electronics

MDPI

Article

Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices

Vasily Desnitsky [1], Igor Kotenko [1,2,*] and Danil Zakoldaev [2]

[1] Laboratory of Computer Security Problems, The Saint-Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), 39, 14 Liniya, 199178 St. Petersburg, Russia; desnitsky@comsec.spb.ru

[2] International Laboratory of Information Security of Cyber-physical Systems, The Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), 49, Kronverksky Prospect, 197101 St. Petersburg, Russia; d.zakoldaev@corp.ifmo.ru

* Correspondence: ivkote@comsec.spb.ru; Tel.: +7-8123287181

Received: 11 March 2019; Accepted: 5 May 2019; Published: 6 May 2019

Abstract: Currently, energy resource exhaustion attacks targeted on modern autonomously working mobile devices are becoming more and more important. The underdevelopment of specialized defenses against energy exhaustion attacks as well as their often hidden nature for the owner of the target device determine a necessity of an integrated approach to modeling and evaluation of this class of attacks and various types of intruders. The paper analyzes conditions of applicability of energy resource exhaustion attacks performed by various classes of intruders, models them on physical implementations of devices for two application areas, and calculates their performance indicators. Application areas are a TCP/IP network of end-user mobile devices and a self-organizing mesh network designed for operational management and emergency response.

Keywords: cyber-physical security; energy exhaustion attacks; denial-of-sleep; modeling and simulation

1. Introduction

Currently cyber-physical systems including mobile embedded microcircuits, physical actuators, detectors as well as traditional networking and executive units are becoming more common in our life. Management in cyber-physical systems comprises both software/informational and physical aspects of interaction between devices and users. Such interaction along with the critical nature of such systems and remote access via the Internet determine the importance of solving cyber-physical security problems connected to protection of the devices, customer data and the organizational/technical infrastructure.

Besides targeted malicious actions exploiting the specificity of a concrete system and its devices, more universal influences, violating the availability of the system's devices, are gaining peculiar importance. The mobile nature of the devices and the possibility of their functioning in an autonomous mode as well as the constraints on available battery resources have led the devices to be vulnerable to energy resources exhaustion (ERE) attacks. In relation to the wide range of cyber-physical applications—transport systems, power grids, water supply control systems, systems of implantable medical devices, etc.—the consequences of their availability violation can lead to serious man-made disasters and significant financial damages caused by inability of the devices partly or fully to perform their business functions.

The core features of ERE attacks are seen as complexity of their recognition, the relative effectiveness of such attacks, and their volatility. The complexity of an ERE attack detection is determined, first, by the fact that often the effect on the device is implicit—by sending through the Internet or a local

communication port a sequences of false demands to the device, which are not naturally isolatable as attacking actions. Second, to keep track of ERE attacks it is necessary not only to analyze the discharging of the battery, but also the discharging speed change. Third, the detection of ERE attacks may be determined by independent aspects of energy resource discharge due to legal software and clients. By affecting a device, an ERE attacker can select the more productive techniques of carrying out the fast draining of the energy resource allotted for the device operation within days, months or even several years.

These circumstances together with a tendency to insufficient security of modern cyber-physical systems from ERE attacks and a lack of effective means for monitoring such attacks lead to the need for additional research in this field and solving the problem of strengthening the security of devices from ERE attacks. It should be noted the architecture of a target device may not assume the presence of technical possibilities for detailed accurate measurement of its energy consumption. Besides, the form factor and operating conditions of the end product can prevent the connection of external hardware and software units to read data on power consumption.

In modern scientific and technical literature, the issues of ERE attacks are mainly represented by current studies of:

- specific types of ERE attacks, such as vampire attacks [1–3], denial-of-sleep attacks [4–8], attacks on specific crypto-protocols, causing increased power consumption on their executing devices [9], various jamming attacks [10,11], replay attacks and collision attacks [12], etc.;
- specific applications and systems analyzed for possible ERE attacks, such as attacks on personal portable mobile devices in direct line of sight [13,14], combined attacks on mobile devices, using vulnerabilities of a cellular network server [15], attacks on separately located sensors [16], attacks on mesh networks built on specific network protocols [17], attacks on drones [18], attacks on implantable medical devices, taking into account various ways to replenish their charge [19], etc.;
- specific recommendations and particular solutions that can be used to protect against a certain type of such attacks, such as isolation of segments and layers of sensor networks to protect the nodes (victims of ERE attacks) [2,20], packet filtering on some intermediate nodes and comparison with passing traffic patterns [17,19], in particular by using machine learning [21].

In contrast to the above works, this paper concentrates on the classification, comparison and evaluation of various types of ERE attacks on cyber-physical devices, ranging from impacts performed at the physical level to various combined attacks involving social and cyber-physical aspects.

The goal of this paper is, first, to model ERE attacks analytically, focusing on various types of attacking influences and their conditions and, second, to simulate some of the attacks in physically implemented cyber-physical scenarios to verify the feasibility of such attacks experimentally and draw some conclusions on their effectiveness.

The main contribution of the paper is a general framework for modeling and analyzing various types of ERE attacks, including the evaluation of their performance indicators.

The novelty of the work is expressed by a suggested unified approach to representing heterogeneous types of ERE attacks on cyber-physical devices, including both purely software and information-based influences through an intruder's manipulation by data packets, code, etc. and complex actions, including the physical and electromagnetic effects on devices. The experimentally obtained data on evaluating the effectiveness of denial-of-sleep attacks on examples of cyber-physical devices has a certain practically oriented novelty as well.

The general framework for modeling and analyzing ERE attacks includes:

- analysis of possible kinds of ERE attacks on cyber-physical devices;
- an ERE intruder model representing knowledge required for simulation and analysis of ERE influences; and

- experimental studies on the modeling and evaluation of ERE attacks on two developed use cases—a network of end-user mobile devices and a self-organizing mesh network designed for operational management and emergency response.

The rest of the paper is structured as follows. Section 2 provides an overview of the related work. Section 3 presents the proposed model of the intruder. Section 4 encompasses description and analysis of two developed use cases. Section 5 contains experimental studies on the use cases. Section 6 provides the analysis of results. Conclusions and directions of further research are presented in Section 7.

