Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 7 (2012) pp. 338-346
© MIR Labs, www.mirlabs.net/jias/index.html

Green-Aware Security: Towards a new Research Field

Luca Caviglione[1], Alessio Merlo[2] and Mauro Migliardi[3]

[1] Institute of Intelligent Systems for Automation
Italian National Research Council (CNR)
Via de Marini 6, 16149, Genova (Italy)
luca.caviglione@ge.issia.cnr.it

[2] e-campus University, Department of Engineering,
Via Isimbardi, 10, 22060, Novedrate, (Italy)
alessio.merlo@uniecampus.it

[3] University of Padova,
Department of Information Engineering (DEI),
Via Gradenigo, 6, Padova (Italy)
mauro.migliardi@unipd.it

***Abstract*: Green Security is a new research field aimed at defining and investigating security solutions under an energy-aware perspective. The aim of Green Security is twofold: 1) evaluating the actual security mechanisms both considering the energy costs and the effectiveness; 2) building new security mechanisms by considering energy efficiency from the design phase. In this paper, we first provide a definition of Green-Aware Security and an early manifest. Thus, we investigate some formalism to model Green-Aware Security issues, then we provide a use case showing how it is possible to model the energy consumption of two Intrusion Detection System (IDS) strategies, then we leverage this model to assess the energy leakage due to the late discovery of bad packets. Finally, we discuss an introductory assessment of the energy costs related to security on mobile device, which is a promising research trend for Green-Aware Security.**

Keywords*: *green aware security, energy awareness, energy consumption, security, Intrusion Detection Systems, mobile devices.

I. Introduction

Electronic data and the capability to exchange them quickly and without interruptions is becoming more and more one of the basic requirements of the economy of our modern society. This growing dependency, though, is showing in other fields too, in fact from military to recent developments of e-government, it is of paramount importance to be able to access and tap into the electronic telecommunication grid.

A second important aspect of the recent evolution of our society is the proliferation of wideband connections. If it is certainly true that a generalized availability of high speed connections opens the market to a large number of innovative web-based applications, it is also true that the always-on Internet turns any home PC into a target for intrusions and drafting into botnets [1]. The dimension of this problem is shown by the generation of a new storm of network attacks that every day accounts for a non-negligible amount of network traffic. In fact, recent network monitoring activities suggest that the number of controlled nodes somehow participating to the malicious activities of a botnet is dramatically increasing.

These reasons, besides others that are beyond the scope of this paper, make security an extremely hot topic both in research and in every day’s practice.

Nonetheless, security is certainly not the only critical aspect of our modern society. In fact, it is also true that our carbon footprint is showing an alarming steadiness in its growth, and that a non-negligible part of this growth is due to computing and networking that are the foundations of the two previously described phenomena.

This fact, as a recent report of the Organization for Economic Co-operation and Development shows [2], has spurred the growth of a generation of green computing initiatives and has turned green computing and networking into another very hot topic both in research [3], [4], [5] and in industrial practices.

However, while Green Computing and Networking are two important topics in the most recent research agenda, security considerations cannot be avoided if we want to devise truly effective measures. In fact, as we have already stated, there is no scenario in our modern society in which security can be considered less than fundamental. From a specular point of view, while the use of security mechanisms very often increases both the computational and the energy demand of a system, this increase is very seldom considered and the modeling of security systems and mechanisms in terms of power consumption is still a largely unexplored field. As an example, the energy requirements of the most popular (*de-jure* or *de-facto* standards) security mechanisms and frameworks are issues almost systematically underestimated. Furthermore, the design of new security solutions on different paradigms (Web, Grid and Cloud) and layers (ranging from network to application) does not usually include a study of energy consumption and demand.

Furthermore, also attacks to systems and the exploitation of their vulnerabilities lack a clear and analytical modeling in terms of their energy aftermaths. This fact, as the appearance of new security attacks focused on draining battery of mobile devices clearly shows, is rapidly turning into a critical issue because of the explosive growth of such energy-constrained devices.

In this paper we present a manifesto of Green-Aware Security, pointing out potential research trends from different points of views. To this aim, we also provide some early attempts to model some aspects related to energy costs of security.

The remainder of the paper is structured as follows: in Section II we point out what Green-Aware Security stands for, while in Section III we discuss the energy issues related to the network layer and we describe a formalism that is fundamental to the task of providing a basic model for energy consumption/saving in security frameworks at different abstraction layers; in particular, in Section IV we provide a prime formalism sufficient for assessing energy consumption at application level, while in Section V we use such formalism to model the energy consumption of a case study: a Distributed Intrusion Detection System (DIDS) on a ISP core network; in Section VI we use this model to evaluate the energy cost of two different strategies for a DIDS, pointing out the energy leakage due to the late discovery of bad packets. In Section VII we investigate the impact of security over mobile devices. Finally, in Section VIII, we provide some concluding remarks and possible future research directions.

II. GREEN SECURITY: A MANIFESTO

An ICT solution provides a set of features to an end-user, and each end-user is expected to use them in a correct way. However, each ICT solution is potentially affected by vulnerabilities which may allow both naïve and malicious end-users to make risky, unwanted and unexpected use of the platform. ICT Security has always been devoted to the definition of mechanisms able to avoid misuse of ICT platforms by malicious users, thus allowing only uses that comply with the intended scope of the system itself.

