electronics

MDPI

Article

Countermeasuring MITM Attacks in Solar-Powered PON-Based FiWi Access Networks

Polyxeni Tsompanoglou [1], Antonios Iliadis [1], Konstantinos Kantelis [1] and Sophia Petridou [2] and Petros Nicopolitidis [1,*]

[1] School of Information Informatics, Aristotle University of Thessaloniki, 541 24 Thessaloniki, Greece
[2] Department of Applied Informatics, University of Macedonia, 546 36 Thessaloniki, Greece
* Correspondence: petros@csd.auth.gr

Abstract: Solar power (SP) passive optical network (PON)-based fiber-wireless (FiWi) access systems are becoming increasingly popular as they provide coverage to rural and urban areas where no power grid exists. Secure operation of such networks which includes solar- and/or battery-powered devices, is crucial for anticipating potential network issues and prolong the life of the network operation. Since optical network units (ONUs) may be powered by SP-charged batteries, energy awareness becomes an important issue, particularly when it comes to reducing ONUs' energy consumption and allowing them to operate in off-grid remote areas. With the PON as the fixed part of these networks, the optical line terminal (OLT) informs the ONUs through a message exchange mechanism when no traffic is present, allowing them to transition to a low-power-consumption sleep mode. However, man-in-the-middle (MITM) attacks pose a serious threat to the message exchange mechanisms, which can eventually drain the energy of battery-powered ONUs resulting in their shutdown. Consequently, this paper introduces two novel mechanisms for reducing ONU energy consumption, namely the *wake-up* and *time-out* mechanisms, which can be used to mitigate the effectiveness of MITM attacks that may seek to affect the unit's operation due to battery drain. The formal verification results show that these goals were effectively achieved.

Keywords: battery-powered optical network units (ONUs); energy saving; fiber-wireless (FiWi) access networks; man-in-the-middle (MITM); passive optical network (PON); solar power

Citation: Tsompanoglou, P.; Iliadis, A.; Kantelis, K.; Petridou, S.; Nicopolitidis, P. Countermeasuring MITM Attacks in Solar-Powered PON-Based FiWi Access Networks. *Electronics* **2023**, *12*, 1052. https://doi.org/10.3390/electronics12041052

Academic Editor: Christos J. Bouras

Received: 29 December 2022
Revised: 26 January 2023
Accepted: 17 February 2023
Published: 20 February 2023

1. Introduction

Renewable energy sources, including solar, wind, and geothermal, have already been integrated into domestic and utility power systems to reduce the carbon footprints and environmental degradation. As solar energy is easily available, it is the most commonly used form of renewable energy [1].

The ever-growing demand to provide broadband coverage to urban and rural regions may cause a significant increase in energy consumption, especially in rural areas, where the grid power supply is limited. Moreover, for sensor devices and Internet of Things (IoT) setups, power supply can be even more challenging, since environmental-monitoring IoT applications may be deployed in remote areas where no power grid is available [2–4]. In such grid-less installations, the power supply of the access points (APs) collecting data from sensors is a crucial issue [5]. Therefore, the exploitation of solar energy using photovoltaic (PV) technology, such as solar panels, is very crucial. From a networking point of view, a lot of capacity to satisfy the increasing bandwidth demands of numerous users and IoT devices. Thus, fiber-wireless (FiWi) networks are a perfect choice since they exploit both optical and wireless technologies for a large aggregate bandwidth and cordless deployment of sensors, respectively [6]. The architecture of a FiWi network contains a passive optical network (PON) backbone comprising a number of optical network units (ONUs) connected to APs and providing, through them, connectivity to a number of wireless sensors. In such

network setups, including devices that should operate in areas far from the power grid, renewable energy sources, mainly solar, have to be exploited to power their components, i.e., ONUs and APs.

However, apart from the energy issues, the security of such solar-powered (SP) FiWi networks' infrastructure is a significant issue as well, since they are typically deployed outdoors in remote areas. They can become targets of attackers who may want to disrupt network services and bring them down, thereby causing high repair costs [7]. Hence, energy awareness, as well as the security and secure operation of solar- and/or battery-powered devices that are vital parts of SP FiWi networks, is a real challenge that has to be addressed. Particularly, it is of fundamental importance in such networks that the battery operation characteristics of their devices should ensure online operation, overcoming various challenges. Predominantly, the battery capacity should ensure the uninterrupted functionality of the network system, taking into consideration the fluctuations of solar energy. During cloudy days, such a system may not be able to reach full battery capacity, resulting in possible power outages that should be avoided. Moreover, as such networks operate far from urban environments, they are prone to a range of attacks such as tampering and intrusions. Including, but not limited to, the man-in-the-middle (MITM) attack, which stands as one of the purposes behind tampering the physical devices of the premises of a SP PON network. Dictated by the fact that MITM attacks can result in network outages through denial of service (DoS) attacks, the presence of a communication protocol that could mitigate the results of this type of threat has become more and more of a necessity for modern SP PON-based FiWi networks.

In this paper we deal with the following problem. We consider an SP PON-based FiWi access network that consists of an OLT, a number of battery-powered ONUs and employs an ONU energy saving mechanism based on control message exchanges between OLT and ONUs. We also consider the presence of an attacker that intercepts the downstream communication and acts as a MITM aiming to attack the energy saving mechanism so as to drain the ONU's battery-based energy resources. We propose mechanisms to improve energy saving for the ONU in case of normal operation as well as proactively countermeasure attacks that aim to drain its energy resources.

The two proposed energy-aware mechanisms, namely the *wake-up* and *time-out* mechanisms, operate in the PON part of the network. We employ a formal verification analysis along with probabilistic model checking as a means to verify their energy impact. The main idea is to model these mechanisms on a SP PON-based FiWi network under a MITM attack and derive quantitative results that verify the improvements in ONU energy expenditure. Our analysis shows that both of them can effectively decrease the ONUs' energy consumption, while the latter can additionally countermeasure the battery drain caused by a MITM attack.

The rest of the paper is organized as follows. Section 2 discusses the importance and real-life applications of SP FiWi networks, related energy-aware studies regarding ONU devices, and the novelty of this work. Section 3 presents and describes the proposed energy-efficient mechanisms, namely the *wake-up* and *time-out*mechanisms, appropriate for SP PON-based FiWi networks. Preliminaries of formal verification are explained in Section 4. In Section 5 the model we designed is presented, while Section 6 discusses our quantitative verification results. Finally, Section 7 concludes the paper.

2. Background and Related Work

2.1. Solar-Powered Fiwi Networks

The implementation of green cellular networks, which are mainly powered by renewable resources, such as solar energy, has increased during the past several years [8]. Initially, the operators used diesel generators as a solution to power the networks' equipment placed in remote areas. The next move was to replace diesel-generated electricity with solar-powered, due to the high operational cost to run and maintain diesel generators at remote cell sites. Thus, SP cellular base stations (BSs) have emerged as a common solution

to power off-grid base stations and reduce their carbon footprint [9]. It is worth mentioning that approximately 43,000 such off-grid BSs have been deployed in locations such as Africa, India, South America, and the Caribbean with predictions of showing an annual growth of up to 30% in their usage due to the increased deployment of equipment in locations where power outages are frequent, and grid power is lacking [10].

This trend is very active nowadays. Indicatively, Deutsche Telekom and Ericsson test autonomous energy supply for remote areas aimed at reducing carbon footprints and saving energy costs. They have used small solar modules placed at mobile sites with a power system to handle maximum power point and voltage conversion, and a management system to control the radio access network (RAN). Moreover, Deutsche Telekom has been sourcing its electricity exclusively from renewable energies, while Ericsson supports the goal of reducing CO_2 emissions by 90% until 2030 enabling innovative telecommunication infrastructure and becoming climate neutral in its own activities [4].

In addition, there is an increasing trend toward using renewable energy to power equipment in FiWi networks. Figure 1 shows the FiWi architecture of an integrated solar-powered solution, including a PON at the fiber back-end and energy-efficient macro base stations at the wireless front-end. An optical line terminal (OLT) residing at the central office of the service provider is connected to several battery-powered ONUs, which can only be powered using solar panels and batteries in the field. A feeder fiber that is subsequently split using a 1:N optical splitter enables the battery-powered ONUs to connect [5,11]. The power system of a macro BS consists of a PV solar panel for energy production, a battery for the energy storage produced by the solar panel, and a controller unit that manages the energy that comes from the solar panel and the battery. A solar panel is also placed to power each ONU. SP wireless sensor nodes are connected to the ONUs through a macro-BS.

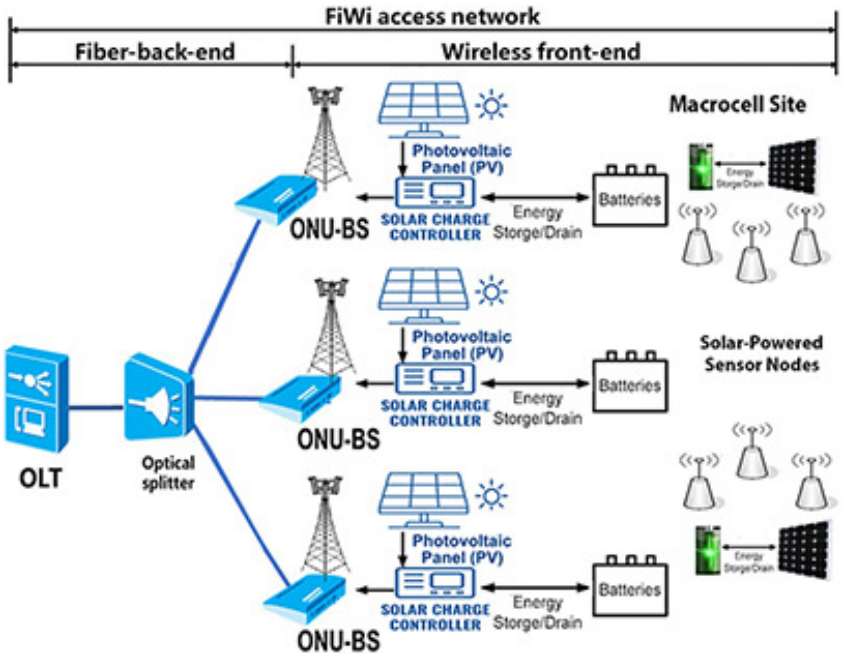


Figure 1. Solar-powered PON-based FiWi network architecture.