2. Related Work

Nowadays development of battery-related technologies fails to keep up with rapidly improving communication/computing tools significantly. This fact as well as the expansion of various business functionalities consuming increasing energy resources determine the importance and critical nature of energy-based attacks [22] that modern mobile and autonomous electronic devices are exposed to. Moreover, attacks reducing energy can be performed, in particular, by forced activation of defenses against other types of attacks on devices, successfully preventing them by consuming additional energy. In this paper we focus mainly on attacks against personal mobile devices and nodes of autonomous sensor networks, while energy attacks against large-scale computing, in particular, cloud systems, when an intruder absorbs large megawatts [5] lie beyond the scope of this study.

Along with traditionally regarded attacks on the violation of confidentiality, integrity, availability and their derivatives, energy resource exhaustion attacks are singled out as well.

In [23] the results of efforts to discover the causes of improper use of the battery of mobile devices are presented. Specifically a method of revealing faulty process and decreasing the resource consumption of the battery by suspending or postponing doubtful actions is proposed. The tracking process is performed up to restoration of regular battery consumption.

As a rule, the first step of energy exhaustion attacks is exploitation of some communication interface of the victim device. In particular, an intruder can mount energy exhaustion attacks by impacting transport layer protocols, which will make it impossible for the victim device to pass into a low power mode [6,24]. Such an attack is called denial-of-sleep and is aimed at preventing the device from passing from a full-featured mode to a limited-mode operation of reduced power consumption (i.e., sleep mode) [7,16,20].

In contrast to the denial-of-service and quality of service (QoS) degradation attacks, Shakhov and Koo [16] justify the complexity and inefficiency of using traditional intrusion detection approaches and tools in relation to the tasks of identifying energy depletion attacks. Specifically, in [16] energy depletion attacks targeted on isolated sensors of wire-less sensor networks are regarded. In particular, Shakhov and Koo show the feasibility of this type of attacks as well as evaluate such attacks and ways to counter them in the scenario of flood attacks by using continuous time Markov chains.

Moyers, et al. [13] examine some ERE attacks on wireless interfaces of Wi-Fi and Bluetooth as well as some combined attacks to analyze their influence on the battery-life period. The consequences of attacks on the battery drain in mobile devices are analyzed, having simulated particular attacks accelerating the depletion of the battery to the maximum of 18.5%.

Buennemeyer, et al. [14] propose a Battery-Sensing Intrusion Protection System (B-SIPS) against the depletion of batteries for mobile computers. The system warns about the change of power of detected attacks on small wireless devices, using the algorithm for dynamic threshold calculation. B-SIPS nodes are used as sensors in a wireless network and construct the basis of the intrusion detection system. B-SIPS implements the correlation of the power consumption of devices with widespread wireless interfaces.

The papers [12,25] address denial of sleep attacks. Boubiche, et al. [12] propose a mechanism to create an intermediate level for effective protection against attacks on the exhaustion of the battery at

the crossing of the physical and data link layers [13]. In particular, they analyze the following types of attacks: sleep deprivation, barrage, replay, broadcast, collision and synchronization attacks.

Racic, et al. [15] present the realization of a battery exhaustion effect by using vulnerabilities of multimedia messaging service (MMS) packets of mobile devices. The attack acts as follows: the intruder collects a list of mobile devices, including their cellular numbers, IP addresses and information about models, by the use of the notification MMS messages. After that the intruder exhausts the battery of the device by transmitting periodic user datagram protocol (UDP) packets, using the stored packet data protocol (PDP) contexts and the search call channel. Two main vulnerable components in the cellular network are singled out, strategies mitigating risks of such attacks are proposed.

More universal ways of conducting energy exhaustion attacks are, in particular, malicious effects that form electromagnetic interference on a victim device [26,27]. In essence, such interferences cause the target device to increase the power of its receiving-transmitting interfaces, as well as repeatedly making transmission attempts due to frequent packet loss.

Karpagam, et al. [10] analyze selective jamming attacks in a wireless sensor network (WSN) that are aimed at selective physical influence the most crucial packets wirelessly passed. The core part of this influence is a real-time packet classification at the physical layer of the connection. The proposed algorithm for preventing such attacks is based on an algorithm of packet hiding, which is implemented between the media access control (MAC) and the physical Open Systems Interconnection (OSI) layers.

Periyanayagi, et al. [11] propose an intellectual swarm based technique aimed at identifying jamming attacks in WSN. The technique enables analyzing data from sensors against jamming attacks, dynamically modifying the exploited communication channel.

Goudar, et al. [4] examine denial-of-sleep attacks in wireless sensor networks, impacting by modification of packets. The authors showed such influences can decrease the average lifetime of a device from several years up to several hours [8]

In particular they distinguish four types of attacks:

Collision attacks are a simultaneous sending of multiple data packets to a device, leading to its discarding and subsequent resubmitting, and thereby involving extra energy consumption.

Overhearing attacks (i.e., forced listening attacks) assume a node receives packets intended for other nodes in the network, so during the receiving these packets the node cannot switch to a power-saving mode (sleep mode). This attack illustrates an indirect influence of the intruder on the victim node, as the intruder affects some other node through modifying destination address of packets it passes.

A similar attack is the control packet overhead attack, involving passing particular system commands as broadcasts, such as RTS (request to send command, i.e., a warning on the preparedness of a device to send any portion of information by means if a serial port) and CTS (clear to send command, i.e., a warning on a feasibility to get data through a serial port) preventing the receiving device to activate the sleep mode.

Over-emitting attacks pass messages to a device that is not ready to get them. The paper [4] also proposes improvements of the MAC protocol for governing wireless sensor networks through centralized cluster management, using a special node-gateway and a proposed WSN architecture, taking into account the monitored behavioral characteristics of the nodes.

Capossele, et al. [8] describe an method to constructing a WSN having devices functioning in a wake-up-receive mode (WuR). WuR assumes the nodes are in an active mode only during a wireless transmission and subsequent procession of data, whereas in the rest time the nodes are in a high energy-efficiency mode. At that switching between the modes is realized by an event-based management. As a protection from denial-of-sleep attacks the authors propose the use of shared secret keys within the proposed key management protocol to determine the address of the compromised node. As a result only an authorized user, who has the key, is able to send data in the network.