Given any ICT platform, to define a comprehensive security solution able to satisfy all the security properties that the platform is expected to meet is quite often a task too complex to be tackled as a whole. Thus, security is commonly obtained by means of a combination of different mechanisms each providing a solution for a specific security issue or property. However, this addictive process made by combining different mechanisms into a complex solution may not lead to the expected security level as security in ICT systems shows some peculiar system level characteristics. We point out the most important aspects:

- ICT Security is Cross-Layer. Complex Systems are designed as layered architectures, where each layer offers services to neighbors according to a specific interface. Security must obviously check that no exploitable flaws are present in each layer, but must also ensure that there is no room for flaws that are generated by unexpected interactions between layers. Thus a layered approach is not enough and a full cross layer view is needed.

- ICT Security is Invasive/Pervasive. Security solutions need to encroach in software and hardware components beyond the interface designed for common use, especially in cooperative distributed systems like Grid [17] or Cloud Computing.

- Security must also take into account each hardware/device and software component related to the whole ICT platform.

- ICT Security is Technology-dependent. The security of a system depends on specific technological implementation details (e.g., the duration and timing of specific operation performed either by software or hardware components) thus security solutions are often valid only as long as a given ICT technology is in use.

In practice, security solutions do not provide any new feature to the user, and they increase complexity and computational demand to the underlying hardware.

From an energy point of view, security increases consumption in order to improve robustness and reliability of ICT platforms. Besides, security solutions have been designed and implemented under an efficacy perspective (i.e. aimed at granting the expected security properties) taking seldom into account performance and optimization.

In this scenario, Green-aware Security is a new research field aimed at merging into Security research energy-aware paradigms and optimizations that have been recently investigated with the advent of Green Computing and Networking.

The main goals of this joint research action are:

- building new techniques and paradigms to assess the energy consumption of security solutions;

- developing future generation security mechanisms optimized both in term of efficacy and energy-consumption;

- defining new security solutions able to adapt their behavior depending on security properties and actual power-consumption.

Summing up, Green-Aware security is a multidisciplinary research field involving knowledge and expertise from many different disciplines, as well as industrial practices, such as Security, High Performance Computing/Networking, Distributed Computing, Silicon Efficiency, Hardware Design, Network Planning and Traffic Engineering, Battery Development, Operational Research for optimal scheduling of process and optimal selection of functional parameters, AI, etc. To better highlight the central role of Green Security, Figure 1 depicts its intrinsic highly interdisciplinary role.

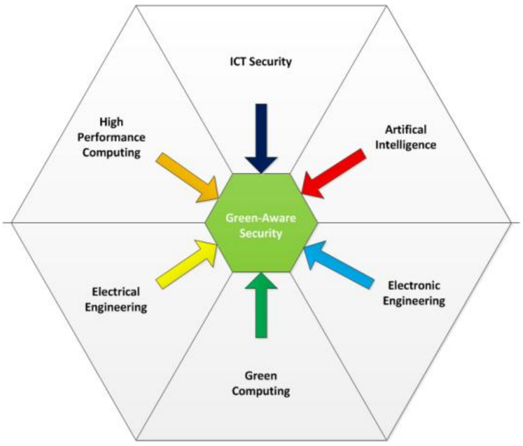

Figure 1: Green-Aware Security as a highly interdisciplinary research field.

As shown, Green-Aware Security is basically a highly interdisciplinary research trend involving heterogeneous expertise both inside and outside the ICT world.

III. Modeling Network Security Mechanisms

In this Section we focus on the investigation of the joint utilization of security solutions and communication networks in the perspective of power consumption or efficiency issues. In fact, the increasing complexity and pervasive nature of Internet applications account for a very complex scenario, where the service infrastructure is mixed with a complex internetwork of resources. Besides, computing and network elements can be also virtualized or arranged in fictitious overlay (e.g., as it happens in Virtual Private Networks scenarios). Therefore, decoupling the impact of network-related security mechanisms from the rest of the deployment can deepen the understanding of energy consumption issues. In fact, the increasing amount of users accessing network services while on the road reflects into an exponential growth of the Internet traffic. At the same time, such huge amount of data to be delivered requires more network devices (e.g., routers), which account for an escalation in the energy consumption [6]. Network security mechanisms are mandatory to properly support the modern usage patterns of Internet. We mention, among the others the most diffuse services: *i*) personal communications such as those based upon the Voice over IP (VoIP) paradigm, requiring security mechanisms to guarantee confidentiality; *ii*) social networking like services, demanding for methodologies to avoid identity theft and privacy issues and *iii*) access to and control of remote applications/devices needing a proper degree of security to be effectively operated through the public Internet. Therefore, understanding the impact in terms of energy consumption of security mechanisms is very complex. To increase this complexity, users also have several devices, often mobile, multiple appliances (e.g., gaming consoles and set-top-boxes) and a more *always connected* attitude [7]. Owing to the intrinsic distributed nature of this “diffuse” Internet, proper protocols must be available to guarantee the correct exchange of information among the involved entities. For instance, personal data are constantly delivered among several devices to have them always synced. As a consequence, the presence of security mechanisms heavily impacts on the power consumption of the Internet, and can clash with green requirements, which are becoming mandatory (see, e.g., reference [8] and references therein). Also, a precise understanding of the scope of security countermeasures (e.g., if deployed in the access network, the core network, end nodes, or in a mixed flavor) and when/how they account for power consumption, allow understanding whether or not, network-oriented techniques for energy consumption can suffice or be unpractical. For instance, the re-engineering of the devices/platforms can be unnecessary for some application, while an adaptive approach can lead to higher benefits. Summing up, mixing security with modern Internet usage trends reflects in a complex “problem space”, and rises, at least, the following *four* main issues.

