Quantitative Model Checking for Assessing the Energy Impact of a MITM Attack on EPONs

P. Tsompanoglou, *Student Member, IEEE*, S. Petridou, *Member, IEEE,* P. Nicopolitidis, *Senior Member, IEEE,* and G. Papadimitriou, *Senior Member, IEEE*

***Abstract*—Broadcasting the downstream traffic makes the Ethernet Passive Optical Networks (EPONs) vulnerable to eavesdropping which is typically the initial step of an active attack, such as Man in the Middle attack (MITM). A MITM attack in such a network can be implemented by employing a fake Optical Line Terminal (OLT) and overwhelm computational, bandwidth, or energy resources. The latter is of great interest since Passive Optical Networks (PONs) are estimated to be the largest energy consumers among optical networks. In this paper we use formal analysis to quantitatively assess the impact of a fake OLT attacking an EPON energy-efficiency mechanism. Formal verification techniques, such as model checking, constitute the perfect candidate for security verification, since they can analyze systems and protocols based on rigorous model definitions. Our results show that a MITM attack increases the energy expenditure, since it enforces the Optical Network Units (ONUs) to stay in the active mode even in cases of none network traffic.**

***Index Terms*—Passive Optical Networks, energy-efficiency mechanism, formal analysis, probabilistic model checking, MITM attack**

I. Introduction

BROADCASTING the downstream traffic in Passive Optical Networks (PONs) raises security issues ranging from simple passive monitoring to more sophisticated active attacks, such as Denial of Service (DoS), Man In the Middle (MITM) attack and masquerading [1]. A MITM attack in energy-efficiency mechanisms is particularly critical since, recently, there has been significant research attention on "green" communications and networking [2]–[5]. Among the PONs, Ethernet PONs (EPONs) attract attention since they are anticipated as big energy consumers due to their massive use as an access technology [6]. Within EPONs, the Optical Network Units (ONUs) are the most energy-consuming equipment, responsible for almost 65% of the total EPON power consumption [2], [6]. Thus, a number of energy-efficiency mechanisms in the literature propose different power modes on the ONUs' operation [2], [3], [7]. Among them, the schemes that are based on control messages' exchange between the Optical Line Terminal (OLT) and the ONU are highly vulnerable to MITM attacks.

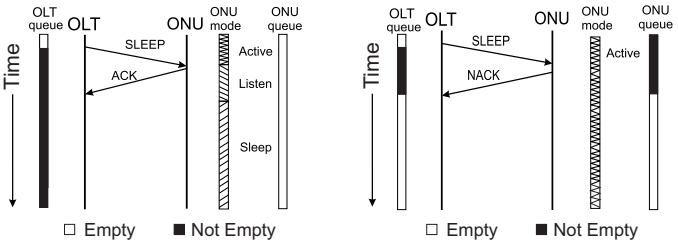
According to the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) $G.987.3$: "An attacker could connect a malicious device at various points on the infrastructure (e.g., by tampering with street cabinets, spare ports, or fibre cables). Such a device could intercept and/or generate traffic. Depending on the location of such a device, it could impersonate an OLT or alternatively it could impersonate an ONU." [8]. Authentication can encounter impersonation attacks among others, however registration-based authentication provides a basic level of authentication of the ONU to the OLT. It does not offer authentication of the OLT to the ONU; thus, mutual authentication is optional according to the operator's security policy [8]. The lack of OLT authentication in EPONs is highlighted by [9], [10]. They notice that EPONs contain an automatic discovery and registration process, while a standard authentication mechanism has not been defined. An attacker can introduce a fake OLT to the network that operates in promiscuous mode and disables the Logical Link Identification (LLID) filtering rules in order to eavesdrop sensitive information and gain access to the network resources. Once a non-legitimate OLT obtains sufficient knowledge of the network, it pretends to be a legal user and launches an attack.