In WSN vampire attacks influencing passed packets at a layer of a routing protocol [1]. Vampire attacks are targeted not so much on some specific host, as on the whole sensor network to

exhaust the energy of all its elements. Mostly these attacks do not flood the network by a false traffic or destruct any packages for their retransmission. Instead the intruder uses formally correct traffic with some tiny modifications in packet routing headers, thereby these attacks turn out to be extremely difficult to detect [1]. As an example a carousel attack, intentionally adding cycles in the packet routes, allows the same message to pass through the same nodes of the sensor network a number of times. A stretch attack reduces energy resource of the network nodes by forcing the use of longest routes via all available nodes.

Mostafa, et al. [9] show a potential vulnerability of Barrett's reduction algorithm used in cryptography, mainly on cyber-physical devices implementing public key cryptography functions. It is assumed the adversary initiates the execution of unnecessary computational operations of the algorithm by substituting the values of certain processor registers. The exploitation of this vulnerability can lead to a significant increase in the execution time of the algorithm, leading to an increase in the energy consumption of the device performing this algorithm. In addition, Mostafa, et al. modified this algorithm, increasing its security against this attack.

The following approaches can be singled out as particular solutions for counteracting the energy exhaustion attacks. For example, in case of sensor networks, Bhattasali, et al. [20] propose the separation of attacked network elements into multiple layers and segments in order to prevent the attackers from influencing the operation of the entire network or some infected node. It is also proposed to use modified cryptography methods with key distribution for nodes inside subgroups of the sensor network, preventing actions to intrude into the network by an attacking node [28].

Recommendations are also made to identify and counteract so called ghost attacks, which initiate the redundant computations on the nodes of ZigBee networks [29]. Patel and Soni consider a monitoring scheme of wireless sensor network nodes in order to detect vampire attacks on the basis of group-based processing of power thresholds of the neighboring nodes [3]. Considering an attack on a specific node, Guo, et al. [17] and Du, et al. [19] propose techniques that enable filtering false information flows provoking the leaving the sleep mode.

3. Generalized Intruder Model

In this section we propose a generalized analytical model of an intruder performing ERE attacks. The model represents a knowledge required for simulation and analysis of this class of attacks. The model is expressed by a formal tuple:

$$M_{\mathrm{ERE}} = (G, O, A, R, F, E, P) \tag{1}$$

G specifies goals of ERE attacks directed to breach the availability of some autonomously working hardware unit. At that battery resource declining can by realized in a rapid gradual or spasmodic way, depending on the nature of the target system and the intruder intentions.

O describes the targets of straightforward or implicit effects of ERE attacks, including sensors of the physical medium, network connections, software components, operating system processes, etc.

A specifies sequences of steps the intruder runs to reach the goals G.

R outlines necessary system resources and means used during an attack, including starting possibilities of the intruder, knowledge and practical skills the intruder possess as well as required time and financial costs.

In our work we differentiate five intruder types in compliance with a classification of the attacker access to a device [30], namely *Type*0—no direct access (social engineering can be used only), *Type*1—remote access through TCP/IP protocol from outside, *Type*2—remote access from nearby by means of Near Field Communication (NFC), Radio Frequency Identification (RFID), ZigBee, etc.), *Type*3—outward access (direct access to RS-232, I2C, etc.) and *Type*4—full access (any modification of the microcircuits and software).

During the analysis we use an intruder classification of intruder capability levels. It comprises the following levels: *Level*1—common typical utilities, known vulnerabilities, *Level*2—specially developed utilities, previously unknown vulnerabilities, *Level*3—team of intruders of *Level*2 (unrestricted resources) [31].

F determines specific conditions and limitations significant for ERE attacks, such as rules for switching between the sleep and regular modes of the hardware unit.

E describes effectiveness of an ERE attack that as an averaged increase of the battery discharging speed after the attack application, whereas *P* denotes possible ways of protection from ERE attacks and attack stealthiness.

Regarding existing papers in the field, the key ERE attack types are identified:

- forced waking of a sleeping device (denial-of-sleep) [13,14] (results of an analysis of this type of attacks are given in Table 1);
- increase of wireless ongoing or outgoing traffic on a device (Table 2);
- forming of electromagnetic interference on wireless channels, causing an increase in transmitter power [10] (Table 3);
- untypical usage (misuse) of a devices' software, including forcing incorrect settings and others (Table 4).

Table 1. Attacks of the denial-of-sleep class.

Attack Goal	Decreasing the Time the Device is in a Sleep Mode in Order to Raise the Power Expenses
Attack features	1. Existence of device idle states of a small energy consumption. 2. Exploiting energy consuming wireless interfaces such as RFID, infrared (IR), NFC, etc. 3. Attack category <*types*1 *and type*2, *level*1 *and above*> [30,31].
Actions of intrude	Growths of the energy consumption of the device by switching its modes *(idle mode → active mode)*.
Required abilities and conditions of intruder	1. Lightweight knowledge of Linux. Downloading and installing typical software tools into the operating system. Skills of performing actions from guides. 2. Minimal time to deploy a new attacking device is needed afterwards the arrangement of software and hardware. 3. Mostly as an equipment it is sufficient to use a typical laptop/single-board computer. A rooted Android device may be needed to execute certain mobile applications.
Conclusion	1. An attack can be fulfilled without straightforward influence of the intruder (i.e., via the wireless interfaces). 2. The attack distance depends on wave frequencies of the wireless protocol and the power of the intruder's antenna. 3. No need for an attacker to be authorized on the target device, intricating a productive protection from such influences.

Table 2. Attacks of wireless traffic growth.

Attack Goal	Increasing Amounts of Income/Outcome Data and Decreasing their Speed
Attack features	1. Typically devices pass data not continuously. An intruder is to increase quantities of data passed and time of the transmission. 2. Attack category <*types*1 *and type*2, *level*1 *and above*>.
Actions of intruder	Attacker logs into the device and starts sending data. To bypass authorization the intruder breaks the key or mounts a replay attack by using some past legitimate traffic.
Required abilities and conditions of intruder	The intruder should have some basic knowledge on the target system to run an attack. A common PC/single-board computer is sufficient for the intruder. A rooted Android device may be required to run some specific soft.
Conclusion	1. An attack can be fulfilled straightforward influence on the device. 2. The attack distance depends on wave frequencies of the wireless protocol and the power of the antenna of the intruder.

Table 3. Forming electromagnetic interference on wireless channels (jamming).