Specifically:

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 due to overhead required transmitting control and encrypted information, as well as credentials.
3. Such protocols and mechanisms can reflect in software layers, which increase consumption through *additional CPU usage*. At the same time, they can be implemented via ad-hoc hardware (e.g., external devices or built-in ICs) also requiring a proper amount of power.
4. Users access to Internet both via wireless and wired access networks, thus, security mechanisms could be deployed at different *layers*, according to the specific deployment.

Issues 1-4 affect the power efficiency of different entities, e.g., the *access network* (case 4), the *core network* (case 1 and 2) and *end-nodes* (case 2, 3 and 4). Therefore, such mapping could be very complex, since more sophisticated services can embrace all the issues, and the results of ongoing research may move and/or mutate the impact point of security measures. This is the case of *proxy*-based architectures [9], where end-nodes are masqueraded via ad-hoc techniques allowing them to dynamically change their energy profiles, via mechanisms such as smart sleeping. In this scenario, it is paramount that a portion of the ongoing research is devoted to the identification of the location where security has the most significant impact within the network architecture, and to the problem of understanding if greening the security measures changes their nature or adds issues in different portion of the network. Another perspective concerns the mapping of issues 1-4 into the well-developed taxonomy of green-aware techniques for the development of energy aware networks. Also, it must be evaluated if non-security oriented power saving techniques can be also beneficial “for free” when applied to security mechanisms. The *three* major techniques, which can be borrowed from the energy-saving research applied to networking, are:

1. *Dynamic Adaptation [14, 15]*: it enables devices to react to particular traffic (or security) criteria via idle periods, voltage reduction and real-time activation/deactivation of portion of the hardware or the software managing security aspects.
2. *Smart Sleeping [14,15]*: it consists of turning on and off the devices according to specific stimuli to save power. The most popular method, as previously mentioned, is based on proxying the target device.
3. *Re-Engineering [14,15]*: power-inefficient devices and protocols are dismantled in favor of more efficient solutions, such as those based on a smaller nanometer production process, or redesigned to achieve a complexity reduction.

However, solutions 1-3 cannot be directly applied for the optimization of the energy consumption of security mechanisms. Rather, they should be carefully tweaked and for the specific scope of reducing the energy impact, while guaranteeing a proper degree of security. This is even true for the case of the even more mobile Internet, where many hosts are handheld and battery operated. Even if modern mobile appliances have a more energy efficient silicon design, they increase the problem space to be addressed when jointly designing security mechanisms and power efficient approaches. .

In this context, Green Security must deeply investigate the security implications of having energy aware mechanisms in place and, at the same time, recognize if the three major aforementioned techniques may introduce additional security flaws. At the same time, it is necessary to understand if reducing the energy consumption of security frameworks may also lead to the reduction of the overall security efficiency, e.g., in terms of detected threats and response time. Obviously, any trade-off of this kind must be fully identified and carefully evaluated. Finally, it is important to understand that security and energy-saving can be (at least potentially) two conflicting goals. Therefore, *green security is an even more challenging proposition in the sense that the reduction of consumptions cannot be assumed as a goal per-se but must be always evaluated in comparison with the correspondent level of security achieved*. Summarizing, it is crucial to develop specific models dedicated to the understanding of the overall power consumption, and to the identification of the impact of security mechanisms to the energy footprint of the whole system. Since security is a pervasive concept, which applies to many different entities, which can be also highly distributed and virtualized (e.g., as it happens in the case of Cloud computing or Grid architectures), developing the proper understanding of its energy-related implications can be unfeasible if not tackled with a *divide-et-impera* approach to obtain lower complexity scopes.

In this perspective, we now try to isolate energy consumptions of network related security mechanisms to maintain a manageable degree of complexity.

IV. An Analytical Model for Green-Aware Security

In this section we present a very basic analytical model to precisely identify the scope of green security. Isolating the contribution to the overall consumptions by breaking up the overall process should help to understand what has to be minimized, where the consumption happens into the network, what has to be measured and what the most suitable techniques are. Such steps are the fundamental research efforts, which have to be performed to bring green security into the field of feasibility. To avoid burdening the notation, in the following, we dropped the dependence of time *t*. Specifically, we aim at having a model like:

$$E^i_{Tot} = E^i_{Net} + E^i_{Sec} \qquad (1)$$

where, E^i_{Tot} and E^i_{Net} are the overall and due to network operations power consumptions for the *i*-th traffic flow, respectively, while E^i_{Sec} is the power consumption of security mechanisms. Due to the high complexity of the scenario, creating an ultimate and unique energy consumption model is unfeasible. While classical green-networking (or computing) approaches minimize E^i_{Net}, green security wants to reduce E^i_{Sec}.