Solar-powered wireless sensors could be connected to a controller to deliver real-time data for environmental monitoring, such as temperature, wind speed, humidity, period of sunlight, or geological monitoring (e.g., volcanoes), where human presence is not always possible. For example, Sierra Electronics merchandises a solar-powered wireless sensor that measures the flow of traffic to determine if there is a traffic jam or to make a forecast of the traffic conditions [12].

Numerous off-grid monitoring and automation applications in the industry, whose locations range from mountaintops to mines, could adapt such an architecture, e.g., oil

and gas production, well and tank monitoring, leak detection, and compressor stations to desert installations. Indicatively, an off-grid integrated solution including an automation platform that supports remote monitoring and control applications using solar panels, durable batteries, a charge controller, wireless networking, and efficient electronics is described in [3]. For network connectivity, the automation platform establishes a cloud-based communication with local wire or Wi-Fi networking or optical fiber by cellular capability through LTE or GSM.

2.2. Related Work

Solar-powered PON-based FiWi access systems have fast spread to remote areas where the grid power supply is not available. Since ONUs are battery-charged by solar power in such types of networks, reducing the ONUs' power consumption is essential in order to run continuously in such isolated areas [13].

To reduce the ONU's power consumption, a number of energy-efficient mechanisms have been proposed in the literature by exploiting the sleep mode of operation. According to the [14] International Telecommunication Union (ITU-T) G.987.3, the reduction in ONU's power consumption in GPONs is achieved by using cyclic sleep and doze sleep modes. In [2], the authors suggest three different deep sleep approaches for drastic power reduction in which almost all the ONU's components, including its chip (system on chip-SoC) are turned off. The technique of fast sleep mode is presented by the authors in [15] and offers energy saving by turning the ONU off for a certain period. A software-defined ONU energy-saving mechanism assigns a sleep duration to the receiver and a wake-up threshold to the transmitter [16]. This mechanism reduces the ONU's transmitter's active time by up to 98%, reducing energy consumption. To provide energy efficiency, the authors in [17] focus on the modeling of the watchful sleep mode with different sleep period variation patterns applied to multiple ONUs. In addition, the authors in [18,19] propose a new aggressive policy by defining long sleep periods considering quality of service (QoS) constraints and highlighting the impact of the non-active periods on the trade-off between energy saving and QoS in Ethernet PONs (EPONs), respectively. The deep sleep technique applied to an ONU with a backup battery is described in the work of [20]. The implementation of such mechanism increases energy efficiency, and as a result, the battery lasts longer to provide reliable phone services.

Nevertheless, such energy-efficient mechanisms that are based on a control message exchange between the OLT and the ONU, are vulnerable to MITM attacks [21]. In the case of SP PON-based FiWi networks, bypassing an energy-efficiency mechanism causes the battery-powered components to be turned into large energy-consuming devices and the ONU's batteries to drain quickly, leading to an ONU shutdown and inevitable service denial. In practice, this is feasible if an attacker connects a malicious device to the PON infrastructure, which is capable of intercepting and generating traffic that impersonates the legitimate OLT. This is explicitly referenced in the recommendation G.987.3 of the ITU-T for the XG-PON standard [22]. This problem is aggravated by the fact that, according to the standard, only the authentication of an ONU by the OLT is mandatory, and mutual authentication between the OLT and an ONU is optional, depending on the operator's discretion [22]. This problem has also been brought to attention by Telecom Italia [23], which noted that an attacker could tamper with the fiber cable that connects an ONU with the splitter, and set up a fake OLT device. Therefore, the ONU cannot detect the fake OLT. Once the fake OLT connection is established, the attacker operates the device in "promiscuous mode", to eavesdrop sensitive system information such as logical link identification (LLID) and media access control (MAC) addresses. Having sufficient knowledge of PON hardware, the attacker joins the network and pretends to be a legitimate ONU to launch a MITM attack.

Table 1 summarizes a brief comparison between the proposed work and the most relevant ones. In the first column, a number of features are listed and, then, each cell provides information that exhibits the differences of the related studies to the current one according to that features. The articles on Table 1 are considered as relevant since they share

the study of energy issues (first row) as common feature. However, the security issues feature still needs to be considered. The work of [21] is the only that addresses this aspect of network operation. Further, the model checking approach is considered only in [18] and [21], whereas all of the papers use different mechanisms. Therefore, this paper, fills this research gap by (a) countermeasuring a potential MITM attack at the optical side of a SP PON-based FiWi network, and (b) proposing two energy-efficient mechanisms between the OLT and the ONUs, using a model checking approach.

Table 1. Comparison of related works with respect to the main features of the current work.

Features	[2]	[15]	[16]	[18]	[21]	**Our Work**
Energy issues	✓	✓	✓	✓	✓	✓
Security issues	×	×	×	×	✓	✓
Evaluation approach	Simulation	Simulation	Simulation	Model checking	Model checking	Model checking
Mechanism	Deep sleep	Fast Sleep	Software-defined mecha-nism	long sleep periods	OLT-triggered sleep request	wake-up and time-out

2.3. Contribution

Motivated by the vulnerability of the energy-efficient mechanisms to MITM attacks and the initial findings of its impact by [21], in this article, a MITM attack in a solar-powered PON-based FiWi network is assumed, where a fake OLT compromised legitimate OLT-ONU communication to drain the energy reserves of the ONU's battery, and as a consequence to interrupt the user's connection from network services and achieve Denial-of-Service (DoS). According to this scenario, the aim of this work is to introduce a formal analysis approach to evaluate the energy impact of two proposed energy-efficient mechanisms inspired by [21,24]. The novelty of this paper is summarized as follows:

1. The *wake-up* mechanism that decreases the time needed for the OLT to successfully transmit the downstream data packets to the ONU is proposed, since the latter is notified by the OLT to transit in active mode when traffic is buffered in the downstream queue. When no down/up stream traffic exists, the ONU transits to sleep mode, and, thus, it decreases its energy consumption.
2. The *time-out* mechanism that proactively countermeasure a MITM attack aiming to drain energy resources from a battery-powered ONU is introduced. The mechanism contributes to decreasing the time the ONU is in the active mode by forcing it to leave this energy consuming mode once a *time-out* interval period has expired.
3. A formal analysis approach that models a SP PON-based FiWi network under a MITM attack is proposed, including the aforementioned mechanisms.
4. It is verified that the two proposed mechanisms improve energy efficiency and can be used to effectively countermeasure a MITM attack in a SP PON-based FiWi network without increasing the model's computational time. In addition, the trade-off between energy consumption and packet delay for different *time-out* mechanism intervals is also presented.

3. Improving Energy Efficiency in a Solar-Powered Fiwi Access Network

In this paper, we design and evaluate two energy-aware mechanisms to study the energy-efficiency of a SP PON-based FiWi network: (i) the *wake-up* mechanism, in which the optical line terminal (OLT) sends a *wake-up* message to the ONU to receive downstream traffic once the latter has completed the listen or sleep cycle; (ii) the *time-out* mechanism, which notifies

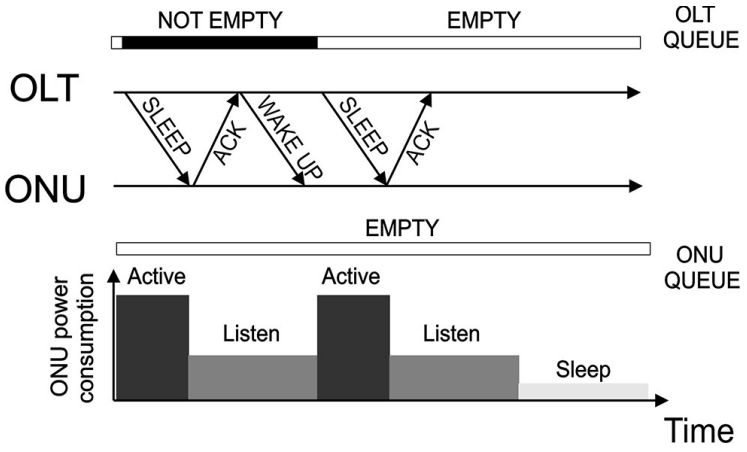
the ONU to transit to the listen and sleep modes when no *sleep* request message has been received for a pre-defined interval period, i.e., an indication of a MITM attack.

In more detail, the ONU has three different modes of operation, *active*, *listen*, and *sleep*, where the energy consumption of each power mode is 3.85 W, 1.28 W, and 0.75 W, respectively, according to the work of [21]. Both ONU and OLT have their own upstream and downstream queues, respectively, and exchange their traffic. Assuming that the ONU is currently in active mode, our baseline mechanism [21] dictates that once the OLT queue is empty, the OLT should send a *sleep* request message to the ONU. When the ONU receives the request, it replies with an *ack* message if the ONU queue is empty and transits to the listen mode, or with a *nack* message if it is not, and stays in the active mode to proceed with data transmission.