Motivated by this security issue in EPONs, in this paper we assume that a fake OLT intervenes the legitimate OLT-ONU communication primarily to eavesdrop the downstream channel [11]. Being installed in the optical path, it can further affect protocols and mechanisms, such as the energy-aware one, which is under investigation in our analysis. Such a scenario is particularly challenging in case of battery-powered ONUs[1,2], since reducing the power requirements during battery operation benefits the ONU's battery life [12]–[14]. Furthermore, keeping track of the network devices' energy profiles helps in designing side-channel defence approaches where, for example, deviations from energy consumption norms could trigger alarms for attack [15].

Given the aforementioned assumption, we introduce a formal analysis approach to evaluate the impact of a MITM attack on an OLT-triggered energy-efficiency mechanism inspired by [2], [7]. The idea is to start with a formal representation of the network, energy-aware mechanism under investigation and attacker, and move on with the full state-space generation and exploration using sound analytical techniques, such as model checking, in order to derive quantitative results regarding the properties of interest. The full state-space exploration of the model gives to networks' analysts and designers the advantage of verifying their solutions under a variety of parameters much earlier than simulation or experimentation; this way balances between realism, due to the complete state-space generation, and experimentation complexity.

[1] https://www.yumpu.com/en/document/read/12016307/epon-onu-advanced-media-technologies

[2] http://www.huaweigpon.cz/wp-content/uploads/Huawei-SmartAX-MA567X-series-ONU-Brochure.pdf



(a) Sleep request acceptance (b) Sleep request refusal

Fig. 1: Message exchange of the energy-aware mechanism

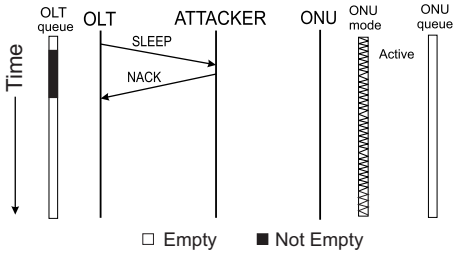


Fig. 2: Energy-efficient mechanism circumvention

The key contributions of this paper include: i) the formal analysis of a MITM attack in an EPON energy mechanism, ii) the design of a configurable model that relates energy and security aspects in EPONs, providing insights for a side-channel defence mechanism, and iii) the evaluation of the attack impact. The model's quantitative results show that the attacker significantly reduces the ONU's energy saving, and thus increases the EPONs' energy expenditure. To the best of our knowledge, this is the first work that assesses the energy impact of a MITM attack in an EPON network.

In the following, Section II briefly describes the attacker's intervention in an energy-aware mechanism. Model checking principles along with the proposed model's details are presented in Section III. Section IV discusses our verification results and Section V concludes the paper.

II. MITM ATTACK IN EPONS' ENERGY EFFICIENCY

The energy-efficient mechanism under analysis is a representative OLT-triggered scheme considering three power modes for the ONU, namely the active, listen and sleep mode [2], [7]. Both devices maintain their own queues, the OLT for the downstream packets and the ONU for the upstream traffic. In a nutshell, when the ONU is in the active mode can either receive downstream traffic or send upstream data. In case that no downstream traffic exists, the OLT sends a $sleep$ request to the ONU that triggers the sleep mode. If downstream packets arrive once a $sleep$ request has already been issued, the OLT begins to buffer them. When the ONU receives the $sleep$ message it decides whether to accept it or not, which depends on the presence of the upstream traffic in the ONU's queue. If the queue is empty and no upstream traffic exists, the ONU accepts the $sleep$ message, replies with an ack message and leaves the active mode, as shown in Fig. 1a. Otherwise, the ONU sends a $nack$ message and remains in the active mode until a new $sleep$ message is sent by OLT, as shown in Fig. 1b. In the latter case the ONU sends its upstream packets which is an indication for the OLT that the ONU remains active and buffering should be stopped.