Quantifying the latter via measurements campaigns, consumption models, or simulations (e.g., by using black box modeling for the more complex settings) are core actions. In fact, if the impact (in terms of power consumption) of the security portion is not relevant, trying a minimization could be inconvenient. The global power consumption (1) can be further refined:

$$E^i_{Sec} = E^i_{Sec,Net} + E^i_{Sec,Dev} \qquad (2)$$

where, $E^i_{Sec,Net}$ and $E^i_{Sec,Dev}$ quantify the power needed by the security mechanisms deployed within the network and the end nodes (e.g., users devices), respectively. Eqs. 1 and 2 can be combined to produce a more comprehensive model, to take into account the overall traffic experienced by a given Internet Service Provider (ISP), i.e.,

$$E_{ISP} = \sum_{i=0}^{N} E^i_{Net} + E^i_{Sec,Net} + E^i_{Sec,Dev} \qquad (3)$$

where, N is the number of sessions managed by the ISP at a given time *t*. The model proposed in 3 has been developed to be general enough to take into account several scenarios, e.g., *i*) if security mechanisms are not employed for a given flow, only the consumption due to network devices can be computed and *ii*) the per-flow granularity can be dropped if not needed. Again understanding via simulations or measurements the user population, which reflects into N, is mandatory to carefully evaluate if green security should be employed. Also, separating the energy consumptions contributions can suggest the best strategy to reduce power consumption (i.e., based on the techniques 1,2 and 3 proposed in Section II). To summarize, one of the main scopes of green security, at least in this preliminary stage, is to quantify, with different degrees of precision, specific contributions (e.g., those previously defined as, $E^i_{Sec,Net}$ and $E^i_{Sec,Dev}$), and where/when they are present within the overall network configuration. This guarantees performing proper design choices. Nevertheless, proper modeling is mandatory to build realistic simulation, also to support engineering of the next-generation of services and infrastructures.

V. Applying a Green-Aware Security Model to a Practical Use Case: Distributed Intrusion Detection

In this Section we show a use case of the model described in the previous section, more in details, we describe how it is possible to evaluate security strategies in a green perspective. In particular, we tailor our model to the problem of describing the energy consumption in a distributed intrusion detection system and we use it to show how two strategies for inspecting incoming packets, equivalent in terms of security effectiveness, can have heterogeneous energy costs, depending on several different factors.

An Internet Service Provider Network (ISPN) can be modeled as an overlay network made of a set of connected routers. Each router supports different operations from package forwarding, storing and analysis. A packet reaching a boundary router (router A in Figure 2) in the ISPN is then forwarded through the network towards another boundary router (router B).

.

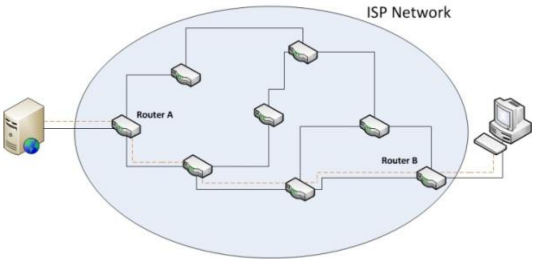

Figure 2: Routers in an Internet Service Provider Network

Trivially, each operation inside the ISPN has an energy cost. As remarked, we are interested in modeling the energy consumptions related to the intrusion detection analysis performed by the routers and the energy cost for the delivery of packets in the ISP. Thus, we ignore, for instance, costs for network management.

A. *Distributed Analysis Model*

We model the ISPN as a set of links and routers, but without modeling the actual topology. Thus, we indicate with

$RSet$

the set of routers in the ISPN and with

the set of links (hops) between routers. An Intrusion Detection System (IDS) like Snort [10] divides the analysis of a packet into a set of independent analysis unit (*au*), such that, as shown in [11] and, the analysis of a packet can be carried out by different routers along the path to the destination. Given $Aus = \{au\}$ the set of all possible analysis units of an IDS, we define a single packet p_i as the ordered sequence of analysis units that the IDS should execute for its security assessment: $p_i = \left[au_1, au_2, \dots, au_{M_i}\right]$, where au_j I Aus . We identify the packet in terms of analysis units only; as a consequence, two packets in the network requiring to be analyzed by the IDS through the same sequence of units are considered identical. Any subsequence of a packet is thus considered a packet. Thus, we refer to any sequence of analysis unit as a packet. We assume that (1) the whole sequence of analysis units should be executed by the IDS in order to flag the packet as good or bad and that (2) the analysis units must be executed orderly, namely au_j should be

executed before .The execution of each analysis unit takes to the consumption of energy from the router running the IDS. We associate an energy value E_{au_j} to the energy consumption required for executing the analysis unit *au*$_j$. Thus, we define the energy cost for the sole analysis of the packet p_i as:

$$E_{p_i} = \sum_{j=1}^{M_i} E_{au_j}$$

Analysis units are executed on routers. With the previous definition of packet, we model a router as a packet consumer. In detail, given a packet $p_i = \left[au_1, au_2, \dots, au_{M_i}\right]$ entering a router, the router processes the first part of the analysis sequence (e.g. for some *j'*) and forwards the remaining sequence (i.e. the packet $\left[au_{j'+1}, au_{j'+2}, \dots, au_{M_i}\right]$) to a neighbor (see Fig. 3).