Attack Goal	**Forcing the Device to Raise the Signal Power During the Wireless Data Transmitting**
Attack features	Commonly wireless modules pass data at the minimum power to decrease battery expenses. Attack category <*type*2, *level*2 *and above*>.
Actions of intruder	Electromagnetic noising on transmission channels.
Required abilities and conditions of intruder	The attacker must have special equipment allowing affecting the communication channel. The one must be in a short distance of the device.
Conclusion	1. An attack can be fulfilled without straightforward influence on the device. 2. The distance depends on wave frequencies and the antenna of the intruder.

Table 4. Misuse of a device's software.

Attack Goal	**Spending Battery by Forcing the Device to Execute Unnecessary Operations**
Attack features	Attack category <*type*0- *type*4, *level*1 *and above*>.
Actions of intruder	Additional CPU load, multiple launch of applications, access energy consuming memory, bypass/breaking optimizations and abnormal use of the software, remote desktop session, etc.
Required abilities and conditions of intruder	Penetration abilities for straightforward/remote access to the device and for executing new software on it.
Conclusion	The attack presumes the most serious effect of the attacker to the device.

All these attacks are assumed to operate continuously until the battery is completely drained.

Note that the goal of the proposed model is to identify and systematize knowledge about possible types of ERE attacks and their characteristics. The model can be used to analyze the specifications of a particular cyber-physical system to determine ERE attacks its devices are prone to. Besides, the results of this analysis can be used as a basis for the development of an integrated information security system.

4. Use Cases

As a basis for modeling and evaluating of ERE attacks, taking into account the generalized intruder model (1), we developed two cyber-physical use cases.

The first one represents a fragment of a TCP/IP network of end-user mobile devices, such as smartphones, tablet computers, laptops, etc., operating primarily from autonomous power supplies and using Bluetooth and Wi-Fi wireless communication protocols under the control of a mobile operating system. The business part of these devices is formed by specific applications capable of communication to other devices in the Internet via cellular networks and local wireless networks. High criticality of business applications in communications with other devices as well as possible dynamic switching between the available and preferable physical communication channels (assuming no interruption of the applications) make the devices rather vulnerable to attacking influences.

Among the four attack classes presented above, the attack of wireless traffic growth, not even presuming mandatory intruder's authorization on the device, is seen as the more relevant for this use case. In particular, even in case of WPA2 keys, which cannot be enumerated effectively by a brute force attacker, sending request sequences to a Wi-Fi interface of the device intensively can significantly reduce the battery life or even exhaust it to zero. Note the increase of the electromagnetic noise or shielding is also quite a universal attack. At that, attacks of an abnormal usage of a devices' software, including activation of energy consuming functions/modules, for example forced switching on a Global Positioning System (GPS) sensor, presume previous remote access and governing the device, which complicates the feasibility of this attack.

The second use case represents a self-organizing mesh network designed for operational management and emergency response. The network is constructed on the base of the ZigBee protocol. Its core elements are wireless XBee s2ZB modules of the coordinator, routers and end devices

roles [32] as well as unmanned aerial vehicles used to ensure connectivity of the network nodes and increase the capacity of communication channels in conditions of poorly predictable physical movement of the nodes.

Figure 1 schematically discloses the main devices of the analyzed prototype and information flows between them [18].

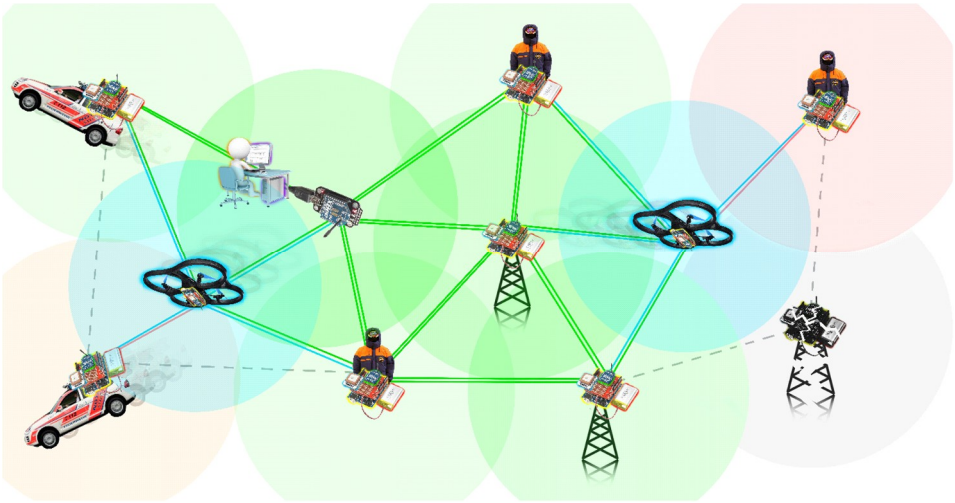

Figure 1. Self-organized wireless network.

Working without direct links to an external microcontroller, such as the Arduino Mega 2560, nevertheless an XBee module has possibilities for connecting some simple sensors, I/O user interfaces and actuators. As a result a network node is capable of operating from a local power supply, the key XBee configuration settings being stored in its nonvolatile memory. XBee is tuned for automatically taking readings of analog or digital input signals and their subsequent repeating passing to some node in the ZigBee network. The interval of sending data can be changed in a range of tenths of a second to several days. In addition, sending business data from an XBee can be initiated by changing the signal level on digital input pins.

An XBee supports a power-saving mode (sleep mode), which is especially important in case when the module is powered from the battery. This mode is oriented primarily on the XBee end devices, which only pass and receive their own business data and do not realize coordination function and routing. So, correctly setting the end device parameters (information exchange, transition of the module into sleep mode and wake-up) allows an XBee to run smoothly and seamlessly for up to several years.

An XBee allows setting a time interval t_X, which the module is in an idle state in. After finishing t_X, the module goes into the sleep mode for a time period t_Y. So it leads to XBee subjection to denial-of-sleep attacks. Generally, in the sleep mode all main XBee units and processes are switched off, excepting a timer, thereby it allows decreasing the current energy expenses up to hundredths of a mA.

