglione, C. Cervellera, Design of a peer-to-peer system for optimized content replication, *Comput. Commun.* 30 (16) (2007) 3107–3116. <http://dx.doi.org/10.1016/j.comcom.2007.05.041>.
- [26] X. Li, F. Chong, A case for energy-aware security mechanisms, in: 2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2013, pp. 1541–1546. <http://dx.doi.org/10.1109/WAINA.2013.5>.
- [27] L.A. Barroso, U. Hölle, The case for energy-proportional computing, *Computer* 40 (12) (2007) 33–37. <http://dx.doi.org/10.1109/MC.2007.443>.
- [28] M. Migliardi, A. Merlo, Modeling the energy consumption of distributed ids: A step towards green security, in: MIPRO, 2011 Proceedings of the 34th International Convention, 2011, pp. 1452–1457.
- [29] M. Migliardi, A. Merlo, Energy consumption simulation of different distributed intrusion detection approaches, in: 2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2013, pp. 1547–1552. <http://dx.doi.org/10.1109/WAINA.2013.214>.
- [30] M. Migliardi, A. Merlo, Improving energy efficiency in distributed intrusion detection systems, *J. High Speed Netw.* 19 (3) (2013) 251–264. <http://dx.doi.org/10.3233/JHS-130476>.
- [31] D.S. Wong, H. Fuentes, A. Chan, The performance measurement of cryptographic primitives on palm devices, in: Proceedings 17th Annual Computer Security Applications Conference, 2001, ACSAC 2001, 2001, pp. 92–101. <http://dx.doi.org/10.1109/ACSAC.2001.991525>.
- [32] C. Hager, S. Midkiff, J.-M. Park, T. Martin, Performance and energy efficiency of block ciphers in personal digital assistants, in: Third IEEE International Conference on Pervasive Computing and Communications, 2005, PerCom 2005, 2005, pp. 127–136. <http://dx.doi.org/10.1109/PERCOM.2005.29>.
- [33] J. Toldinas, R. Damasevicius, A. Venckauskas, T. Blazauskas, J. Ceponis, Energy consumption of cryptographic algorithms in mobile devices, *Elektron. Elektrotech.* 20 (5) (2014) 158–161. URL <http://dx.doi.org/10.5755/j01.eee.20.5.7118>.
- [34] A. Castiglione, G. Cattaneo, M. Cembalo, A.D. Santis, P. Faruolo, F. Petagna, U.F. Petrillo, Engineering a secure mobile messaging framework, *Comput. Secur.* 31 (6) (2012) 771–781. <http://dx.doi.org/10.1016/j.cose.2012.06.004>. URL <http://www.sciencedirect.com/science/article/pii/S016740481200096X>.
- [35] A. Kejariwal, S. Gupta, A. Nicolau, N. Dutt, R. Gupta, Energy efficient watermarking on mobile devices using proxy-based partitioning, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 14 (6) (2006) 625–636. <http://dx.doi.org/10.1109/TVLSI.2006.878218>.
- [36] A. Castiglione, G. Cattaneo, G. Maio, F. Petagna, Sec3t: Secure end-to-end communication over 3g telecommunication networks, in: 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011, pp. 520–526. <http://dx.doi.org/10.1109/IMIS.2011.65>.
- [37] P. Miranda, M. Siekkinen, H. Waris, Tls and energy consumption on a mobile device: A measurement study, in: 2011 IEEE Symposium on Computers and Communications (ISCC), 2011, pp. 983–989. <http://dx.doi.org/10.1109/ISCC.2011.5983970>.
- [38] K. Lee, N. Dutt, N. Venkatasubramanian, An experimental study on energy consumption of video encryption for mobile handheld devices, in: IEEE International Conference on Multimedia and Expo, 2005, ICME 2005, 2005, pp. 1424–1427. <http://dx.doi.org/10.1109/ICME.2005.1521698>.
- [39] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, *Comput. Netw.* 54 (15) (2010) 2787–2805. <http://dx.doi.org/10.1016/j.comnet.2010.05.010>. URL <http://dx.doi.org/10.1016/j.comnet.2010.05.010>.
- [40] D. Raymond, R. Marchany, M. Brownfield, S. Midkiff, Effects of denial of sleep attacks on wireless sensor network mac protocols, in: 2006 IEEE Information Assurance Workshop, 2006, pp. 297–304. <http://dx.doi.org/10.1109/IAW.2006.1652109>.
- [41] D. Boubiche, A. Bilami, A defense strategy against energy exhausting attacks in wireless sensor networks, *Journal of Emerging Technologies in Web Intelligence*, 5 (1) URL <http://ojs.academypublisher.com/index.php/jetwi/article/view/jetwi05011827>.
- [42] J. Yin, S.K. Madria, Esecrout: An energy efficient secure routing for sensor networks, *Int. J. Distrib. Sens. Netw.* 4 (2) (2008) 67–82. URL <http://dx.doi.org/10.1080/15501320802001101>.