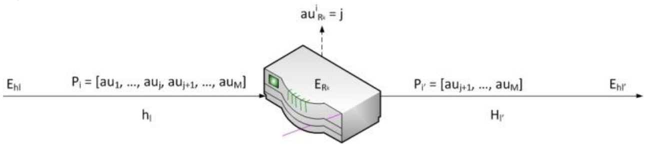
$au^i_{R_k} = j$
E_{hl}
$P_i = [au_1, \dots, au_j, au_{j+1}, \dots, au_M]$
E_{R_k}
$P_{i'} = [au_{j+1}, \dots, au_M]$
$E_{hl'}$
h_l
$H_{l'}$

Figure 3: Energy model of ISPN routers

Since each router is not a machine dedicated for the sole analysis, we argue that only a given amount of energy can be used for intrusion detection purposes in any moment. Moreover, we argue that such value is floating over time, depending on the workload of the router. Hence, we indicate with E_{R_k} the amount of energy that, in a given moment, the IDS on router R_k can use for analyzing the content of a packet.

Therefore, given a packet p_i , the number of consecutive analysis units that the router can process is provided by the maximum value $au^i_{R_k}$ such that

. We refer to $au^i_{R_k}$ as the number of analysis units that the router R_k can process for the packet p_i in a given moment.

Beyond the pure analysis, the energy consumption of the ISPN comprises the **routing** of the packet from the entrance point (router A in Fig. 2) to the exit one (router B). Given the

set of links( ) and a packet p_i , we associate a value to each link in *LSet*, defining the energy consumption required for forwarding the packet p_i on that link. Note that the activity of the router (both analysis and forwarding) has no effects on the dimension of the packet. For this, from delivery perspective, the packet is recognized as invariant during its travel through the ISP. As a consequence, the energy cost of delivery is independent from the order of the links. Thus, given a subset of L links $H_L \subseteq LSet$, that connect A to B, we define the energy cost of forwarding the packet p_i along such path as:

for

Note that in a scenario without a distributed IDS analysis, packets are straightly routed from router A to router B through the shortest or quicker path. Thus, the routing is driven by the sole delivery purpose. On the contrary, in a DIDS scenario where analysis is completed through different routers and choices are made on the basis of the available analysis capabilities the distributed analysis has also consequences on the routing of the packets and on the length L of the routing path from A to B; we investigate this aspects in the use cases. The total energy consumption for packet analysis and routing in an ISPN with IDS analysis is globally defined as:

$$E_{TOT_i} = E_{p_i} + E_{H_L} = \sum_{j=1}^{M_i} E_{au_j} + \sum_{i=1}^{L} E_{\mathbf{I}_l}^{i}$$

Referring to equation (2), it is simple to obtain that $E_{Sec,Dev}^{i} = \sum E_{p_i}$ and $E_{Sec,Net}^{i} = \sum E_{H_L}$ on the total amount of analyzed packets.

VI. Evaluating the Energy Leakage of IDS Strategies

We show here how the proposed energetic model permits to assess the energetic cost of an IDS strategy. In particular, given an ISP topology, the proposed model allows to evaluate the whole energetic cost of analyzing and routing packets among end-point routers. This global evaluation can be useful to compare the energy consumption of different strategies on the same topology and ISP traffic. This would support an adaptive IDS that switches from a strategy to another depending on the characteristics of traffic and on the energy availability of the single routers of the ISP. Moreover, it is possible to evaluate the actual exploitation of such availability by the analysis process. To this aim, we show how the provided model can be used to assess the energy leakage due to the late discovery of bad packages by considering two strategies as use cases. In our example, we suppose to work on a dataset of N packets travelling the IDS network in a period of time. We indicate with b_N the percentage of bad packets. For the sake of simplicity, we make some strong assumptions on the general model:

- All packets are identical in term of analysis units: $p_i = [au_1, au_2, \dots, au_M] \quad i\ \mathbf{I}\ [1, N]$
- All analysis units have the same energy consumption: $E_{au_j} = E_{au} \quad j\ \mathbf{I}\ [1, M]$
- All links have the same energy cost:
- All routers have the same energy availability per packet and, thus, are able to process an identical number of analysis units:

Under these hypotheses, we consider two different IDS strategies and we use the proposed model to evaluate the energy leakage due to a delayed detection of bad packages. Thus, we point out under which conditions one strategy is preferable to the other one, under a sole energetic perspective. We consider a *centralized strategy* and the *closed-loop strategy* of TIFIPS (Travelling Information For Intrusion Prevention Systems) protocol [12]. Regarding the first approach, the packages are routed from the source A to B following the shortest route of length *pl* (i.e. as it would be without packet inspection), thus all analysis units are processed at the exit point only (B). This is a common strategy for some Distributed IDS in an ISPN.