During the sleep an XBee cannot receive and send radio packets and perform data communication through the UART (Universal Asynchronous Receiver/Transmitter) interface. However a message sent to the sleeping XBee wirelessly will not be lost—it is stored in a buffer at the parental device and waits for the end of the sleep period to be passed again.

Apart from denial-of-sleep impacts the grows of wireless traffic generated by a compromised or false XBee node as well as quite universal attack on creation of electromagnetic interference are of great significance. Abnormal software usage attack has fairly limited application to a standalone XBee due to ability of an intruder to change some XBee configuration settings only.

On the basis of the proposed (in Section 3) intruder model, representing the knowledge of typical types of ERE attacks, let us assess the possible types of these attacks for the two mentioned use cases and identify the most significant ones.

The factors determined in the model allow us to obtain a qualitative assessment of the criticality of each ERE attack in its application to the use cases UC1 and UC2 (see Table 5).

Table 5. Energy resources exhaustion (ERE) attack criticality.

Use Cases UC_1, UC_2	**$Attack_1$ (Denial-of-Sleep)**	**$Attack_2$ (Traffic)**	**$Attack_3$ (Jamming)**	**$Attack_4$ (Misuse)**
G → O (correspondence of the attack goal to the attack object)	**2** (the devices operate in two modes and switch between them, depending on the business functionality)	**2** (according to the scenario, large portions of data can be transmitted between devices occasionally)	**2** (all communications take place wirelessly)	**2** (the mobile communicator is based on the mobile operating system, the network node is based on a firmware. They both are with various settings that affect power consumption)
S (complexity of actions A of the attack)	**2** (successful/ unsuccessful authorization attempts, ping requests, etc.) (types 1,2 intruders)	**0–1** (the need to access one of the network devices to generate traffic to this node or to introduce a false node into the network to perform man-in-the-middle or man-in-the-end effects) (types 1,2 intruders)	**2** (relative ease of operation with appropriate equipment) (type 2 intruder)	**0** (the need for direct access to the device software) (types 1–4 intruders)
R (resources, tools)	**2** (minimum equipment needed) (level 1 intruder)	UC1: **1** (publicly available equipment) UC2: **0** (special equipment) (levels 1,2 intruders)	**1** (availability of prepared equipment for generating electromagnetic interference) (levels 1,2 intruders)	UC1: **1** (publicly available equipment) UC2: **0** (special equipment) (levels 1–3 intruders)
E (expected effectiveness)	**2**	**2**	**2**	**2**
P (attack stealthiness)	**2** (it is difficult to distinguish small portions of normal and abnormal traffic)	**2** (it is difficult to distinguish large portions of normal and abnormal traffic)	**1** (the presence of interference is easy to establish, but it may be difficult to establish that it is an attack)	0-2 (it depends on the specific type of misusage)
Sum	**UC1: 10 UC2: 10**	**UC1: 7–8 UC2: 6–7**	**UC1: 8 UC2: 8**	**UC1: 5–7 UC2: 4–6**

Table 5 exposes the following factors:

(i) the correspondence of the attack goal G to the attack object O ('G → O');
(ii) the complexity S of the attack actions A;
(iii) resources and tools R needed by the attacker;

(iv) the expected attack effectiveness E;
(v) the attack stealthiness P.

The values of the factors are determined by experts on a three-point scale: 0 means the value of the factor is small, 1—the value of the factor is medium, 2—the value of the factor is high.

Note that here E means the expected effectiveness of an ERE attack that is based on its a priori assessments, and generally E can be refined empirically.

In Table 5 the corresponding cells contain the justification for the determination of the primary values of individual factors. As a result, a cumulative account of all the factors considered shows the highest criticality of denial-of-sleep attacks for both use cases, so we investigate this type of attacks more in detail experimentally in the further section.

5. Experimental Results

On an Android 5.1-based LG Nexus 5 we demonstrated an attack of the forced switching a mobile device to a more energy consuming mode by using its wireless interface. We simulated an attack through a Bluetooth module by Kali Linux tools. We used *Bluetoothctl* to detect the target device and get its details, after that *l2ping* was used to sequentially send ping requests. Figure 2 depicts the attack trace.

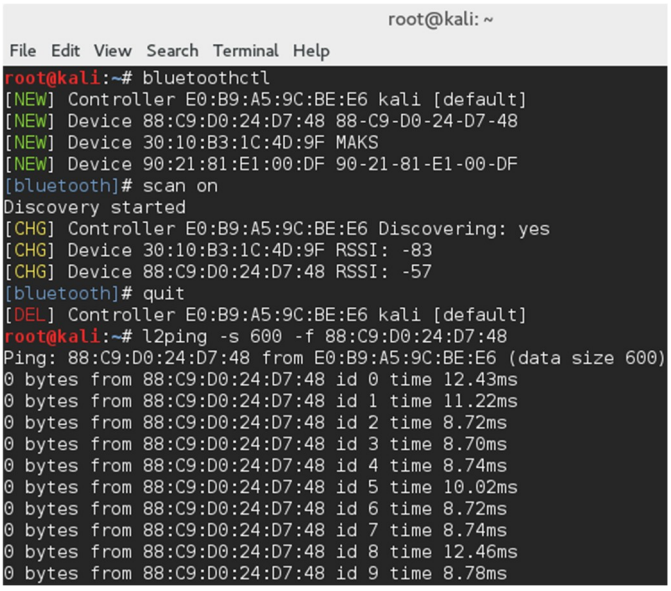

Figure 2. Tracing of vector of ERE attack on the Nexus 5.

In the experiment, the energy consumption measurements were carried out in a normal device mode and under the attack. In both cases the measurement data were obtained immediately after a complete pre-charging the device during 4 h. Excepting the cellular communication module and Bluetooth the other core ones such as other network elements and the screen were switched off during the experiment. Neither exterior device manipulations nor operating system or any application update were performed.

Battery consumption data were obtained programmatically by reading values of *BatteryManager.EXTRA_LEVEL* variable, presenting the charge level. The energy measurement results with 20 min scale are demonstrated in Figure 3.