- [43] B. Deb, S. Bhatnagar, B. Nath, A topology discovery algorithm for sensor networks with applications to network management, 2002.
- [44] E. Vasserman, N. Hopper, Vampire attacks: Draining life from wireless ad hoc sensor networks, *IEEE Trans. Mobile Comput.* 12 (2) (2013) 318–332. <http://dx.doi.org/10.1109/TMC.2011.274>.
- [45] J. Grosschadl, A. Szekely, S. Tillich, The energy cost of cryptographic key establishment in wireless sensor networks, in: Proceedings of the 2Nd ACM Symposium on Information, Computer and Communications Security, ASIACCS '07, ACM, New York, NY, USA, 2007, pp. 380–382. <http://dx.doi.org/10.1145/1229285.1229334>. URL <http://doi.acm.org/10.1145/1229285.1229334>.
- [46] A. Wander, N. Gura, H. Eberle, V. Gupta, S. Shantz, Energy analysis of public-key cryptography for wireless sensor networks, in: Third IEEE International Conference on Pervasive Computing and Communications, 2005, PerCom 2005, 2005, pp. 324–328. <http://dx.doi.org/10.1109/PERCOM.2005.18>.
- [47] T. Martin, M. Hsiao, D. Ha, J. Krishnaswami, Denial-of-service attacks on battery-powered mobile computers, in: Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04), PERCOM '04, IEEE Computer Society, Washington, DC, USA, 2004, p. 309.
- [48] X. Ma, P. Huang, X. Jin, P. Wang, S. Park, D. Shen, Y. Zhou, L.K. Saul, G.M. Voelker, edocto: Automatically diagnosing abnormal battery drain issues on smartphones, in: Proceedings of the 10th USENIX Conference on Networked Systems Design and Implementation, nsdi'13, USENIX Association, Berkeley, CA, USA, 2013, pp. 57–70. URL <http://dl.acm.org/citation.cfm?id=2482626.2482634>.
- [49] R. Racic, D. Ma, H. Chen, Exploiting mms vulnerabilities to stealthily exhaust mobile phone's battery, in: 2006 Securecomm and Workshops, 2006, pp. 1–10. <http://dx.doi.org/10.1109/SECOCOMW.2006.359550>.
- [50] R. Pizzolante, B. Carpentieri, A. Castiglione, A. Castiglione, F. Palmieri, Text compression and encryption through smart devices for mobile communication, in: 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013, pp. 672–677. <http://dx.doi.org/10.1109/IMIS.2013.121>.

- [51] U. Fiore, F. Palmieri, A. Castiglione, V. Loia, A. De Santis, Multimedia-based battery drain attacks for android devices, in: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), 2014, pp. 145–150. <http://dx.doi.org/10.1109/CCNC.2014.6866562>.
- [52] M. Curti, A. Merlo, M. Migliardi, S. Schiappacasse, Towards energy-aware intrusion detection systems on mobile devices, in: 2013 International Conference on High Performance Computing and Simulation (HPCS), 2013, pp. 289–296. <http://dx.doi.org/10.1109/HPCSim.2013.6641428>.
- [53] L. Zhang, B. Tiwana, R. Dick, Z. Qian, Z. Mao, Z. Wang, L. Yang, Accurate online power estimation and automatic battery behavior based power model generation for smartphones, in: 2010 IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2010, pp. 105–114.
- [54] A. Merlo, M. Migliardi, P. Fontanelli, On energy-based profiling of malware in android, in: Proceedings of the 2014 International Conference on High Performance Computing and Simulation, HPCS '14, IEEE, 2014, pp. 535–542. <http://dx.doi.org/10.1109/HPCSim.2014.6903732>.
- [55] G. Jacoby, R. Marchany I., N.J. Davis, Battery-based intrusion detection a first line of defense, in: Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004, 2004, pp. 272–279. <http://dx.doi.org/10.1109/IAW.2004.1437827>.
- [56] T. Buennemeyer, M. Gora, R. Marchany, J. Tront, Battery exhaustion attack detection with small handheld mobile computers, in: IEEE International Conference on Portable Information Devices, 2007, PORTABLE07, 2007, pp. 1–5. <http://dx.doi.org/10.1109/PORTABLE.2007.35>.
- [57] T. Buennemeyer, G. Jacoby, W. Chiang, R. Marchany, J. Tront, Battery-sensing intrusion protection system, in: 2006 IEEE Information Assurance Workshop, 2006, pp. 176–183. <http://dx.doi.org/10.1109/IAW.2006.1652093>.
- [58] A. Castiglione, F. Palmieri, U. Fiore, A. Castiglione, A. De Santis, Modeling energy-efficient secure communications in multi-mode wireless mobile devices, J. Comput. Syst. Sci., <http://dx.doi.org/10.1016/j.jcss.2014.12.022>.
- [59] C. Krintz, Y. Wen, R. Wolski, Application-level prediction of battery dissipation, in: Proceedings of the 2004 International Symposium on Low Power Electronics and Design, 2004, ISLPED '04, 2004, pp. 224–229. <http://dx.doi.org/10.1109/LPE.2004.1349340>.