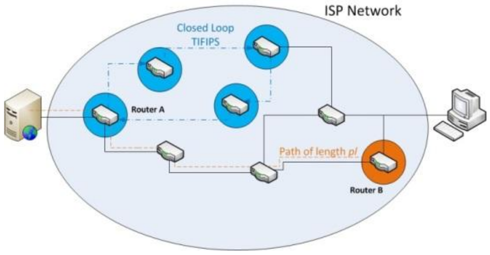

Figure 4: Centralized and Closed Loop TIFIPS use cases: circles show the routers involved in the analysis process.

The second strategy is the basic approach in the TIFIPS protocol. Once a packet reaches router A, it is routed in a closed loop of routers. Each router analyses a number of analysis units depending on the energy availability (i.e. au_R) and forwards it to the next router in the loop. This is left only when the analysis is complete and the packet is returned to router A (see Figure 4).

A. Energy leakage assessment

Under our assumptions, the total amount of energy consumed for the analysis of each packet is

$E_{p_i} = M\ E_{au} \quad \forall\ i\ \mathbf{I}\ [1, N]$

The amount of energy needed to perform intrusion detection on N packets (i.e. $N\ E\downarrow(p\downarrow i\ ))$ is invariant between the centralized and closed loop strategy since each analysis unit should be processed by routers, independently from strategy. In fact, it is inacceptable to deliver a packet outside the ISPN which is not completely analyzed. Thus, the energy leakage regards the sole routing and it is measured, as remarked, in terms of energy wasted for routing bad package uselessly along the ISPN. In fact, an efficient IDS strategy can reduce the number of hops traveled by every bad packet by providing an early detection of the bad packets. To this aim, it is simple to understand that the best case can be reached when all packages are completely analyzed on the A router, thus allowing only good packets to travel along the ISPN. In this case, the energy cost of routing only good packets is given by:

Since we are focusing on distributed IDS, this case is uninteresting; however, the complete analysis on the entrance node is a hardly realistic behavior, since the traffic that enters into a ISPN is hard to be estimated, thus the main effort of an entrance router is on routing the traffic inside the ISPN, allocating very few or null resources for packet analysis. Taking into account this ideal scenario as the best case, we first assess the energy amount for packet routing in the proposed strategies, extracting the energy leakage as a difference between such amount and the best case. In the centralized approach, all packages travel to router B and then are analyzed. Thus, the total cost for routing is provided by:

$$E^{C}_{H_{pl}} = N\ pl\ E_H$$

The energy leakage is given by:

$$Leak_C = E^{C}_{H_{pl}} \mid E^{Best}_{H_{pl}} = b_N\ N\ pl\ E_H$$

In the closed loop TIFIPS, all packets are traveled along a loop of routers and then only the good ones are routed along the *pl* path. The number of hops traveled for analysis depends on the number of analysis units processed by each router in the closed loop. In practice, the number of hops in the loop corresponds to the number of routers that should be visited in order to complete the analysis. This value is provided by the ceiling of $^{M}/_{au_R}$. The energy cost for routing in closed loop TIFIPS is then given by:

$$E^{T}_{H_{pl}} = N\ \left\lceil \frac{M}{au_R} \right\rceil E_H + (100 \mid b_N)\ N\ ¡$$

Therefore, the energy leakage is provided by:

$$Leak_T = N\ \left\lceil \frac{M}{au_R} \right\rceil E_H$$

In general, there no exists an optimal strategy. The energy efficiency of a strategy depends on the value of single variables, namely the characteristics of the both packets and network, in any moment. Thus, the best strategy is the one that minimizes the energy leakage under the actual status of traffic and ISPN. In particular, the modeling in our sample use cases shows that energy leakage can depend on very different aspects (path length (*pl*) and bad packet percentage (b_N) in centralized strategy; energy availability on routers (au_R) and analysis units of packets (*M*) in TIFIPS). For instance, the centralized strategy is trivially better than the closed loops

when $\left\lceil ^{M}/_{au_R} \right\rceil \mid b_N\ pl$.

For instance, this happens when router on the loops have very few energy to exploit for packet inspection. On the contrary, the closed loop strategy reveals to be more suitable if routing cost are high due to long paths (e.g. ISP with a big network topology) or with high percentage of bad packets. Each ISP should monitor the value of all variable involved in the all strategies and then triggering adaptively among strategies in different periods, or assign strategies to proper classes of packets, in order to reduce energy leakage. Note that the minimization of the energy leakage does not affect the level of security since all analysis units are processed. Other information on this prime energy assessment can be found in [13].

VII. IMPACT OF SECURITY OVER MOBILE DEVICES

Modern mobile devices are becoming cost-effective and also equipped with different air interfaces assuring their connectivity to the Internet. Most popular mechanisms are the IEEE 802.11 and the General Packet Radio Service (GPRS) or the Universal Mobile Telecommunication System (UMTS). Such transmission technologies allow reaching high data rates, and make portable network appliances well suited to access the plethora of services offered by the Internet. At the same time, they impose additional requirements, especially in terms of on-board power, which is mostly provided via batteries. Even if technologies of batteries, as well as silicon efficiency, made important advancements in the last years, excessive power consumptions still remains the major weakness when adopting portable and handheld machineries.