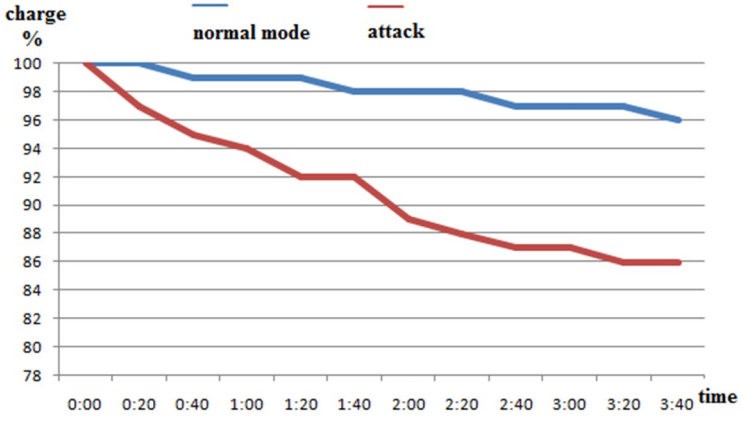

Figure 3. Evaluation of the effectiveness of ERE-attack on the Nexus 5.

The attack efficiency was calculated as a ratio of a charge changes under the attack and in a normal mode by the end of the measuring time gap. Although this technique allows explicitly programmatically obtaining attack efficiency, generally it is not precise enough. In particular the fall of the charge level by 1% does not always mean a real reduction of the accumulated energy on certain fixed amount. Alternatively one could use software profilers that allow getting more detailed data on power consumption, however these can be quite energy consuming and result in distortions as a side effect. In addition not all smartphones have built-in current sensors with access to their data through an application programming interface. Thus the hardware based energy measurement when technically possible is seen as the more promising and demonstrated in the next use case.

In the experiments we demonstrated a mixed attack on XBee (target end node) operating in energy saving mode scheduled at specific intervals. The attack is simulated by passing requests from a fake XBee (Attacker Node End). On the target XBee, the following power saving parameters were set, namely SM = 4 (cyclic sleep mode), ST = 1000 msec (time before sleep), and SP = 10,000 msec (cyclic sleep period). The attacker accomplishes periodical passing data to the target node (2 per sec.). Such data resets the ST timer, not allowing the node to go back to the sleep mode (i.e., denial-of-sleep attack). The mixed nature of this attack is that, apart from hampering the XBee movement to the sleep mode, some additional energy consumption is fulfilled also as a result of data reception instead of the XBee being in the idle mode (i.e., attack of wireless traffic increasing). Figure 4 discloses the diagram of the test bench simulating such kind of the attack.

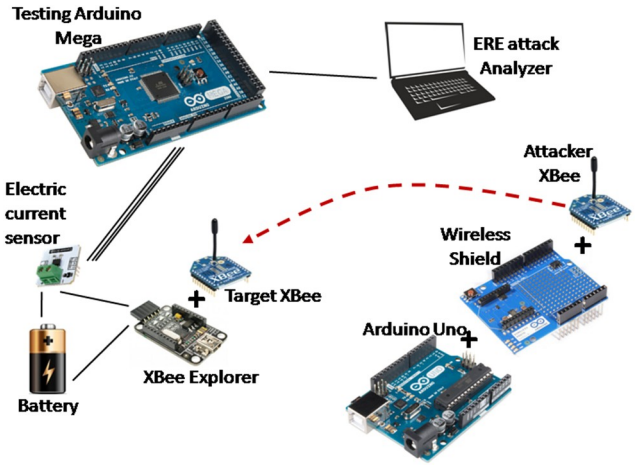

Figure 4. Diagram of the test bed for simulating ERE attack on XBee.

The object of the attack is Target XBee of an end device role. It operates from an autonomous power source, and is measured by an Allegro ACS712 circuit (Allegro & Sanken Semiconductors,

New York, NY, USA) based current sensor. An extra chip implementing end device business logic is connected to the XBee. The sensor readings are taken by a testing microcontroller Arduino Mega 2560 and passed to the PC via the UART interface in the form of logs for subsequent processing and evaluation. The malicious node represents an Arduino Uno R3 linked to an XBee via a Wireless Shield. The Uno firmware contains a sketch regularly sending data to a specified ZigBee destination address.

The current consumption measurements in the idle mode regularly changed by the sleep mode for SP period as well as energy consumption undo the attack are represented in Table 6. These are the mean data for one wakefulness loop of 1sec activity and sleep during 10 sec.

Table 6. The results of the XBee power consumption in normal mode and under attack.

Time Period, msec	0–1000	1000–11,000
I_{IDLE}, mA	45	8
I_{ATTACK}, mA	51	51

Under the conditions assuming that the attack is carried out uniformly, with the same intensity along its entire length, the wasting current during the modeled attack of a constant intensity is calculated as a constant value I_{ATTACK} = 51 mA, whereas in the sleep mode it is 8 mA. The attack effectiveness is expressed by:

$$E = I_{ATTACK} \cdot (t_2 - t_1) / \int_{t_1}^{t_2} I_{IDLE}(t)dt, \quad (2)$$

where the consumption in the idle mode I_{IDLE} is calculated as a mean value by the Lagrange interpolation method. The experiment was performed repeatedly over the time period t_2 - t_1 = 600 sec. The effectiveness E = 4.488 indicates that an attack more than 4 times faster exhausts the battery life of the XBee node.

6. Discussion

Generally, ERE attacks are applicable to devices using autonomous exhaustible power sources. The experiments have confirmed the potency of ERE attacks to reduce the lifetime rapidly. The variability of such attacks is limited by a variety of influences on more energy-consuming units to increase the intensity of their use. At the same time, ERE attacks make sense only if the device has a critical purpose and its business functions cannot be suspended to recharge the battery. Such attacks lose effectiveness if the drained device or the battery can be replaced rapidly. ERE attacks are seen as extremely important in various application domains. In particular, realizing an ERE attack on an unmanned aerial vehicle (drone) allows exhausting implicitly its energy used by the engine, raising a risk the owner of the drone will not have enough time to land in an emergency and the drone will crash.

Another example presents autonomous modules of a Smart City, such as mobile interactive road signs/traffic lights, pollution sensors, etc. being attacked by a dishonest competitor to cause to frequent maintenance and extra expenses during the system management. The assumed intruder's skills and knowledge on the devices (e.g., sleep mode settings, victim identifier, XBee PAN ID, encryption key used, etc.) are application specific. Performed experiments on the modeling of two attacks for different devices show the strength of the ERE attacks to reduce the life time of battery of devices several times, which is quite important for mission-critical systems.