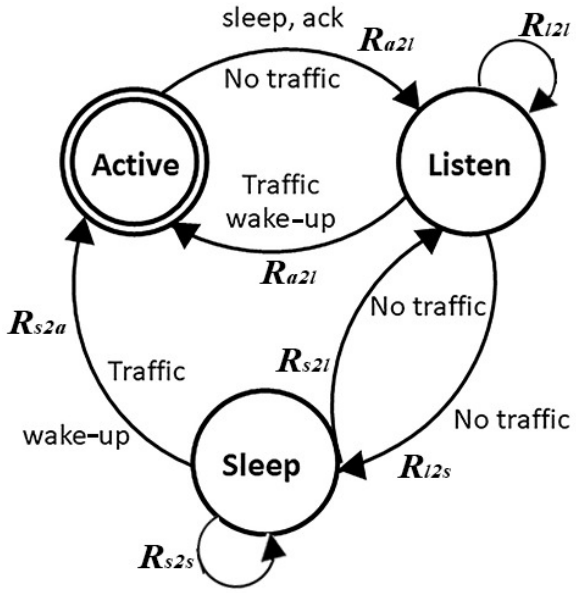
Figure 2a depicts the idea of the *wake-up* mechanism, which complements the aforementioned baseline mechanism to achieve higher energy saving for the ONU. More precisely, once the ONU replies with an *ack* message, the ONU will transit to the listen mode. While in listen mode, all downstream traffic is buffered in the OLT's queue. If any upstream traffic appears during the listen mode, the ONU will transit to the active mode and transmit it. Once the listening cycle has been completed, the ONU will receive a *wake-up* notification message from the OLT in case downstream traffic appears during its listening cycle; thus, it returns to the active mode in order to receive that downstream traffic. If neither downstream traffic has appeared in the OLT's queue nor upstream traffic has appeared in ONU's queue during ONU's listening cycle, the ONU will not receive any *wake-up* message and will, thus, transit to the sleep mode.

The ONU sleep mode cannot be interrupted, and as a result, both the OLT and the ONU will buffer their packets until the ONU completes the sleep cycle. There are three possible transition choices once the ONU's sleep cycle expires: (i) if upstream traffic has arrived in the ONU's queue during its sleep cycle, the ONU will transit to the active mode to serve it; (ii) if downstream traffic has arrived in the OLT's queue during ONU's sleep cycle, the ONU will receive a *wake-up* message to transit to active mode in order to receive this traffic; and (iii) if neither upstream nor downstream traffic appears during the ONU's sleep cycle, the ONU will transit to the listen mode.

Figure 2b shows how the ONU can transit among the active, listen, and sleep states following the *wake-up* mechanism. Transitions among the ONU states are identified by the messages exchanged between the OLT and ONU using the labels *sleep*, *ack*, or *wake-up*, while the traffic within the queues is identified by either the label "Traffic" or "No traffic". Furthermore, the ONU's transition rates between the active, listen and sleep power modes are presented, where notation $R_{x2x'}$ expresses the transition rate from state x to x'. The time period d_{state} specifies the rate to stay in the state, i.e., $R_{x2x} = 1/d_{state}$. In more detail, as d_{listen} specifies the time period to remain in the listening state, the rate $R_{l2l} = 1/d_{listen}$ is used. This means that if the listen period is too long, the energy saving would be deteriorated, and if the listen period is too short, the ONU would be forced to make early transitions to sleep, which would increase the packets' delay. In addition, the rate at which we remain in sleep state can be expressed as $R_{s2s} = 1/d_{sleep}$ for a period of d_{sleep} duration. The trade-off under consideration is significantly influenced by the length of the sleep period because short sleep periods increase packet delay but reduce overall energy savings. In this work, we derive the d_{listen} and d_{sleep} values from our previous analysis [18]. However, both of them can be configured according to the problem under investigation, since they are parameters in the model.



(**a**) Message exchange



(**b**) ONU transitions

Figure 2. Message exchange of the energy-aware mechanism and ONU transitions between its states while using the Wake-up mechanism.

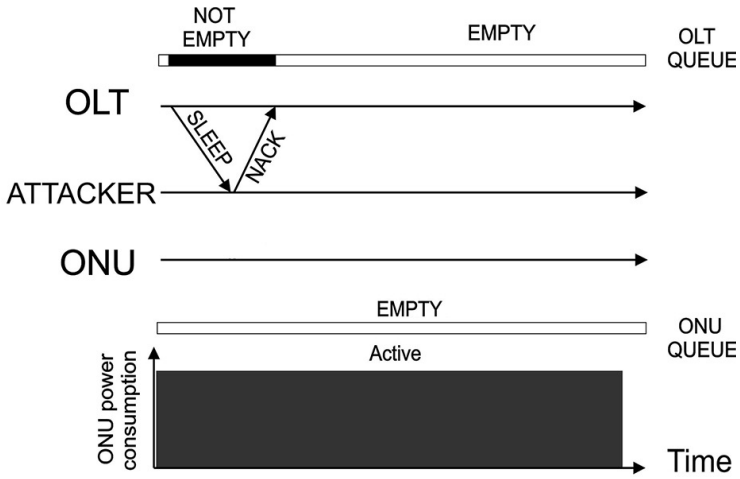
The transition times for ONU's state transitions derived by [18] are presented in Table 2. As shown in Table 2, transitions from active to listen mode is of the nanoseconds' order and, thus, the corresponding transition rate, R_{a2l}, and as with R_{a2l}, the rateR_{l2a} is not taken into account in the model. Further, the table shows the transition time needed between listen to the sleep mode. When the listen period expires, the ONU transits to the sleep mode with rate $R_{l2s'}$ in 2.88 µs, which is the time required by the ONU to turn off its transceiver. Finally, the transition time from sleep to active mode is shown. In the event that d_{sleep} expires, the ONU transits to the active mode with rate R_{s2a}, which requires a significant amount of time, i.e., 2 ms, in order to turn on its transceivers and to synchronize with the network [19].

Table 2. Average transition times for ONU state transitions derived by [18].

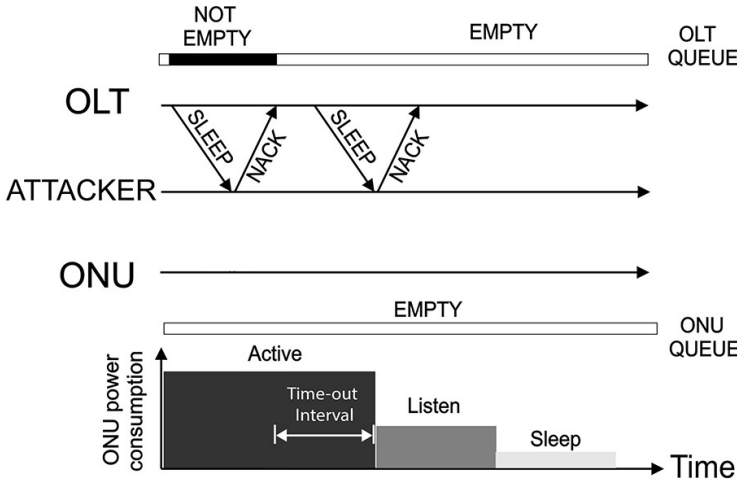
States	Active	Listen	Sleep
active	-	*ns*	-
listen	*ns*	d_{listen}	2.88 µs
sleep	2 ms	2 ms	d_{sleep}

Since PONs are vulnerable to attacks because of their broadcasting architecture, we assume that a MITM attack, which is inspired by the work of [21], disrupts the operation of the *wake-up* mechanism. Figure 3a shows that an attacker stands between the OLT and the ONU, intercepts the OLT's sleep requests meant for the ONU and replies steadily with a *nack* message in order to force the ONU to stay in the energy-consuming active mode. In the case of a battery-powered ONU, the attacker can successfully execute a DoS attack. Our way to countermeasure such attacks is by applying the *time-out* mechanism, as shown in Figure 3b.

We define a *time-out* interval period that resets every time: (i) the ONU receives downstream traffic from the OLT, (ii) the ONU transmits upstream traffic to the OLT, and (iii) the ONU receives a sleep request from the OLT. If the ONU does not receive or transmit any traffic nor receive any sleep request during this interval period, it transits to the listen mode. Namely, no activity during the *time-out* period operates as an alarm indication, which protects ONU's energy levels by forcing it to leave the active mode.



(**a**) Message exchange without *time-out* mechanism.



(**b**) Message exchange with proposed *time-out* mechanism.

Figure 3. Message exchange of the energy-aware mechanism proposed in [21], as well as when using the *time-out* mechanism.

Considering the ONU's power consumption in active, listen, and sleep modes, the two suggested mechanisms contributed to the reduction in the ONU's energy consumption, which entails energy efficiency improvement on a SP PON-based FiWi. Figure 2a shows that the ONU wakes up, by receiving the *wake-up* message sent by the OLT and transits to active mode only when downstream traffic appears. Otherwise, it does not receive it,

and, thus, it transits to the listen mode, and then to the sleep mode, reducing its power consumption. Moreover, in Figure 3a, the ONU increases its power consumption since the attacker forces the ONU to stay in active mode [21].

On the contrary, the proposed *time-out* mechanism acts as a guard time and prevents energy exhaustion for the ONU. While the ONU's queue is empty, the device change to the listen and sleep mode successively. Due to the *time-out* interval, the ONU is not deceived by the attacker's *nack* messages, and it transits to the listen mode and eventually to the sleep mode, as shown in Figure 3b. Thus, it reduces its energy consumption since it stays for less time in the active mode. That way, the system avoids the service outage and countermeasures the attack.

The proposed mechanisms do not increase the computational overhead of the system implementation. The mechanisms employ only control message exchanges, which does not require any additional computation. The main addition is related to the existence of a timer that fires the next transition without the use for polling mechanisms or any other CPU-demanding processes. Computational time is affected only in the study of the approach via model checking, as it affects the time the model requires to finish.

4. Formal Verification for SP PON-Based FiWi Energy Analysis

Model checking is an automated verification and validation technique based on exploring the states of a model of a real-life system [25]. Probabilistic model checking computes probabilities and quantitative measurements, such as the expected power consumption. It can be successfully applied to many application domains, e.g., new communication technologies, communication protocols, security protocols, etc. Furthermore, it requires the construction of a probabilistic model, e.g., Markov chain, M, derived from a description of a probabilistic system by using a high-level modelling language and the formal specification of quantitative properties which are declared as formulae ϕ based on temporal logic. To verify the quantitative properties of a system model, probabilistic model checking typically explores the model's full state space [18]. On this basis, we assess the energy impact of the two suggested energy-efficient mechanisms on an SP PON-based FiWi from Section 3.