Leaving the active mode (Fig. 1a), the ONU transits to the listen mode. This mode could be interrupted upon the appearance of upstream traffic which, in turn, causes the ONU to go back to the active mode. Transition from listen to active mode due to the upstream traffic arrival also entails that the OLT should stop buffering the downstream packets. If the listen mode has not been interrupted, the OLT continues to buffer its packets and after a configurable listen period and no traffic in either direction, the ONU transits to the sleep mode for an uninterrupted period of time, i.e., a configurable sleep period. During this period both downstream and upstream traffic are buffered in the corresponding queues. Once the sleep period duration has been completed, the ONU transits either to the active mode if there are buffered packets in queues or to the listen mode if no data appear while it was in the sleep mode. The listen mode is a good practice to avoid early active-to-sleep transitions, since the time consumed in listen-to-active transitions is negligible, but transitions from the sleep to active mode demand 2 ms [2]. According to [2], tuning the listen and sleep periods can efficiently balance the trade-off between the packets' delay and energy saving.

Such a mechanism could be easily circumvented by a MITM attack [16]–[18] with negative impact on the desirable energy-saving levels. In practice, the attacker sets up a fake OLT on the fiber connection between an ONU and the splitter to define a security mechanism with the legitimate ONU. Therefore, the ONU have no means to detect the fake OLT [11]. The legitimate OLT sends a $sleep$ request and buffers the packets that arrive in its queue. Then, the attacker, pretending the legitimate ONU, intercepts the $sleep$ requests and responds to the legitimate OLT with $nack$ instead of ack messages as shown in Fig. 2.Once the legitimate OLT receives the $nack$ message, it sends its buffered packets to the legitimate ONU. In practice, the attacker does not intercept any downstream data packets; it remains connected to the network to intercept only the $sleep$ messages from the legitimate OLT. As a result, the ONU is forced to stay in the energy-consuming active mode, which is particularly interesting in case of battery-powered ONUs [12]. In this paper, we present a novel model to evaluate the energy impact of such a MITM attack.

III. FORMAL VERIFICATION OF AN EPON MITM ATTACK

This work uses model checking as a means to formally verify a MITM attack on an EPON energy-efficiency mechanism. Model checking is a fully automated technique of verifying computer-based systems [19]- an EPON under MITM attack in our case - that will meet its requirements, e.g., in terms of energy-saving. Typically, given a system model, probabilistic model checking proceeds with a systematic exploration of the model's full state space to verify its desirable reachability properties [19]. This way, the energy-aware impact of a MITM attack on an EPON can be quantitatively verified through automatically checking all reachable states of its corresponding

TABLE I: Rates of the $EPON_{MITM}$ model

Rates	Description
λ_{down}	Packet's arrival rate in the downstream channel
λ_{up}	Packet's arrival rate in the upstream channel
μ	Packet service rate
$1/d\_listen$	Rate of staying in the listen mode
$1/d\_sleep$	Rate of staying in the sleep mode
$1000/2.88$	Rate of transition rate from the listen to the sleep mode
r_{fk}	Rate of fake OLT intervention

model, developed in line with the network's specifications, energy-aware parameters and attack behavior.

An EPON is a continuous real-time system mastered by packets' exchange over a fibre optic both in the downstream or upstream channel, while the energy-efficiency mechanism implemented at the ONUs' side is modeled by a Markov chain [3]. From a model checking perspective, the packets' arrival and service rates, the ONU's transition rates among its modes, i.e., active, listen and sleep, and the rate of a fake OLT intervention are perfectly matched with the Continuous Time Markov Chains (CTMCs) primitives, i.e., one can specify the rate of making a transition from one state to another [2], [19]. Probabilistic choice arises in case of race conditions, i.e., when two or more transitions in a state are candidates. CTMCs are amenable to analytical treatment and numerical computation. A relevant model regarding the computational and transmission cost of a security protocol in hardware-constraint devices also uses CTMC [20], while in [17], the authors exploit model checking and CTMCs as a means of verifying the resiliency of Near Field Communication (NFC) protocol against relay attacks.

In practice, we start with modeling the ONU energy-efficiency mechanism described in Section II; next, we aligned the model with the EPONs' specifications regarding for example, the rates in the downlink and uplink channels, the packets' length, and the queues in both sides; finally, we added the fake OLT entity to model the attacker's behavior. We released the proposed $EPON_{MITM}$ CTMC model as an open-source [3].