ERE attack detection appears to be an application-specific intelligent process, including detailed monitoring data on power consumption of the device, its software and hardware modules transitions between specific modes, logs on starting and suspending applications, local storage calls, etc. All these data should be used to analyze events and verify feasibility of correlation rules to detect signs of ERE attacks.

Detection should be specific to the expected ERE attack type. In particular for an attack of a wireless incoming traffic growth, the traffic should be validated for its legitimacy, starting from its source, application protocol, other header and payload, considering the history of interaction. ERE attack monitoring is application-specific as well. The use cases expose differences in current consumption measurements by software and hardware means having inherent limitations and precision.

ERE attack detection can be energy consuming itself according to developers of cyber-physical systems. Generally hardware based measurements are regarded as less power consuming, more customizable and more exact; however it may be more difficult to implement it due to the need of soldering the current sensor to the battery contacts physically.

The discussed instances of attacks as well as their complexity can significantly differ by amounts of prior intruder's knowledge of the victim device and specific applications running on it. For instance, for XBee based devices such information may include sleep mode parameters (SM, ST, SP, etc.), the unique 64-bit address of the victim host, the network PAN ID, symmetric encryption key (if used), etc.

Let us analyze the practical applicability of the four types of energy exhaustion attacks considered:

- Denial-of-sleep attack. This type of attack is specific to stand-alone or autonomous modules moving in space, including modules with long-term functioning—for example, terminal nodes of the sensor network, BodyNet elements, wireless devices. communications, etc., assuming an ability to activate core computing and communication functions sporadically when a certain type of event occurs.
- Growth of wireless ongoing or outgoing traffic on a device. This type of attacks is specific to autonomously working devices and modules in the field of wireless communication, involving the receipt and transmission of digital multimedia content. The volume of traffic transmitted is determined by semantic rules of a particular application area, which are rather difficult to validate by automated means on particular traffic patterns.
- Creation of electromagnetic interference on wireless channels, causing an increase in transmitter power. This type of attack is specific to components of receiving/transmitting wireless devices, including those capable of dynamic self-organization and rebuilding, as well as physically moving in space with varying relief, presence of natural or artificial obstacles and other factors that can affect the availability, speed and quality of communications between individual devices. An example of such systems is a system for ensuring operational management and response in emergency and crisis situations. The system is deployed and rebuilt on the ground to ensure reliable and secure communication between devices of rescue service by using ZigBee, LoRa (Long Range), and other mesh protocols. At that, the situational nature of the structure and composition of the self-organized communication network provides the possibility of alternately increasing and decreasing the power of the receiving/transmitting components of the devices, balancing between raising the signal to meet communication requirements and reduce its power to minimize the energy expenses. As a result, there is a need to monitor the validity of a possible increase of the transmitter power of the autonomously operating network nodes.
- Untypical usage (misuse) of a devices' software, including forcing incorrect settings and others. This type of attack is typical in multi-task devices—smartphones, laptops, etc.—assuming the possibility of background running of software applications, running hidden computing processes, deploying local data storages and other capabilities that are potentially suitable for their exploitation by an intruder to deplete energy. In addition, the choice of "non-optimal" trajectories and automatic ways to move unmanned aerial vehicles with unjustified hangs, speed acceleration and slowdown and other features can also adversely affect the battery consumption of the drone and reduce the maximum technically achievable time of its flight.

7. Conclusions

In the paper we have considered a general framework intended to model and analyze energy resources exhaustion attacks, including analysis of possible types of attacks on cyber-physical devices, an intruder model and experimental studies on the modeling and evaluation of attacks.

The paper contains simulation and evaluation of ERE attacks on two cyber-physical case studies—fragments of cyber-physical systems having limited energy resources. These use cases differ in specificity of particular expert knowledge used, including details of the attacked devices, wireless protocols and ways to analyze energy consumption.

The experiments have demonstrated the possibility of modeling ERE attacks both analytically and on real microcircuits of a particular scenario to develop application specific security components against such attacks.

Moreover, ERE attack modeling could be introduced into already existing complex techniques of creation and improvement of secure embedded devices [33,34].

Having researched some common regularities of ERE attacks both by analytical approach to deduce conditions of ERE attacks and empirically to measure the effectiveness on physical equipment, we are planning to concentrate on ERE attack-detection techniques by means of machine learning in specific application domains.

Author Contributions: V.D. constructed the models and designed the experiments; I.K. developed the use cases, surveyed the state-of-the-art and generalized experimental data. D.Z worked with experimental data and analyzed them. All authors wrote the paper.

Funding: This research is being partially supported by the grants of the RFBR (projects No. 16-29-09482, 18-37-20047, 18-07-01488, 18-07-01369, 18-29-22034 and 19-07-00953), by the budget (the project No. 0073-2019-0002), by Government of the Russian Federation (Grant 08-08) and Grant of President of Russia No. MK-5848.2018.9.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Farzana, T.; Babu, A. A light weight PLGP based method for mitigating vampire attacks in Wireless Sensor Networks. *Int. J. Eng. Comput. Sci.* **2014**, *3*, 6888–6895.
2. Sharma, M.K.; Joshi, B.K. Detection & prevention of vampire attack in wireless sensor networks. In Proceedings of the 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC), Indore, India, 17–19 August 2017.
3. Patel, A.A.; Soni, S.J. A Novel Proposal for Defending against Vampire Attack in WSN. In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015.
4. Goudar, C.P.; Kulkarni, S.S. Mechanisms for Detecting and Preventing Denial of Sleep Attacks and Strengthening Signals in Wireless Sensor Networks. *Int. J. Emerg. Res. Manag. Technol.* **2015**, *4*, 263–269.
5. Palmieri, F.; Ricciardi, S.; Fiore, U.; Ficco, M.; Castiglione, A. Energy-oriented denial of service attacks: An emerging menace for large cloud infrastructures. *J. Supercomput.* **2015**, *71*, 1620–1641. [CrossRef]
6. Raymond, D.R.; Brownfield, M.I.; Marchany, R.C.; Midkiff, S.F. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. *IEEE Trans. Veh. Technol.* **2009**, *58*, 367–380. [CrossRef]
7. Chen, C.; Hui, L.; Pei, Q.; Ning, L.; Qingquan, P. An effective scheme for defending denial-of-sleep attack in wireless sensor networks. In Proceedings of the IEEE Fifth International Conference on Information Assurance and Security, Xi'an, China, 18–20 August 2009.
8. Capossele, A.T.; Cervo, V.; Petrioli, C.; Spenza, D. Counteracting Denial-of-Sleep Attacks in Wake-Up-Radio-Based Sensing Systems. In Proceedings of the 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), London, UK, 27–30 June 2016.