In order to represent a system with probabilistic behavior, we build a Markov-based model that contains a set of states and a number of state transitions from one state to another. There are a number of probabilistic models, namely discrete-time Markov chains (DTMCs) and continuous-time Markov chains (CTMCs), Markov decision processes (MDPs), etc. Among them, DTMC is fully probabilistic, in the sense that one can specify the probability of making a transition from one state to another. While CTMCs represent probabilistic choice similarly to DTMCs, they also permit modeling of continuous real time, rather than discrete time-steps, and specify the rate of state transitions. From a probabilistic model checking perspective, CTMC is a suitable choice due to its advantage to represent transitions that occur between each pair of states specified by a *rate* value and labels.

In this work, our model represents the ONU-OLT communication along with the mechanisms discussed in Section 3, as well as an MITM attack scenario disrupting their operation using CTMC [26]. For the proposed model, the ONU's transition rates among its states, i.e., active, listen, sleep, as they presented at the state machine of Figure 2b, the attacker's rate and the packet's arrival and service rates correspond to the CTMCs primitives. Because of this, we opted for CTMC since it perfectly fits for our modeling. Along the same lines, similar proposals were made in previous works published in the literature, concerning the use of CTMC modeling. For example, in [27], CTMC is also used in a model that concerns the computational and transmission costs of security protocols in hardware-constrained environments; additionally, in [28], the near field communication (NFC) protocol is tested against a relay attack by means of model checking and CTMC, as well as the authors in [21] develop a CTMC representation of an MITM attack on an Ethernet passive optical network (EPON) energy-efficiency mechanism together with cost-related properties that are verified over the full state space of the model.

The CTMC principles are further described in order to explain the observed model's behavior. Formally, the proposed model which is a tuple (S, s_{init}, R, L), consists of S, which is a countable set of states, $s_{init} \sim\in S$ is the initial state, a transition rate matrix $R : S \times S \to \mathbb{R}_{\geq 0}$ and a labeling function $L : S \to 2^{AP}$. The rates $R(s, s')$ are stored in the so-called rate matrix R, which represents a transition from a state s to s' within time t. The probability of this transition is described as a negative exponential distribution $1 - e^{-R(s,s')t}$, the parameter of which is the transition rate of $R_{s2s'}$ [25]. Labels are defined to model the transitions of the system by the labeling function $L(s) \in s^{AP}$ that assigns one or more of *atomic properties* taken from the set AP, to any state s of the system.

In addition to the probabilistic results, CTMC supports also rewards to receive quantitative results of the system model, such as power consumption. A reward structure enhances the structure of a given CTMC model. It consists of a (ρ, ι) tuple, where $\rho : S \to R_{\geq 0}$ is the state reward function and $\iota : S \times S \to R_{\geq 0}$ is the transition reward function. Although there are four types of rewards, we use in our model the cumulative reward of the form $\mathcal{R}_{\sim r}[C^{\leq t}]$, which states that the expected reward cumulated up to time-instant t is $\sim r$, and the instantaneous reward property of the form $\mathcal{R}_{\sim r}[I^{=t}]$, which states that the expected value of the reward at time-instant t is $\sim r$, where the relation operator $\sim\in \{<, \leq, \geq, >\}$.

In our analysis, instantaneous rewards represent the expected packet delay, whereas cumulative rewards represent the expected energy consumption. The time property of these rewards is usually derived using probabilistic results.

5. Modeling of the Energy-Aware Mechanisms

In this paper, we use probabilistic model checking as a way to verify improvements in energy saving achieved by the two proposed mechanisms, namely the *wake-up* and the *time-out* mechanisms. We assume SP PON-based FiWi under a MITM attack, an EPON system in our case, taking into account our initial findings [21].

In practice, we use the Prism model checker [26] and define five modules, namely M_{olt}, M_{onu}, M_{qolt}, M_{qonu}, M_{attack}, which correspond to the OLT and ONU devices, their own queues, and the attacker, respectively. The behavior of each module of our CTMC model is described by a set of commands.

The modules M_{qolt} and M_{qonu} represent the queues of OLT and ONU, respectively. They receive and buffer a number of data packets in either downstream or upstream directions, correspondingly. Packets' arrival and service are controlled by the rates: (i) λ_{down} for downstream packets' arrival; (ii) λ_{up} for the upstream packets' arrival; and (iii) μ for their service rate.

The behavior of the legitimate OLT and ONU devices is modeled by the modules M_{olt} and M_{onu}, respectively. The packets' transmission between the OLT and the ONU in either direction depends on the aforementioned rates, i.e., λ_{down}, λ_{up}, and μ, as well as on the ONU's state, i.e., active, listen, or sleep. In the module M_{onu}, the time spent in the listen mode is denoted as d_{listen} and specifies the rate $1/d_{listen}$ of staying in this mode, while the time spent in the sleep mode is defined as d_{sleep} and specifies the rate $1/d_{sleep}$ of staying in the sleep mode. The devices communicate when the ONU is in active mode, while the other two modes contribute to the ONU's energy saving when no traffic exists. Regarding the baseline energy-aware mechanism [21], it is modeled by exchanging the control messages, i.e., *sleep*, *ack*, and *nack*, between the OLT and the ONU.

The module M_{attack} models the attacker's behavior, which connects a fake OLT device between the legitimate OLT and ONU. The fake OLT intercepts the *sleep* requests, sent by the legitimate OLT, and replies with *nack* messages in respect with a rate of r_{fk}. Values of r_{fk} range from 0 to 1 corresponding to the rate of the attacker's intervention, i.e., 0 means that the attacker does not intercept any *sleep* request, while 1 means that the attacker intercepts all *sleep* requests. In brief, higher r_{fk} rates correspond to higher chances of a successful *sleep* request interception. Once the attacker successfully intercepts a *sleep* request, it responds with a *nack* message back to the OLT to keep the ONU in active mode and, hence, to consume power.

Our model activates the *wake-up* mechanisms, Figure 2a, when the downstream packet arrival rate λ_{down} is at the low-end, i.e., light traffic conditions, and the OLT queue is empty. Hence, the OLT sends a *sleep* request to the ONU, and the ONU replies with an *ack* message since the upstream arrival rate λ_{up} is light and there may not exist any upstream traffic on M_{qonu} during this period of time. Then, it transits from the active to the listen mode in negligible time [18] and stays in it for a time period d_{listen}. If any downstream traffic is received during the listen mode period, which depends on λ_{down}, it was buffered at the OLT's queue, and once the listen period expired the ONU received a *wake-up* message from the OLT in order to transit to the active mode and receive the buffered downstream packets. Once the OLT's queue becomes empty again, the OLT sends a *sleep* request to the ONU. If the ONU's queue is also empty, it replies with an *ack* message and transits first to the listen mode and then to sleep mode in 2.88 μs that corresponds to the time needed by the ONU to turn off its transceiver [19]. It should be noted that this transition occurred because there was no downstream traffic while in listen mode. The ONU stays in sleep mode for a period d_{sleep} and, as a result, saves energy.

During the sleep period, the received down/up stream traffic is buffered at the OLT's and the ONU's queues. The sleep mode period cannot be interrupted by neither downstream nor upstream traffic arrivals. Moreover, if any downstream traffic received during sleep mode (which depends on λ_{down}) is buffered at the OLT's queue and once the sleep period expires the ONU will receive a *wake-up* message from the OLT in order to transit to the active mode and receive the buffered downstream packets. If the OLT's queue is still empty at the time the sleep mode period expires, the ONU will not receive a *wake-up* message and instead, will or will not wake up depending on the ONU's queue status.

The *time-out* mechanism is activated and serves to countermeasure a MITM attack (Figure 3a) during which the attacker receives the *sleep* request from the legitimate OLT and replies with a *nack* message with a rate depending on the r_{fk} parameter's value. In the M_{onu} module, we define $d_{ltimeout}$ as the *time-out* interval period, which specifies the rate $1/d_{timeout}$ for the ONU's transition to the listen mode when neither traffic nor *sleep* requests arrive at the device (Figure 3b).

Inside the Prism model, we also define properties to express its expected behavior. Probabilistic results are derived by the application of the probability operator into sets of states and paths, $P{\sim}p[.]$, where the relation operator $\sim \in \{<, \leq, \geq, >\}$ and the probability bound $p \in [0, 1]$. In the proposed model, we use the form of the probabilistic property $P =?[F\ \phi]$, where = ? replaces the bound operator p, F stands for "eventually" and ϕ represents the path formulae. The aim is to calculate the probability that the model "eventually" satisfies the path formulae ϕ, e.g., the probability that a number of upstream packets have been successfully received by the OLT [26]. Moreover, we define reward properties in our CTMC model using the operator R to receive quantitative results, such as the expected energy consumption within a certain time period.

6. Quantitative Verification Results

Prism model checker [26] was used for the design and analysis of the proposed *wake-up* and *time-out* mechanisms, and we derive quantitative verification results were run on a core i7 2.4 GHz system with 8 GB of RAM. To align our model with the specifications of an EPON access network, we assume C = 1.25 Gbps for both down and upstream channel and l = 1518 bytes for packet length.

Table 3 contains information regarding the state space produced once our CTMC model is built and no attack has occurred (i.e., r_{fk} = 0). We notice that increasing the number of transmitted packets in both down/up stream directions causes a non-linear increase in the state space (S) in line with the total number of the model's states, the number of transitions among them, the number of iterations, and the time needed to solve the model. The rest of modeling parameters, i.e., packet arrival and service rates ($\lambda_{up}, \lambda_{down}, \mu$), the duration of listen, sleep, and *time-out* periods ($d_{listen}, d_{sleep}, d_{timeout}$), as well as the rate of attacker's intervention (r_{fk}) do not affect the model's state space.

Table 3. State space results.