More specifically, our $EPON_{MITM}$ model, comprises 5 modules, namely $\mathcal{M} = \{M_{olt}, M_{onu}, M_{qolt}, M_{qonu}, M_{attck}\}$. M_{olt} and M_{onu} correspond to the legitimate devices, i.e., the OLT and the ONU, which transmit a number of data $packets$ in the downstream and upstream direction, respectively. The M_{onu} models the three modes of the ONU's operation which is considered to consume $3.85W$, $1.28W$ and $0.75W$ in the active, listen and sleep mode, correspondingly [2] (energy consumption levels are configurable parameters). These modules also deploy the energy-efficiency mechanism by synchronizing the control messages' exchange, i.e., $sleep, ack$ and $nack$. M_{qolt} and M_{qonu} represent the queues at the OLT and ONU side, respectively. They model the packets' arrival at each direction, their buffering once the ONU is in the sleep mode and their dropping when each queue is full. Finally, M_{attck} models the fake OLT which intervenes in the OLT-ONU message exchange and circumvents the energy-efficiency mechanism they have adopted.

[3]https://github.com/XeniaTsomp/ModelChecking.git

In brief, downstream data packets arrive at M_{qolt} with rate λ_{down} and the ONU receives them only in the active mode with service rate μ. If no downstream traffic exists, e.g., λ_{down} is light and M_{qolt} is empty, the OLT sends a $sleep$ request to the ONU which, based on the rate λ_{up} and the M_{qonu} status, can respond with an ack or $nack$ message. In case of ack response, the ONU transits from the active to the listen mode and stays to it for a time period d_listen. This period specifies the rate $1/d\_listen$ of staying in the listen mode. The time to transit from the active to the listen mode is of the nanoseconds' order and thus, the corresponding transition rate is not considered in the model. Once the listen period is expired, the ONU transits to the sleep mode with rate $1000/2.88$ which corresponds to the time, i.e., 2.88 μs needed by the ONU to turn off its transceiver [2]. The ONU stays to the sleep mode for a time period d_sleep which defines the rate $1/d\_sleep$ of staying in this mode. Table I summarizes all the aforementioned rates. In our model, the M_{onu} can skip the listen mode upon the traffic appearance, but it cannot interrupt the sleep period. Obviously, none of the above transitions occur and the ONU stays in the active mode, if it responds with $nack$ message due to the upstream traffic.

In case that a fake OLT circumvents the energy-efficiency mechanism, the broadcasted $sleep$ requests are received by it (downstream data packets are not affected); the module M_{attck} corresponds to the non-legitimate OLT device which acts as a man in the middle. We assume a sophisticated attacker whose intervention is not necessarily binary (0 or 1), but it is defined in line with the ratio r_{fk} (Table I). In practice, once the M_{attck} receives the transmitted $sleep$ requests, according to the r_{fk} parameter, it permanently responds to them with $nack$ messages, i.e., regardless of the upstream conditions. This way it forces the ONU to remain in the active mode even in cases that it would transit to the listen and sleep ones. We adopt two cases for the r_{fk} ratio: 0.5 and 0.99 in order to model the average and worst cases; in the latter case a MITM causes the greatest damage to an energy-aware mechanism such the one under investigation.

To analyze the MITM attack impact on the energy mechanism, the $EPON_{MITM}$ model is enhanced with reward structures (or "costs") that express the power consumption of ONU in the non-attack and attack cases. Cumulative rewards are employed to calculate the expected percentage of sleep requests acceptance and the levels of energy saving achieved by an energy mechanism under MITM attack. Their quantitative results are presented in Section IV.

IV. Quantitative Verification Results

The PRISM model checker [19] is used for the design and analysis of the proposed $EPON_{MITM}$ Markov model and the results are derived by a core i7 4.1 GHz machine with 8 GB of RAM. To align the model with the EPON's specification, we assume $C = 1.25$ $Gbps$ for both down and upstream channel and $l = 1518$ $bytes$ for packets' length [2].