Furthermore, to turn mobile terminals into real enablers for network applications, proper security requirements must be supported, both at the application and at network level. In order to guarantee such constraints, many protocols, methodologies and software components are available, mostly directly ported from the “desktop” world. However, supporting security does not come for free, since its algorithms and data signaling require CPU cycles, memory, storage and bandwidth. As a consequence, security can reflect into additional power consumptions, thus shortening the battery life, and ultimately, worsening the user experience. The availability of limited power may also generate additional security issues as it can represent an exploitable weakness of the device itself. As an example, let us consider a new wave of hazards, which could be defined as energy-draining attacks. Put briefly, they aim at stimulating traffic processing or responses within the end users’ devices (e.g., via unsolicited network traffic or forcing erratic and CPU consuming behaviors) to produce quick and earlier battery depletions.

Thus, with the increasing diffusion of mobile devices, green security must also take into account specific issues and possible countermeasures/optimizations for power-limited devices.

Possible research issues and industrial developments are, among the others:

- introduce a set of features to force upper bounds of security-related process as to avoid malicious battery drains. In other words, security over mobile devices should also rely on a concept of “energy sandbox”;
- develop mechanisms to enable scaling of security services to save energy at run-time, as to conform to the actual level of energy availability, thus assuring an adaptable behavior to mobile nodes;
- promote the definition of standard security levels and related consumptions in order to forecast the battery life and to have proper “energy signatures” to reveal energy-aimed attacks. Besides, power profiles should be defined in order to reduce the arbitrariness of developers, and to prevent additional weaknesses.

Additional mid-term countermeasures (besides those earlier described in Section III dealing with the network infrastructure) are as follows:

- perform a shift of some security mechanisms from devices to the network, at least for those with very limited power resources. This approach can resemble proxying, but requires a very complex engineering, since it also clashes with issues related to handover and mobility. Besides, it also needed to envisage ad-hoc network strategies for battery powered devices to reduce risks of attacks. To mention a possible simple mechanism based on middle-boxes, we cite the usage of Network Address Translation (NAT) machineries to prevent unsolicited ingoing network traffic for specific devices. This could be very effective in reducing the effectiveness of attacks based on ping flooding or port scanning, which can quickly drain the battery of many portable devices (see, e.g., reference [16] for several tests about battery draining via simple network attacks).

For the aforementioned reasons green security is especially critical both for mobile devices, and for access networks supporting mobile nodes.

VIII. CONCLUSIONS AND FUTURE WORK

As discussed, Green Security aims at defining and investigating security mechanisms in the perspective of explicitly take into account their energy consumption requirements. Additionally, the increasing demand of power also accounts for additional security countermeasures, as to avoid that energy becomes an exploitable items too. Nevertheless, energy optimizing techniques and related additional machineries also requires the adoption of energy-aware security frameworks, which can prevent the injection of additional weak points within the overall infrastructure (e.g., proxy to manage sleeping devices can become exploitable hosts, or introduce additional hazards due to the breaking of the end-to-end semantic of the TCP).

However, their development rises two important issues: i) "*are energy-aware techniques secure?*" and, most importantly, ii) "*can green security guarantee the same performances of* CO_2*-prone techniques?*". This is why "*Green Security*" is crucial, and must be kept into account when performing engineering of green-aware telecommunication infrastructures. In this paper we have presented a formalism to describe security systems in terms of their energy consumption, and we have leveraged this formalism to define an energy consumption model for Distributed Intrusion Detection Systems. Then we have used this model to describe two different policies for Distributed Intrusion Detection in terms of their energy requirements and finally we have evaluated these two policies.

Future work aims at refining the concept of Green Security, also trying to perform field measurements over deployed devices to quantify the energy impact of security. This will enable to produce numerical models (for instance, via black-box modeling approaches a-l àneural network, which are commonly used to model telecommunications-related behaviors [18]) and to perform simulation analysis also for better revealing the priorities needed in the design. At the same time, Green Security should continue to sync with other "greening" initiative in order to early detect possible design flows, as well as to port the most cutting-edge technique into the Green Security world. With such foundation will be also possible to enrich modeling and to disseminate results to the Industrial world, which is the "real" responsible in the development of the devices. Lastly, also network operators should have Green-Security-oriented models for efficiently planning their deployment, and possible actions to reduce consumptions (e.g., ad-hoc billings to reduce power peaks) while guaranteeing the maximum level of security to their customers.

REFERENCES

[1] F. Naseem, M. Shafqat, U. Sabir, and A. Shazad, "A Survey of botnet Technology and Detection", International Journal of Video and Image Processing and Network Security, Vol. 10 No:01.

[2] OECD, Working Party on the Information Economy, Towards Green ICT strategies: Assessing Policies and Programmes on ICTs and the Environment, available online at http://www.oecd.org/dataoecd/47/12/42825130.pdf

[3] Van Heddeghem W., Vereecken W., Pickavet M., Demeester P., Energy in ICT - Trends and research directions, Proc. Of the IEEE 3rd International Symposium on Advanced Networks and Telecommunication Systems (ANTS), New Delhi, 14-16 Dec. 2009.