		No Attack		
Transmitted packets	Total states of S	Transitions	Iterations	Time (s)
2×10^3	75,152	226,948	51	1.07
2×10^4	320,328,811	1,096,965,442	411	375.93
2×10^5	59,874,695,911	206,900,548,642	4011	1916.90

Shortly after the building phase, model checking verifies the properties of interest expressed in continuous-time stochastic (CSL) logic. We start with the proof-of-concept property, $P =? [F \leq C_0\ finish]$, which evaluates the probability of finding final states before the time interval specified by C_0 has elapsed, for which the formula "finish" is true. This formula represents the Boolean expression that controls whether all packets defined in the following CSL query have been transmitted and received successfully. More specifically, the query is:

$$\begin{aligned} Q_1 : \mathcal{P} =? [F \leq C_0\ finish], C_0 = 100, \\ packets_{down} = 1000,\ packets_{up} = 1000, \\ \lambda_{down} = 0.2 \ldots 1, \lambda_{up} = 0.6,\ \mu = 1, r_{fk} = 0, \\ d_{listen} = 8 \text{ ms},\ d_{sleep} = 20 \text{ ms},\ d_{timeout} = 35 \text{ ms} \end{aligned}$$

provides the probability that 1000 downstream packets will be transmitted by the OLT and received successfully by the ONU and 1000 upstream packets will be transmitted by the ONU and received successfully by the OLT within 100 ms when arrival rate λ_{down} varies from 0.2×10^2 to 1×10^2 packets/ms and λ_{up} is fixed at 0.6×10^2 packets/ms. Different λ_{down} values express different downstream traffic arrival rates, hence, in case of our model λ_{down} = 0.2, 0.6 and 1 represents light, medium and high downstream traffic, respectively The r_{fk} parameter is set to zero, since we firstly consider a non-attack scenario, while the $d_{timeout}$ is predefined at a balanced value of 35 ms. This choice takes into account that a low value will cause the ONU to *time-out* often causing delays even without the presence of an attacker but will result in higher energy saving, while a high $d_{timeout}$ value will cause a low delay but high energy consumption when an attacker is present. Being a parameter in the proposed model, $d_{timeout}$ can be modified accordingly to follow the specific characteristics of a PON. As already mentioned, the same applies for the values of parameters d_{listen} and d_{sleep} whose choices are derived by [19]. The impact of the $d_{timeout}$ parameter on the trade-off between energy consumption and packet delay is demonstrated later on this section (Figures 11 and 12).

Results of Q_1 are depicted in Figure 4, where the proposed model (solid line) is being compared with [21] (dotted line). We notice that the curves of our model move to the left as the downstream packet arrival rate, λ_{down}, increases. This indicates that the model is completed sooner.

Specifically, in the work of [21], the curve corresponding to $\lambda_{down} = 1$ reaches probability 1.0 when $C_0 = 100$ ms, while at this time probability is 0.99 and 0.82 for $\lambda_{down} = 0.6$ and $\lambda_{down} = 0.2$, respectively. Lower values of the rate λ_{down} entail a higher probability for the OLT to send sleep requests and for the ONU to respond with an *ack* message, causing delays in the model's completion.

On the other hand, when we employ the proposed *wake-up* and *time-out* mechanisms, the curves move further to the left, which entails that the model is completed even sooner. A major difference from [21] is that, at time $C_0 = 100$ ms, this model has been completed even for $\lambda_{down} = 0.2$. This is anticipated since the ONU turns to active mode more often as a result of the *wake-up* mechanism. More specifically, when $\lambda_{down} = 0.2$ the model needs 100 ms to finish, when $\lambda_{down} = 0.6$ the model needs 40 ms to finish; and when $\lambda_{down} = 1$, the model needs 38 ms to finish. For a better comparison regarding the time that the model is being completed, i.e., reaches probability 1.0, Figure 5 shows the bars of time in ms

for different values of λ_{down}. Comparing the yellow bars [21] with the purple ones that correspond to our proposed model, we notice that the latter finish, 1.5, 2.75, and 2.6 times faster when $\lambda_{down} = 0.2$, $\lambda_{down} = 0.6$ and $\lambda_{down} = 1$, respectively.

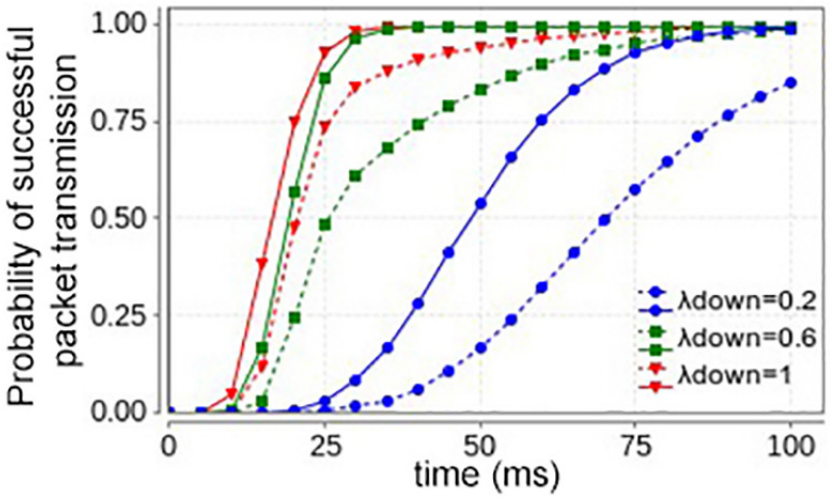


Figure 4. Proof-of-concept-results for downstream and upstream traffic: mechanism proposed in [21] (dotted line), *time-out* and *wake-up* mechanisms (solid line).

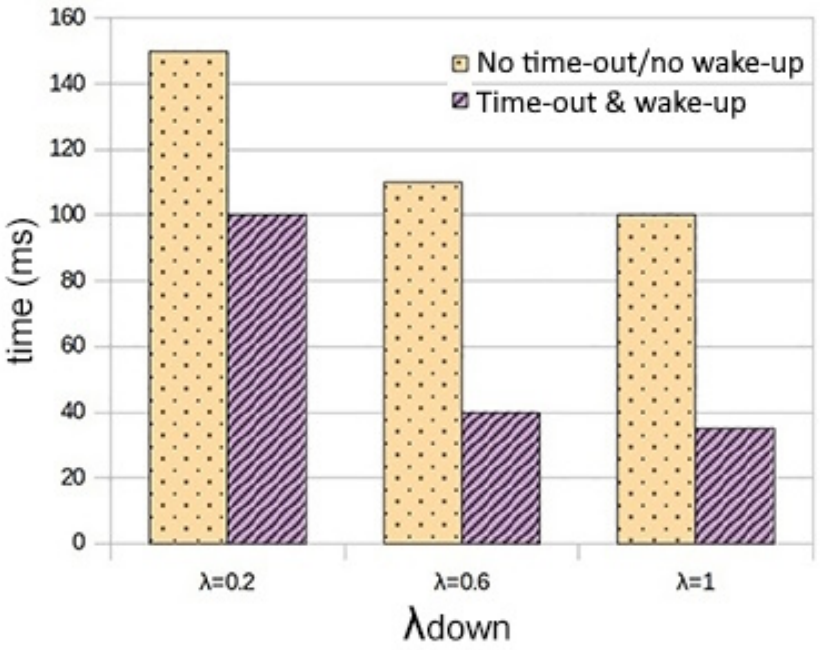


Figure 5. Time required for proposed model and model [21] to be completed with probability of 1 when λ_{down} varies from 0.2 to 1 and $\lambda_{up} = 0.6$.

In addition to the probabilistic results, we evaluate the impact of both *wake-up* and *time-out* mechanisms, taking into consideration the case of a MITM attack on the energy-aware mechanism. We employ rewards to receive quantitative results of the system model, such as power consumption. Specifically, we use the cumulated reward property of the form $\mathcal{R}_{\sim r}[C^{\leq t}]$ to measure the consequences of a MITM attack on the energy levels of a solar-powered ONU.

We derive results of Figure 6 defining the query:

$$Q_2 : \mathrm{R}\{\text{“}energy\_consumption\text{”}\} =? \; [C \leq C_0], \; C_0 = 100$$
$$packets_{down} = 1000, \; packets_{up} = 1000,$$
$$\lambda_{down} = 0.2 \ldots 1, \; \lambda_{up} = 0.6, \; \mu = 1, \; r_{fk} = 0 \ldots 1,$$
$$d_{listen} = 8 \text{ ms}, \; d_{sleep} = 20 \text{ ms}, \; d_{timeout} = 35 \text{ ms}$$

which provides the expected energy consumption in line with the λ_{down} arrival rate, taking into account different values of the r_{fk} parameter.

In Figure 6, the blue, green, and red curves represent the different values of intervention rate, i.e., 0 (blue), 0.5 (green), and 1 (red), which denote that the attacker does not intercept any sleep request from the OLT, intercepts half of the sleep request messages that the OLT sends or all of them, correspondingly. In this figure, the expected energy consumption is plotted for different values of λ_{down}, keeping the $\lambda_{up} = 0.6$. The dotted line represents the results from [21], while the dashed line refers to the proposed model having only the *wake-up* mechanism activated and the solid line having both energy-saving mechanisms activated.

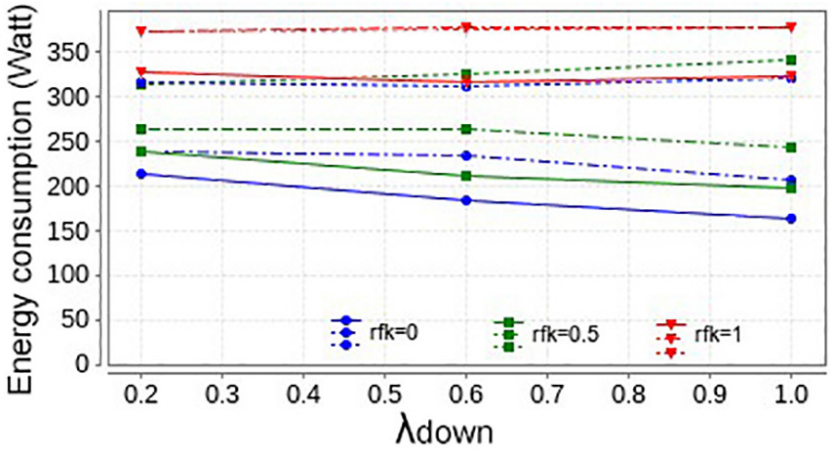


Figure 6. Energy consumption consequences of a MITM attack: mechanism proposed in [21] (dotted line), *wake-up* mechanism (dashed line), both *wake-up* and *time-out* mechanisms (solid line).