Designing the $EPON_{MITM}$, we actually model the EPON under investigation as a finite-state transition system consisting of a number of states along with all transitions between them.For example, the ONU can transit from the state where it

TABLE II: $EPON_{MITM}$ state space results

		No Attack			Attack		
Transmitted packets	Traffic	Total states of S	Transitions	Time (sec)	Total states of S	Transitions	Time (sec)
10^3	downstream	766	1490	0.046	988	1919	0.167
10^3	upstream	154	266	0.032	156	268	0.041
2×10^3	down/up-streams	65 664	209 868	0.321	82 927	277 524	0.323

has received a $sleep$ request to the state in which it replies with a $nack$ message to the OLT because of no upstream traffic. For this model we assume an initial model state by defining the number of $packets$ that should be exchanged in an OLT-ONU communication, while we also specify the formula "finish" as a boolean expression controlling that all $packets$ have been eventually transmitted and received successfully. Satisfying the "finish" formula, the model reaches the final state. Transitions between states depend on the rates defined on Table I.

From the above, it is clear that the proposed model is mastered by the number of $packets$ transmitted either in down or upstream direction and Table II provides information about the state space produced in line with them. The columns denote the total number of model's states S, the number of transitions between them, and the time needed to solve the model. Downstream traffic modeling is more demanding compared to the upstream, which is intuitively expected, since the energy mechanism is OLT-triggered and the MITM attack is related to the downstream operation, e.g., both of them entail a large number of messages being exchanged. This also implies that the model state space is augmented in the presence of the attacker since the ONU remains in the active mode and forces the OLT to send sleep requests more frequently. It is also notable that combining traffic in both directions causes a non-linear increase in the model's state space. Its magnitude denotes the depth of this analysis, while the verification's requirements, in terms of hardware resources and time, show a clear advantage of the proposed approach compared to the cost and time-demanding experimentation-based approaches.

Once the model is built, model checking verifies the properties in interest. Properties are expressed in Continuous Stochastic Logic (CSL) and appropriately defined formulaes are used to verify them. Typically, a formula returns "yes" or "no" once a property is satisfied or not, respectively. In probabilistic model checking, a formula is evaluated over states and paths and returns the probability under question. In our case, a path formula ϕ is used as a parameter of the $P{\sim}p[.]$ operator and we employ the property $P =?\ (\phi)$ to evaluate the probability that the path formula ϕ is satisfied, i.e., the probability of certain events [20].

We start with the proof-of-concept property $P =?\ [F \leq C_0\ finish]$ to find and quantitative evaluate final states (F) before the time instant C_0, for which the formula "finish" is true. More explicitly, we define the CSL query:

$$Q_1 : \mathcal{P} =?\ [F \leq C_0\ finish], C_0 = 100,\ packets = 1000$$
$$\lambda_{down} = 0.2 \ldots 1,\ \mu = 1,\ r_{fk}$$
$$d_{listen} = 8\ ms,\ d_{sleep} = 20\ ms$$

whose explanation is "which is the probability that 1000 downstream packets will be transmitted by the OLT and

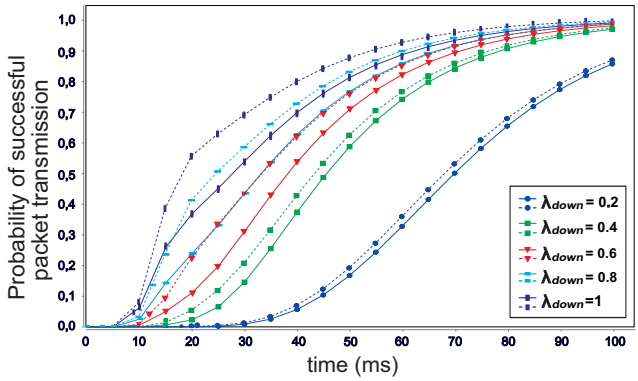


Fig. 3: Proof-of-concept-results in downstream traffic (a) non-attack (simple line), (b) attack (dashed-line) with $r_{fk} = 0.5$.