[4] Bianzino A., Chaudet C., Rossi D., Rougier J., A Survey of Green Networking Research, IEEE Communications Surveys & Tutorials, 2010 , Page(s): 1 – 18.

[5] N. Hardavellas, M. Ferdman, B. Falsafi, A. Ailamaki, Toward Dark Silicon in Servers, IEEE Micro, Volume: 31 Issue 4 pp 6 – 15, July-Aug. 2011

[6] J. Baliga, K. Hinton, R. S. Tucker, "Energy Consumption of the Internet," Joint International Conference on Optical Internet and the 32nd Australian Conference on Optical Fibre Technology (COIN-ACOFT07), Melbourne, Australia, June 2007.

[7] M. Gupta, S. Singh, "Greening of the Internet", 2003 International Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM03), Karlsruhe, Germany, August 2005, pp. 19 - 26.

[8] S. N. Roy, "Energy Logic: A Road Map to Reducing Energy Consumption in Telecommunications Networks," 30th International Telecommunications Energy Conference (INTELEC08), San Diego, CA, USA, September 2008.

[9] K. Christensen, C. Gunaratne, B. Nordman, "Managing Energy Consumption Costs in Desktop PCs and LAN Switches with Proxying, Split TCP Connections, and Scaling of Link Speed", International Journal of Network Management, Vol. 15, No. 5, pp. 297 - 310, September-October 2005, Wiley.

[10] Casewell B. and Beale J., SNORT 2.1, Intrusion Detection, second ed. Syngress, May 2004

[11] Debar H., Curry D., Feinstein B., "The Intrusion Detection Message Exchange Format (IDMEF)", rfc 4765, March 2007, http://www.ietf.org/rfc/rfc4765.txt

[12] Migliardi M., Stringhini G., Travelling Information For Intrusion Prevention Systems, Proc. of the 2010 International Conference on Security and Management, Las Vegas, Nevada, USA, July 12-15, 2010.

[13] Migliardi M., Merlo A., Modeling the Energy Consumption of an IDS: a step towards Green Security, Proc. of the 34th International Convention on Information and Communication Technology, Electronics and Microelectronics, 23rd – 27th of May, 2011, Opatija (Croatia).

[14] A. Bianzino, C. Chaudet, D. Rossi, and J. Rougier. A survey of green networking research. Communications Surveys Tutorials, IEEE, pp. 1 -18, May 2010.

[15] 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 Communications Surveys and Tutorials (COMST), vol. 13 no. 2, pp. 223-244, May 2011.

[16] L. Caviglione, A. Merlo, "Energy Impact of Security Mechanisms in Modern Mobile Devices", Network Security, Elsevier, Vol. 2012, No. 2, Feb. 2012, pp. 11-14.

[17] A. Merlo, "A Cooperative Model for Resource Sharing on Grid", Journal of Information Assurance and Security, Vol.6, No, 2, Jan 2011, pp. 106-114.

[18] L. Caviglione, "A Simple Neural Framework for Bandwidth Reservation of VoIP Communications in Cost-Effective Devices", IEEE Transactions on Consumer Electronics, IEEE, Vol. 56, No. 3, pp. 1252 - 1257, August 2010.

Author Biographies

Luca Caviglione is a Researcher at the Istituto di Studi sui Sistemi Intelligenti per l'Automazione (ISSIA) of the Italian National Research Council (CNR). He has a PhD in Electronic and Computer Engineering from the University of Genoa, Italy. His research interests include peer-to-peer (p2p) systems, IPv6, social networks, wireless communications, and network security. He is author and co-author of 80 academic publications, and several patents in the field of p2p. He has been involved in Research Projects funded by the ESA, the EU and MIUR. He is a Work Group Leader of the Italian IPv6 Task Force, a contract Professor in the field of p2p networking and a Professional Engineer. He is involved in the Technical Program Committee of many International Conferences, and regularly serves as a reviewer for the major International Journals. From 2011, he is an Associate Editor for the Transactions on Emerging Telecommunications Technologies, Wiley. Also, he is in the Editorial Board of the International Journal of Trust Management in Computing and Communications, Inderscience.

Alessio Merlo received his PhD in Computer Science from University of Genoa (Italy) where he worked on performance and access control issues related to Grid Computing. He is currently serving as an Assistant Professor at e-Campus University, Department of Engineering. His research interests are focused on performance and security issues related to Web and distributed systems. He is currently working on security issues related to Android platform.

Mauro Migliardi Mauro Migliardi is born in Genoa (Italy) in 1966. He got a Laurea degree in Electronic Engineering from the University of Genoa in 1991 and a PhD in Computer Engineering from the University of Genoa in 1995. From January 1998 to February 2000 he has been a research associate at Emory University and one of the main investigators in the HARNESS heterogeneous metacomputing project. From March 2000 to April 2005 he has been an assistant professor at the University of Genoa. Since 2005 he is Associate Professor at the University of Padua. He has also produced more than ninety scientific papers published in national and international, peer reviewed conferences and journals. His main research interest is the engineering of complex, mobile, pervasive, distributed, social systems and high performance networks.