It is clear that using our proposed mechanisms, the expected energy consumption at the ONU decreases with the increase in λ_{down}. This is the case when the *wake-up* mechanism is used, and it is amplified with lower levels of energy consumption when it is employed in conjunction with the *time-out* one. On the contrary, in [21] the energy consumption increases as both λ_{down} and the r_{fk} rate increase. This is owed to the decrease in sleep requests' acceptance ratio. In fact, the impact of the *wake-up* mechanism is more evident for higher λ_{down} rates, since the packets' transmission is completed sooner and the ONU transits to the sleep mode. Meanwhile, the impact of the *time-out* mechanism on the energy consumption compared to [21] is enhanced for higher r_{fk} rates, since the sleep request acceptances decrease and the ONU transits to sleep mode due to the *time-out*.

To highlight the advantage of applying the proposed mechanisms simultaneously, Figure 7 displays the energy consumption for different r_{fk} rates when $\lambda_{down} = 0.6$ and $\lambda_{up} = 0.6$. As shown in the figure, the *wake-up* mechanism provides lower energy consumption for mild and low interception rates as much as 18.8% under medium-class intervention by the attacker ($r_{fk} = 0.5$) compared to [21]. Applying both the proposed mechanisms, the system achieves the best performance concerning energy efficiency outperforming the [21] by almost 38.7% ($r_{fk} = 0$), 34.4% ($r_{fk} = 0.5$), and 17.3% ($r_{fk} = 1$) less energy consumption compared to [21]. All in all, both mechanisms work together efficiently, decreasing the energy consumption even for high rates of λ_{down} and r_{fk}.

What is interesting enough is the fact that the energy-saving characteristic of the proposed schemes does not come with high packet delay. For this, delay-related results in Figure 8 derived by the following query:

$$Q_3 : \mathrm{R}\{\text{“}delay\text{”}\} =? [I = T],\ T = 100,$$
$$packets_{down} = 1000,\ packets_{up} = 1000,$$
$$\lambda_{down} = 0.2 \ldots 1,\ \lambda_{up} = 0.6,\ \mu = 1,\ r_{fk} = 0,$$
$$d_{listen} = 8 \text{ ms},\ d_{sleep} = 20 \text{ ms},\ d_{timeout} = 35 \text{ ms}$$

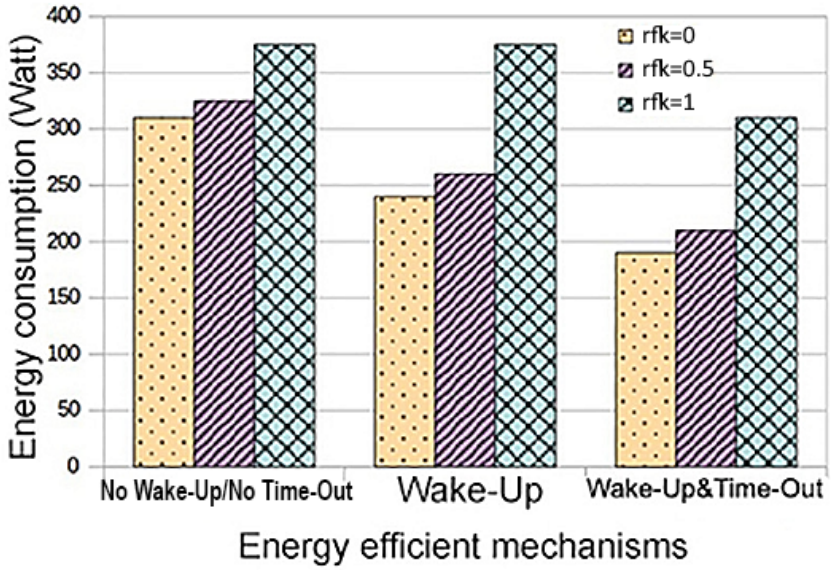


Figure 7. Energy consumption for different attacker intervention rates r_{fk} when $\lambda_{down} = 0.6$ and $\lambda_{up} = 0.6$.

The query Q_3 provides the downstream packet delay for different values of λ_{down} in case of model [21] (dotted line), as well as when both *wake-up* and *time-out* mechanisms are applied (solid line). For the delay performance, our model is augmented with the reward structure X = *delay* which counts queuing and transmission delay. The packets that arrive while the ONU is sleeping do not have to wait for a sleep cycle to complete, since the *wake-up* mechanism is active. The comparative results are shown in Figure 8.

At the beginning, packets start to arrive in the OLT queue, resulting in the increase in packet delay. In case of [21] (dotted lines), disrupting the ONU's sleep cycle is not possible, causing the OLT to buffer any incoming downstream packets increasing the OLT queue eventually, resulting to higher delay compared to our model (solid lines), whose *wake-up* mechanism causes the ONU to stop the sleep cycle in order to receive packets from the OLT queue. For example, when $\lambda_{down} = 0.2$ the blue, dotted line [21] has a peak average packet delay of 7.6 ms, which is clearly higher compared to 4.6 ms provided by the corresponding solid blue line (both mechanisms). After their peak (at $C_0 = 40$ ms model time), both blue lines decline, indicating the delay decreases due to the fact that the OLT queue is emptying of packets. Obviously, higher values of λ_{down} entails lower packets' delay since the ONU stays in the active state and receives them. The same behavior is exhibited for $\lambda_{down} = 0.6$ and 1 giving again to the proposed model constantly lower values of delay, proving the efficiency of the introduced mechanisms.

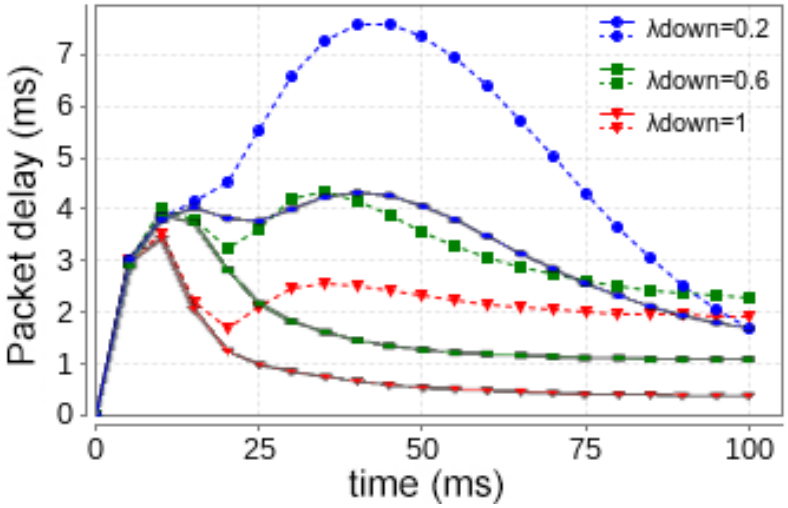


Figure 8. Downstream packet delay: mechanism proposed in [21] (dotted line) *wake-up* and *time-out* mechanisms (solid line).

The query Q_4 provides the expected number of *wake-up* mechanism activations for different $d_{timeout}$ and different r_{fk} values. The comparative results are shown in Figure 9.

$$Q_4 : \mathrm{R}\{\text{“}wake\_ups\text{”}\} =? \; [C \leq C_0], \; C_0 = 100$$
$$packets_{down} = 1000, \; packets_{up} = 1000,$$
$$\lambda_{down} = 0.2 \ldots 1, \; \lambda_{up} = 0.6, \; \mu = 1, \; r_{fk} = 0, 0.5, 1,$$
$$d_{listen} = 8 \text{ ms}, \; d_{sleep} = 20 \text{ ms}, \; d_{timeout} = 10, 35, 100 \text{ ms}$$

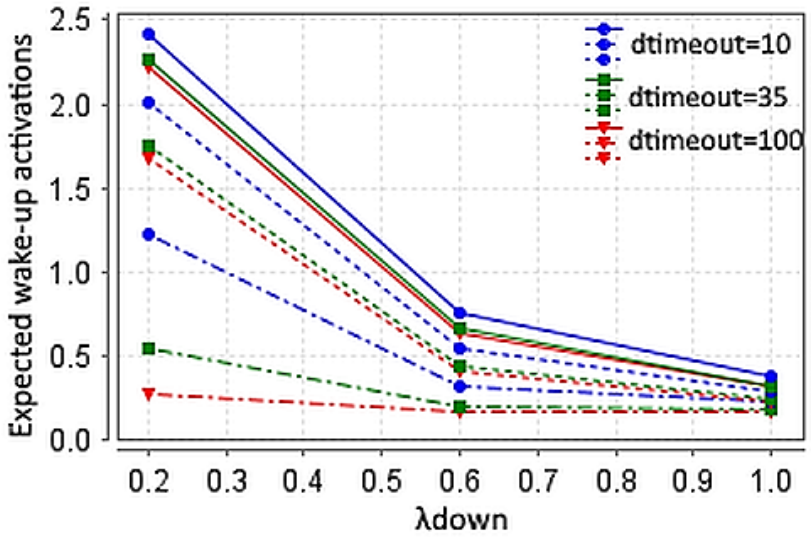


Figure 9. The expected number of times the *wake-up* mechanism activates for different $d_{timeout}$ and different r_{fk} values. r_{fk} = 0 (solid line), r_{fk} = 0.5 (dotted line), and r_{fk} = 1 (dashed line).

As shown in Figure 9, the *wake-up* mechanism is activated more frequently in the absence of an attacker (r_{fk} = 0, solid line) since the ONU transits to the sleep state without any barrier caused by a potential attacker. As expected, when $d_{timeout}$ = 10 ms, the *wake-up* mechanism activates more times compared to higher $d_{timeout}$ values, since the ONU transits to sleep more frequently. For high λ_{down} values, the *wake-up* seems less effective, since the ONU transits to the sleep state less frequently. Additionally, for high r_{fk} rates (r_{fk} = 1 dashed line), the *wake-up* mechanism is rarely activated, since the attacker intercepts all

sleep requests, resulting to ONU staying active for longer periods of times. Consequently, the *wake-up* mechanism is more effective for low λ_{down} values while an attacker is not present. It should be reminded that the *wake-up* mechanism does not counter a MITM attack, instead, it is a mechanism that results to lower packet delay and higher energy saving as shown in previous figures.