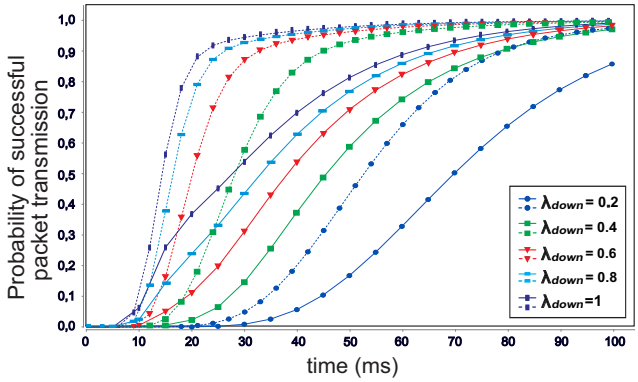


Fig. 4: Proof-of-concept-results in downstream traffic, (a) non-attack (simple line), (b) attack (dashed-line) with $r_{fk} = 0.99$.

received successfully by the ONU within 100 ms when packet arrival rate varies from 0.2×10^2 to 1×10^2 $packets/ms$, the service rate is 1 and no upstream traffic exists?". For the property defined in Q_1, we set the parameters of listening and sleep periods at 8 ms and 20 ms, respectively, since according to [2] this setup balances the trade-off between the packets' delay and energy saving. Obviously, their values can be appropriately tuned in respect to the EPON characteristics.

We execute the query Q_1 three times and derive the results illustrated in Fig. 3 and 4 for: (i) non-attack case (used as ground-truth scenario in both figures), (ii) attack case with fake OLT intervention rate $r_{fk} = 0.5$, and (iii) attack case with fake OLT intervention rate $r_{fk} = 0.99$. The verification process searches the full state space produced in order to find final states before C_0, for which the formula "finish" will be true. The state space consists of 766 states and 1490 transitions in the non-attack case, and it slightly increases with 988 states and 1919 transitions in the attack case, according to Table II.

Fig. 3 contrasts the non-attack case (simple line) with the

attack (dashed line) for $r_{fk} = 0.5$. We can see that the curves of probability move to the left as the downstream packet arrival rate, i.e., λ_{down}, increases. This indicates that the model is completed sooner. More specifically, when $C_0 = 100\ ms$, the curves corresponding to higher packet arrival rates reach probability 1.0, while those of $\lambda_{down} = 0.4$ and $\lambda_{down} = 0.2$ show that the model will be completed with probability 0.96 and 0.85, respectively. Arrival rates at the low side dictate light downstream traffic which entails higher probability for the OLT to send $sleep$ requests and for the ONU to respond with ack message. Thus, the ONU's transitions to the listen and sleep mode cause delays to the model. On the other hand, the attack case results show that the curves move slightly to the left, which entails that the model is completed sooner. Setting $r_{fk} = 0.5$ means that the fake OLT intervenes in the OLT-ONU communication and intercepts half of the $sleep$ requests messages; data packets are send and received without any disruption.

The consequences of the attack are more intense in case we set a high intervention rate, i.e., $r_{fk} = 0.99$. This indicates that the attacker receives almost all of the $sleep$ requests messages and thus none of them are received by the ONU. Fig. 4 shows that the curves representing the attack are moved further to the left compared to the attack case with $r_{fk} = 0.5$, which proves that the model needs even less time to be completed. A major difference from the no attack case is that, at time $C_0 = 100\ ms$, the model has been completed even for low arrival rates, e.g., $\lambda_{down} = 0.2$. Intuitively, such a behavior is anticipated since the ONU stays longer in the active mode due to the MITM attack. Our probabilistic model checking analysis contributes in quantifying the expected outcome, e.g., helps in decision making when a threshold in probability should be certainly reached.

Overall, the results of Fig. 3 and Fig. 4 verify and quantify the impact of network parameters, e.g., the packets' arrival rate, along with the attacker's behavior, expressed in line with the rate of intervention, on the probability of successful packet transmission and eventually on the model's time completion. In addition, Table II allows us to evaluate the way that the number of transmitted packets influences the state space; in model checking is critical to control the state space and detect the parameters that may result in spate space explosion.