- [60] A.-D. Schmidt, F. Peters, F. Lamour, S. Albayrak, Monitoring smartphones for anomaly detection, in: Proceedings of the 1st International Conference on MOBILE Wireless MiddleWARE, Operating Systems, and Applications, MOBILWARE '08, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 2007, pp. 40:1–40:6. URL <http://dl.acm.org/citation.cfm?id=1361492>. 1361542.
- [61] N. Balasubramanian, A. Balasubramanian, A. Venkataramani, Energy consumption in mobile phones: A measurement study and implications for network applications, in: Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement Conference, IMC '09, ACM, New York, NY, USA, 2009, pp. 280–293. <http://dx.doi.org/10.1145/1644893.1644927>. URL <http://doi.acm.org/10.1145/1644893.1644927>.
- [62] A. Carroll, G. Heiser, An analysis of power consumption in a smartphone, in: Proceedings of the 2010 USENIX Conference on USENIX Annual Technical Conference, USENIXATC '10, USENIX Association, Berkeley, CA, USA, 2010, 21–21, URL <http://dl.acm.org/citation.cfm?id=1855840>. 1855861.
- [63] A. Rice, S. Hay, Decomposing power measurements for mobile devices, in: 2010 IEEE International Conference on Pervasive Computing and Communications (PerCom), 2010, pp. 70–78. <http://dx.doi.org/10.1109/PERCOM.2010.5466991>.
- [64] L. Zhang, B. Tiwana, Z. Qian, Z. Wang, R.P. Dick, Z.M. Mao, L. Yang, Accurate online power estimation and automatic battery behavior based power model generation for smartphones, in: Proceedings of the Eighth IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, CODES+ISSS '10, ACM, New York, NY, USA, 2010, pp. 105–114. <http://dx.doi.org/10.1145/1878961.1878982>.
- [65] Y. Xiao, R. Bhaumik, Z. Yang, M. Siekkinen, P. Savolainen, A. Yla-Jaaski, A system-level model for runtime power estimation on mobile devices, in: Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on Int'l Conference on Cyber, Physical and Social Computing (CPSCom), 2010, pp. 27–34. <http://dx.doi.org/10.1109/GreenCom-CPSCom.2010.114>.
- [66] M. Dong, L. Zhong, Self-constructive high-rate system energy modeling for battery-powered mobile systems, in: Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services, MobiSys '11, ACM, New York, NY, USA, 2011, pp. 335–348. <http://dx.doi.org/10.1145/1999995.2000027>.
- [67] C. Yoon, D. Kim, W. Jung, C. Kang, H. Cha, Appscope: Application energy metering framework for android smartphones using kernel activity monitoring, in: Proceedings of the 2012 USENIX Conference on Annual Technical Conference, USENIX ATC '12, USENIX Association, Berkeley, CA, USA, 2012, p. 36.
- [68] S. Hao, D. Li, W.G.J. Halfond, R. Govindan, Estimating mobile application energy consumption using program analysis, in: Proceedings of the 2013 International Conference on Software Engineering, ICSE '13, IEEE Press, Piscataway, NJ, USA, 2013, pp. 92–101. URL <http://dl.acm.org/citation.cfm?id=2486788>. 2486801.
- [69] A. Nacci, F. Trov, F. Maggi, M. Ferroni, A. Cazzola, D. Sciuto, M. Santambrogio, Adaptive and flexible smartphone power modeling, Mobile Netw. Appl. 18 (5) (2013) 600–609. <http://dx.doi.org/10.1007/s11036-013-0470-y>.
- [70] M. Dong, L. Zhong, Chameleon: A color-adaptive web browser for mobile oled displays, IEEE Trans. Mob. Comput. 11 (5) (2012) 724–738. <http://dx.doi.org/10.1109/TMC.2012.40>.
- [71] D. Shin, Y. Kim, N. Chang, M. Pedram, Dynamic voltage scaling of oled displays, in: Proceedings of the 48th Design Automation Conference, DAC '11, ACM, New York, NY, USA, 2011, pp. 53–58. <http://dx.doi.org/10.1145/2024724.2024737>.
- [72] N. Gobbo, A. Merlo, M. Migliardi, A denial of service attack to gsm networks via attach procedure, in: A. Cuzzocrea, C. Kittl, D. Simos, E. Weippl, L. Xu (Eds.), Security Engineering and Intelligence Informatics, in: Lecture Notes in Computer Science, vol. 8128, Springer, Berlin Heidelberg, 2013, pp. 361–376. http://dx.doi.org/10.1007/978-3-642-40588-4_25. URL http://dx.doi.org/10.1007/978-3-642-40588-4_25.
- [73] A. Merlo, M. Migliardi, N. Gobbo, F. Palmieri, A. Castiglione, A denial of service attack to umts networks using sim-less devices, IEEE Transactions on Dependable and Secure Computing 11 (3) (2014) 280–291. <http://dx.doi.org/10.1109/TDSC.2014.2315198>.