The query Q_5 provides the expected number of *time-out* mechanism activations for different $d_{timeout}$ and different r_{fk} values. The comparative results are shown in Figure 10.

$$Q_5 : \mathrm{R}\{\text{“}time\_outs\text{”}\} =? \; [C \leq C_0], \; C_0 = 100$$
$$packets_{down} = 1000, \; packets_{up} = 1000,$$
$$\lambda_{down} = 0.2 \ldots 1, \; \lambda_{up} = 0.6, \; \mu = 1, \; r_{fk} = 0, 0.5, 1,$$
$$d_{listen} = 8 \text{ ms}, \; d_{sleep} = 20 \text{ ms}, \; d_{timeout} = 10, 35, 100 \text{ ms}$$

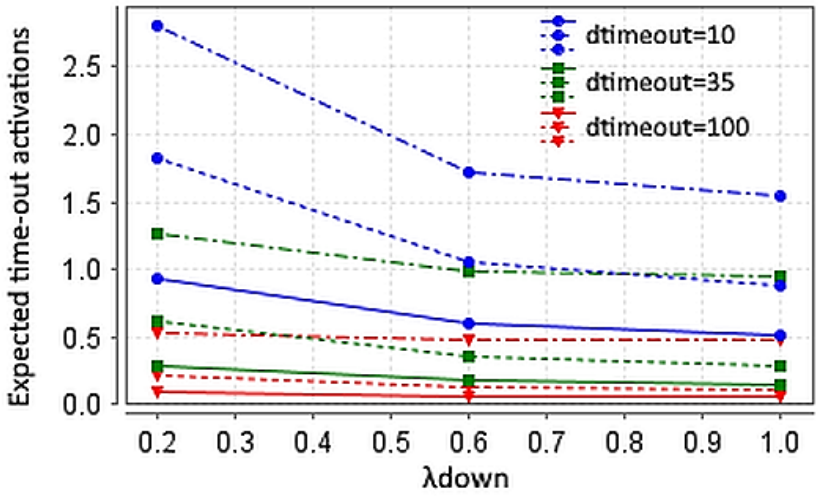


Figure 10. The expected number of times the *time-out* mechanism activates for different $d_{timeout}$ and different r_{fk} values. r_{fk} = 0 (solid line), r_{fk} = 0.5 (dotted line), r_{fk} = 1 (dashed line).

As shown in Figure 10, the *time-out* mechanism really shows its potential for lower λ_{down} and higher r_{fk} values. For $d_{timeout}$ = 10 ms the blue lines are higher as expected, since the ONU time-outs more frequently. In case of r_{fk}=0, the *time-out* mechanism has a lower effect, since it is designed to counter a MITM attack. Although, as shown in Figure 10, the *time-out* mechanism is also expected to activate for λ_{down} = 0.2. $d_{timeout}$ values higher than 10 ms do not really have much of effect in our model in case of not having a MITM attack. Additionally, as expected, setting a higher $d_{timeout}$ value results to less mechanism activations. Setting a lower $d_{timeout}$ value results to more *time-out* mechanism activations which entails the ONU transits to sleep mode more often, hence, increasing the overall packet delay. Finally, in order to set the optimal $d_{timeout}$ we need to take into consideration various model parameters such as r_{fk}, λ_{down}, delay and energy consumption. Consequently, if a system aims to maximize energy saving while tolerating an increase in packet delay, low $d_{timeout}$ values (such as 10 ms) should be considered. On the other, if a system aims to minimize delay, higher $d_{timeout}$ values (such as 35 ms) are optimal.

The query Q_6 provides the expected energy consumption for different $d_{timeout}$ and different r_{fk} values. The comparative results are shown in Figure 11.

$$Q_6 : \mathrm{R}\{\text{“}energy\_consumption\text{”}\} =? \; [C \leq C_0], \; C_0 = 100$$
$$packets_{down} = 1000, \; packets_{up} = 1000,$$
$$\lambda_{down} = 0.2 \ldots 1, \; \lambda_{up} = 0.6, \; \mu = 1, \; r_{fk} = 0, 0.5, 1,$$
$$d_{listen} = 8 \text{ ms}, \; d_{sleep} = 20 \text{ ms}, \; d_{timeout} = 10, 35, 100 \text{ ms}$$

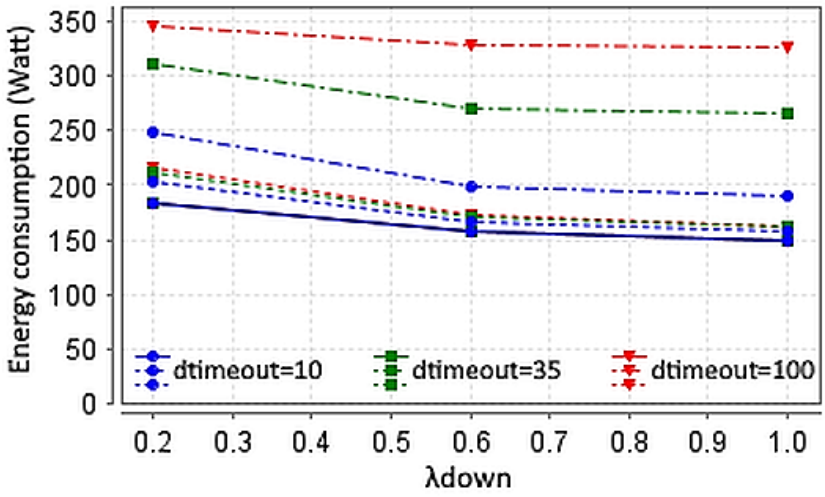


Figure 11. Energy consumption consequences for different $d_{timeout}$ and different r_{fk} values. $r_{fk} = 0$ (solid line), $r_{fk} = 0.5$ (dotted line), $r_{fk} = 1$ (dashed line).

In Figure 11, the blue, green, and red curves represent the different $d_{timeout}$ values, i.e., 10 (blue), 35 (green), and 100 (red), which denote the *time-out* interval period until *time-out* activation. In this figure, the expected energy consumption is plotted for different values of λ_{down}, keeping the $\lambda_{up} = 0.6$. The solid line represents a model where the attacker is not present ($r_{fk} = 0$), while the dashed line refers to a model where the attacker intercepts all *sleep requests* sent from the OLT ($r_{fk} = 1$) and the dotted line a model where half of the *sleep requests* are intercepted ($r_{fk} = 0.5$).

As shown, the energy consumption is higher when $r_{fk} = 1$ and it reaches its highest point when $d_{timeout} = 100$ ms, showing that such a high $d_{timeout}$ value is inappropriate. Comparing $d_{timeout} = 10$ ms when $r_{fk} = 1$ (blue dashed line) and $d_{timeout} = 35$ ms when $r_{fk} = 1$ (green dashed line), the first clearly has the advantage in terms of energy consumption since the ONU transits to the sleep state more frequently, but in the expense of expected increased packet delay. Additionally, while $r_{fk} = 0$ (solid lines), different $d_{timeout}$ values have the same outcome, since the *time-out* mechanism is not as effective in the absence of an attacker. As shown, when $r_{fk} = 0.5$, the results between different $d_{timeout}$ values are almost identical.

Finally, as already mentioned, lower $d_{timeout}$ values result to increased packet delay. For this, delay related results in Figure 12 derived by the query Q_7:

$$Q_7 : \mathrm{R}\{\text{“}delay\text{”}\} =? \, [C \leq C_0], \; C_0 = 100$$
$$packets_{down} = 1000, \; packets_{up} = 1000,$$
$$\lambda_{down} = 0.2 \ldots 1, \; \lambda_{up} = 0.6, \; \mu = 1, \; r_{fk} = 1,$$
$$d_{listen} = 8 \text{ ms}, \; d_{sleep} = 20 \text{ ms}, \; d_{timeout} = 10, 35 \text{ ms}$$

In Figure 12, the expected packet delay is plotted for different values of λ_{down}, keeping the $\lambda_{up} = 0.6$ while the attacker intercepts all *sleep requests* ($r_{fk} = 1$) since it is shown from earlier figures that the *time-out* mechanism is more effective for higher r_{fk} values. The solid lines represent the results when $d_{timeout} = 35$ ms, while the dotted lines refers to $d_{timeout} = 10$ ms. When we set $d_{timeout} = 10$ ms the curves move further to the right, which entails increased delay in comparison to $d_{timeout} = 35$ ms. This shift to the right is more distinctive when $\lambda_{down} = 0.2$, while higher λ_{down} values have an identical result in terms of delay.

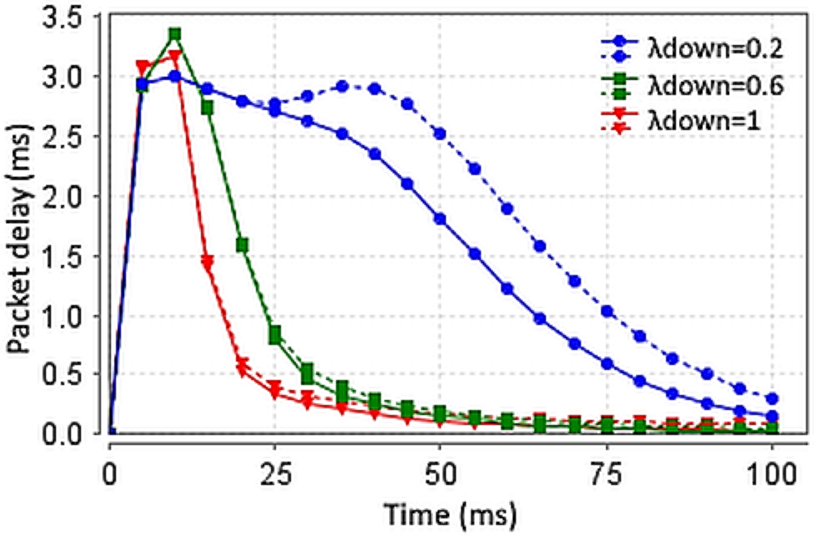


Figure 12. Packet delay for different $d_{timeout}$ values. $d_{timeout}$ = 35 ms (solid line), $d_{timeout}$ = 10 (dotted line).