Apart from the above probabilistic results, we use cumulative reward properties, to generate results associated with the expected energy saving in attack and non-attack cases, and this way, to assess the impact of the MITM attack. Results of Fig. 5 and 6 are derived through exhaustive verification of state space (Table II) which is a benefit over simulation-based techniques which only evaluate a finite number of traces. The form $\mathcal{R}_{\sim r}[C^{\leq t}]$ states that the expected reward cumulated up to time-instant t is $\sim r$, where the relation operator $\sim \in \{\leq, <, \geq, >\}$.

The initial expected consequence of the attack is the disorder of the exchanged $sleep, ack$ and $nack$ messages. Indeed, because of the attacker's intervention, the ONU does not receive the total number of sleep requests being sent by the OLT, which is reflected in the sleep requests acceptance ratio. We evaluate it through dividing the number of ack messages

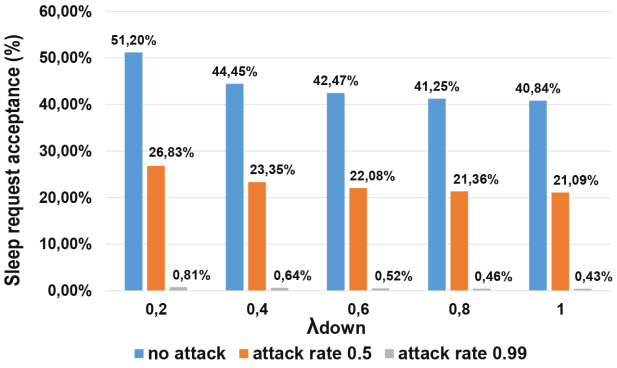


Fig. 5: The percentage of sleep requests acceptance

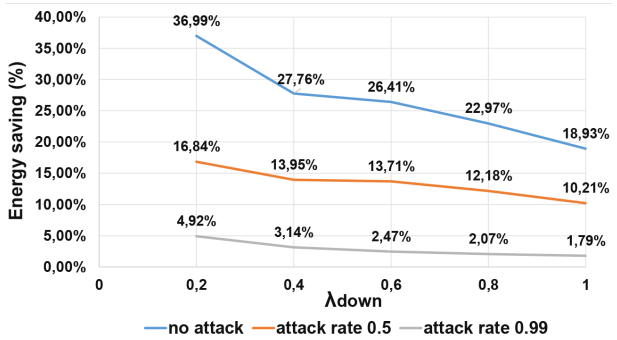


Fig. 6: Energy saving consequences of MITM

by the number of $sleep$ requests. The query the Q_2:

$$Q_2 : \mathrm{R}\{\text{“}sleep\text{”}\} =? \ [C \leq C_0], \ C_0 = 100, \ packets = 2000$$
$$\lambda_{down} = 0.2 \ldots 1, \ \lambda_{up} = 0.7 \ \mu = 1, \ r_{fk}$$
$$d_{listen} = 8\ ms, \ d_{sleep} = 20\ ms$$

and a similar one $Q_3 : \mathrm{R}\{\text{“}ack\text{”}\} =?$, with the same parameters, which correspond to cumulative reward properties calculating the expected number of $sleep$ request messages sent by the OLT (Q_2) and the expected number of ack response messages sent by the ONU (Q_3) within 100 ms of models' operation, time needed for model to be finished under the aforementioned parameters. We consider the realistic scenario of packets' transmission in both directions; we fix the upstream rate at 0.7×10^2 and vary the downstream one from 0.2×10^2 to 1×10^2 $packets/ms$.

Fig. 5 shows that the sleep requests' acceptance ratio decreases as the downstream packet arrival rate, λ_{down}, increases. The outcome is calculated for the non-attack scenario as well as for the attack scenario under the aforementioned intervention ratios for the fake OLT, i.e., $r_{fk} = 0.5$ and $r_{fk} = 0.99$. Indicatively, in non-attack conditions, our model starts with 51.20% sleep requests' acceptance ratio by the ONU when $\lambda_{down} = 0.2$ and results in 40.84% when $\lambda_{down} = 1$. In case that the fake OLT intervenes with $r_{fk} = 0.5$ the sleep requests' acceptance ratio drops to 26.83% when $\lambda_{down} = 0.2$ and even further to 0.81% for the same λ_{down} when the OLT discards almost every sleep request, i.e., $r_{fk} = 0.99$.