9. Mostafa, M.S.; Banerjee, T.; Hasan, M.A. Energy Exhaustion Attack on Barrett's Reduction. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018.
10. Karpagam, R.; Archana, P. Prevention of Selective Jamming Attacks Using Swarm Intelligence Packet-Hiding Methods. *Int. J. Eng. Comput. Sci.* **2013**, *2*, 2774–2778.
11. Periyanayagi, S.; Sumathy, V.; Kulandaivel, R. A Defense Technique for Jamming Attacks in Wireless Sensor Networks Based on Sensor Networks. In Proceedings of the International Conference on Process Automation, Control and Computing, Coimbatore, India, 20–22 July 2011.
12. Boubiche, D.E.; Bilami, A. A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks. *J. Emerg. Technol. Web Intell.* **2013**, *5*, 18–27. [CrossRef]
13. Moyers, B.R.; Dunning, J.P.; Marchany, R.C.; Tront, J.G. Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices. In Proceedings of the 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 5–8 January 2010.
14. Buennemeyer, T.K.; Gora, M.; Marchany, R.C.; Tront, J.G. Battery Exhaustion Attack Detection with Small Handheld Mobile Computers. In Proceedings of the IEEE International Conference on Portable Information Devices, Orlando, FL, USA, 25–29 May 2007.
15. Racic, R.; Chen, D.M.; Chen, H. Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery. In Proceedings of the 2006 Securecomm and Workshops, Baltimore, MD, USA, 28 August–1 September 2006.
16. Shakhov, V.; Koo, I. Depletion-of-Battery Attack: Specificity, Modelling and Analysis. *Sensors* **2018**, *18*, 1849. [CrossRef] [PubMed]
17. Guo, Z.; Harris, I.G.; Jiang, Y.; Tsaur, L. An efficient approach to prevent Battery Exhaustion Attack on BLE-based mesh networks. In Proceedings of the International Conference on Computing, Networking and Communications (ICNC), Santa Clara, CA, USA, 26–29 January 2017.
18. Desnitsky, V.; Kotenko, I.; Rudavin, N. Ensuring Availability of Wireless Mesh Networks for Crisis Management. *Int. Symp. Intell. Distrib. Comput.* **2018**, *798*, 344–353. [CrossRef]
19. Du, X.; Samachisa, A.; Hei, X.; Lukowiak, M. Defending resource depletion attacks on implantable medical devices. In Proceedings of the IEEE Global telecommunications conference (GLOBECOM 2010), Miami, FL, USA, 6–10 December 2010.
20. Bhattasali, T.; Chaki, R.; Sanyal, S. Sleep deprivation attack detection in wireless sensor network. *Int. J. Comput. Appl. (IJCA J.)* **2012**, *40*, 19–25, arXiv preprint arXiv:1203.0231. 2012. [CrossRef]
21. Desnitsky, V.; Kotenko, I. Machine Learning based Detection of Denial-of-Sleep Attacks in Wireless Sensor Networks for Crisis Management. In Proceedings of the 2018 IEEE XXI International Conference on Soft Computing and Measurements (SCM-2018), Saint Petersburg, Russia, 23–25 May 2018.
22. Fiore, U.; Palmieri, F.; Castiglione, A.; Loia, V.; De Santis, A. Multimedia-based battery drain attacks for Android devices. In Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2014.
23. Shin, S.; Lee, T.; In, H.P. Defending Battery Exhaustion Attacks on Mobile Systems. In Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, Seattle, WA, USA, 20–24 July 2009.
24. Jo, M.; Han, L.; Tan, N.D.; In, H.P. A survey: Energy exhausting attacks in MAC protocols in WBANs. *Telecommun. Syst.* **2015**, *58*, 153–164. [CrossRef]
25. Krishnan, M. Intrusion Detection in Wireless Sensor Networks. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.3793&rep=rep1&type=pdf (accessed on 25 February 2019).
26. Gelenbe, E.; Kadioglu, Y.M. Battery Attacks on Sensors. In Proceedings of the International Symposium on Computer and Information Sciences, Security Workshop, London, UK, 26–27 February 2018.
27. Ghildiyal, S.; Mishra, A.K.; Gupta, A.; Garg, N. Analysis of denial of service (dos) attacks in wireless sensor networks. *Int. J. Res. Eng. Technol.* **2014**, *3*, 2319-1163. [CrossRef]
28. Hsueh, C.T.; Wen, C.Y.; Ouyang, Y.C. A secure scheme against power exhausting attacks in hierarchical wireless sensor networks. *IEEE Sens. J.* **2015**, *15*, 3590–3602. [CrossRef]
29. Cao, X.; Shila, D.M.; Cheng, Y.; Yang, Z.; Zhou, Y.; Chen, J. Ghost-in-ZigBee: Energy depletion attack on ZigBee-Based wireless networks. *IEEE Internet Things J.* **2016**, *3*, 816–829. [CrossRef]

30. Rae, A.J.; Wildman, L.P. A Taxonomy of Attacks on Secure Devices. In Proceedings of the Australia Information Warfare and Security Conference, York, Australia, 20–21 November 2003; pp. 251–264.
31. Abraham, D.G.; Dolan, G.M.; Double, G.P.; Stevens, J.V. Transaction security system. *IBM Syst. J.* **1991**, *30*, 206–228. [CrossRef]
32. Digi XBee Documentation. Available online: https://www.digi.com/support/productdetail?pid=3430 (accessed on 25 February 2019).
33. Desnitsky, V.; Kotenko, I.; Chechulin, A. Configuration-based approach to embedded device security. In Proceedings of the International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, St. Petersburg, Russia, 17–19 October 2012; pp. 270–285.
34. Desnitsky, V.; Levshun, D.; Chechulin, A.; Kotenko, I. Design technique for secure embedded devices: Application for creation of integrated cyber-physical security system. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2016**, *7*, 60–80.