Comparing Figures 11 and 12 when λ_{down} = 0.2 the energy consumption of $d_{timeout}$ = 10 ms (blue circle point) is lower than $d_{timeout}$ = 35 ms (green square point) by ∼20%, while the delay of $d_{timeout}$ = 35 ms (blue solid curve) is lower than $d_{timeout}$ = 10 ms (blue dotted curve) and after 35 ms, it continues to maintain a distance ranging between 20% and 45%. Therefore, setting the optimal $d_{timeout}$ value should take into consideration the trade-off between energy consumption and packet delay, based on each application/system preferences.

7. Conclusions

This paper proposes two energy-aware mechanisms, namely the *wake-up* and the *time-out*, that effectively improve the energy efficiency of a solar-powered PON-based FiWi access network without increasing the model's computational time, while investigating the energy impact of a MITM attack of such access network systems. We showed that the *wake-up* mechanism has the advantage of completing packet transmission sooner and improving energy saving, since the ONU avoids unnecessary transitions to the sleep mode and, thus, it transits more often from the listen to the active mode instead from the sleep to the active mode. The second transition case is more energy demanding since short sleep periods benefit the packets' delay, but they limit the potential energy saving. We also verified that a balanced *time-out* interval period combined with the *wake-up* mechanism further improves energy saving without significantly affecting the packets' delay. As shown, applying both the proposed mechanisms, the system achieves higher performance concerning energy efficiency, since it outperforms the [21] by almost 38.7% (r_{fk} = 0), 34.4% (r_{fk} = 0.5), and 17.3% (r_{fk} = 1) while improving packet delay by up to 50% for low downstream packet arrival rates. In addition, the effects of *wake-up* and *time-out* mechanisms are more distinctive for low λ_{down} values, and at, the same time, the *time-out* mechanism shows a clear effect when the MITM attack intercepts all *sleep requests* sent from the OLT. As shown, lower $d_{timeout}$ values result to higher energy saving in expense of delay, therefore, the trade-off between energy and delay should be considered before setting a system's optimal $d_{timeout}$ value. Finally, it is showed that our proposed mechanisms can effectively countermeasure a MITM attack on SP battery-powered ONUs in PON-based FiWi access systems, with a negligible increase in packet delay.

Overall, the wireless section of FiWi systems has many issues such as the use of separate MAC address for each client and high energy consumption. The proposed mechanisms focus on the PON section of a FiWi system and mainly on its energy consumption in normal operations much like under MITM attack. Consequently, the aforementioned FiWi

issues are not taken into account in our model. Our future plans include an extension of the current model including the wireless section of the FiWi system which deserves a separate study and we plan to address in our future work. We believe that our proposed mechanisms present a promising solution for future SP PON-based FiWi access networks.

Author Contributions: Conceptualization, S.P. and P.N.; Data curation, A.I., P.T., S.P. and P.N.; Formal analysis, A.I. and S.P.; Investigation, A.I., P.T., S.P. and P.N.; Methodology, A.I., P.T. and S.P.; Validation, A.I. and S.P.; Visualization, P.T. and A.I.; Writing—original draft, A.I., P.T., S.P. and P.N.; Project administration, S.P. and P.N.; Resources, A.I., P.T., S.P. and P.N.; Supervision, S.P., P.N. and K.K.; Writing—review and editing, A.I., P.T., S.P., P.N. and K.K.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Wu, X.; Yang, C.; Han, W.; Pan, Z. Integrated design of solar photovoltaic power generation technology and building construction based on the Internet of Things. *AEJ Elsevier* **2022**, *61*, 2775–2786. [CrossRef]
2. Ujikawa, H.; Yamada, T.; Suzuki, K.I.; Otaka, A.; Nishiyama, H.; Kato, N. In Stand-Alone and Cooperative Deep Sleep for Battery-Driven Optical Network Unit. *IEEE IoT J.* **2016**, *3*, 494–502. [CrossRef]
3. Dave, P. "Automation Goes Off-Grid". 1 December 2020. Available online: https://www.processingmagazine.com/process-control-automation/article/21164839/automation-goes-offgrid (accessed on 20 December 2022).
4. PHILIPP KORNSTÄDT, "Solar Power for Mobile Network". February 2021. Available online: https://www.telekom.com/en/media/media-information/archive/solar-power-for-mobile-network-619496 (accessed on 20 December 2022).
5. Gupta, A.; Srivastava, A.; Bohara, V.A. Resource allocation in solar-powered FiWi networks. *IEEE Access* **2020**, *8*, 198691–198705. [CrossRef]
6. Gu, Z.; Lu, H.; Zhu, D.; Lu, Y. Joint power allocation and caching optimization in fiber-wireless access networks. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi National Exhibition Centre, Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–7.
7. Sundararajan, A.; Chavan, A.; Saleem, D.; Sarwat, A.I. A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security. *Energies* **2018**, *11*, 2360. [CrossRef]
8. Chamola, V.; Krishnamachari, B.; Sikdar, B. Green energy and delay aware downlink power control and user association for off-grid solar-powered base stations. *IEEE Syst. J.* **2017**, *12*, 2622–2633. [CrossRef]
9. Chamola, V.; Sikdar, B. Solar powered cellular base stations: Current scenario, issues and proposed solutions. *IEEE Commun. Mag.* **2016**, *54*, 108–114. [CrossRef]
10. Zhang, Y.; Meo, M.; Gerboni, R.; Marsan, M.A. Minimum cost solar power systems for LTE macro base stations. *Comput. Netw. Elsevier* **2017**, *112*, 12–23. [CrossRef]
11. Sharma, V.; Sharma, S.; Kumar, A. Passive Optical Network: A New Approach in Optical Network. In Proceedings of the 2020 International Conference on Advances in Computing, Communication & Materials (ICACCM), Tula's Institute, Dehra Dun, Uttarakhand, India, 21–22 August 2020; pp. 295–300.
12. High Sierra Electronics Inc. "StormLink® RWIS One—Model 5409 Series". 15 February 2022. Available online: https://hsierra.com/product/stormlink-rwis-one-model-5409-series/ (accessed on 27 December 2022).
13. Van, D.P.; Rimal, B.P.; Maier, M.; Valcarenghi, L. ECO-FiWi: An energy conservation scheme for integrated fiber-wireless access networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3979–3994. [CrossRef]
14. ITU-T, "Rec, G. 984.3: Gigabit-capable Passive Optical Networks (GPON): Transmission Convergence Layer Specification". March 2014. Available online: https://www.itu.int/rec/T-REC-G.984.3 (accessed on 27 December 2022).
15. Lingas, N.; Uddin, M.R. Sleep Mode on Delay Sensitive Traffic on Optical Network Unit. In Proceedings of the 2021 23rd International Conference on Advanced Communication Technology (ICACT), On-Line Presentation over Internet, 7–10 February 2021; pp. 407–410.
16. Pakpahan, A.F.; Hwang, I.S. Adaptive ONU Energy-Saving via Software-Defined Mechanisms in TDMA-PON. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 3–6 July 2018; pp. 137–142.
17. Zhu, M.; Zeng, X.; Lin, Y.; Sun, X. Modeling and analysis of watchful sleep mode with different sleep period variation patterns in PON power management. *J. Opt. Commun. Netw.* **2017**, *9*, 803–812. [CrossRef]

18. Petridou, S.; Basagiannis, S.; Mamatas, L. Formal methods for energy-efficient EPONs. *IEEE Trans. Green Commun. Netw.* **2017**, *2*, 246–259. [CrossRef]
19. Petridou, S.; Basagiannis, S.; Mamatas, L. Energy-efficiency analysis under QoS constraints using formal methods: A study on EPONs. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 137–142.
20. Ujikawa, H.; Yamada, T.; Yoshimoto, N. Demonstration of timer-based ONU deep sleep for emergency communication during power failure. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; pp. 2413–2417.
21. Tsompanoglou, P.; Petridou, S.; Nicopolitidis, P.; Papadimitriou, G. Quantitative model checking for assessing the energy impact of a MITM attack on EPONs. *Internet Technol. Lett.* **2021**, *5*, 277. [CrossRef]
22. ITU-T G.987.3, "10-Gigabit-Capable Passive Optical Networks (XG-PON): Transmission Convergence (TC) Layer Specification". January 2014. Available online: https://www.itu.int/rec/T-REC-G.987.3/en (accessed on 27 December 2022).
23. de Lutiis, P.; amico, R.D.; Costa, L. Next Generation Access Network (in)security. In Proceedings of the Telecom Italia Group, Sophia Antipolis, France, 13–14 January 2009.
24. Fiammengo, M. Sleep Mode Scheduling Technique for Energy Saving in TDM-PONs. Master's Thesis, KTH, School of Information and Communication Technology, Stockholm, Sweden, 2011.
25. Kwiatkowska, M.; Norman, G.; Parker, D. Quantitative analysis with the probabilistic model checker PRISM. In *Electronic Notes in Theoretical Computer Science*; Elsevier: Amsterdam, The Netherlands, 2006; pp. 5–31.
26. Kwiatkowska, M.; Norman, G.; Parker, D. Stochastic model checking. International School on Formal Methods for the Design of Computer. In *Communication and Software Systems*; Springer: Berlin, Germany, 2007; pp. 220–270.
27. Basagiannis, S.; Petridou, S.; Alexiou, N.; Papadimitriou, G.; Katsaros, P. Quantitative analysis of a certified e-mail protocol in mobile environments: A probabilistic model checking approach. In *Computers & Security*; Elsevier: Amsterdam, The Netherlands, 2011; pp. 257–272.
28. Alexiou, N.; Basagiannis, S.; Petridou, S. Formal security analysis of near field communication using model checking. In *Computers & Security*; Elsevier: Amsterdam, The Netherlands, 2016; pp. 1–14.