The models' behavior and results actually show that the influence of attack is greater at low rates compared to the

high ones, because low λ_{down} means that the OLT sends $sleep$ requests with higher probability and for a given λ_{up} the ONU accepts them with also high probability. Increasing traffic rate means that the ONU stays longer on the active mode, and thus, refuses requests for transitions in the sleep mode, e.g., it responds with $nack$ messages. We also conclude that the more the attacker receives the sleep requests from the legitimate OLT, the smaller the sleep request acceptance ratio by the ONU, which inevitably results in a lesser benefit in terms of energy saving as we show right afterwards.

In line with the previous outcome, the second tangible consequence regards the levels of energy saving which deteriorate when the energy mechanism is under attack. We derive the results of Fig. 6 defining the query Q_4:

$$Q_4 : \mathrm{R}\{\text{“}energy\_saving\text{”}\} =? \ [C \leq C_0], \ C_0 = 100$$
$$packets = 2000, \ \lambda_{down} = 0.2 \ldots 1, \ \lambda_{up} = 0.7 \ \mu = 1, \ r_{fk}$$
$$d_{listen} = 8 \ ms, \ d_{sleep} = 20 \ ms$$

Fig. 6 shows the impact of the MITM attack on the energy-efficiency mechanism in line with the λ_{down}. On the first place, we notice that energy saving decreases from 36.99% to 18.93% as λ_{down} increases from 0.2 to 1 in the no attack case. This is owed to the decrease of the sleep requests acceptance ratio confirmed in Fig. 5. Furthermore, our model assesses the impact of the attack and provides us with quantitative results which show that the energy saving is reduced from 16.84% to 10.21% when $r_{fk} = 0.5$ and even more from 4.92% to 1.79%, when $r_{fk} = 0.99$. Since the percentage of sleep requests acceptance is decreased under attack when λ_{down} increases, the ONU transits to sleep mode for even less period of time. Thus, it remains in active mode resulting to more energy consumption which is responsible for the reduction of energy saving. It is remarkable that the impact of attack is even more intense at low arrival rates, since it is expected that the ONUs will be in sleep mode during the non peak hours. According to our model, the energy saving is 36.99% in the non-attack case when $\lambda_{down} = 0.2$, which drops to 1.79% when $\lambda_{down} = 1$ in the attack case ($r_{fk} = 0.99$), which indicates that the attack results in an order of magnitude increase in energy expenditure.

V. Conclusions, countermeasures and future work

In conclusion, the quantitative results of the proposed analysis show the implications of a MITM attack on an EPON energy-efficiency mechanism. The results confirm that the attacker is responsible for the mechanism's disorder and reduction of the energy saving which concludes in network's high power consumption. An approach that would contribute in avoiding the energy-saving decrease in case of an attack is that the ONU supports a longer sleep period which avoids the frequent transitions among the ONU's modes and increases the energy saving by definition. However, a long sleep period causes packet delays and/or drops due to the longer queue waiting time when the ONU's transmitters are switched off. Thus, the trade-offs in energy, security, and performance requirements need to be investigated and definitely deserve a separate analysis.

We are currently working on cost-effective ways to face such an attack. We plan to implement an OLT-ONU authentication protocol to verify that both parties are legitimate, and to prevent a malicious user from impersonating one of them. The purpose is to introduce and analyze a by-design secure and energy-efficient mechanism for EPONs.

References

[1] Hajduczenia *et al.*, “On EPON security issues,” *IEEE Commun. Surv. Tutor.*, vol. 9, no. 1, pp. 68–83, 2007.

[2] S. Petridou, S. Basagiannis, and L. Mamatas, “Formal Methods for Energy-Efficient EPONs,” *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 246–259, 2018.

[3] S. Petridou, S. Basagiannis, and L. Mamatas, “Energy-efficiency analysis under QoS constraints using formal methods: A study on EPONs,” in *2017 IEEE International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.

[4] J. Zhang and N. Ansari, “Toward Energy-Efficient 1G-EPON and 10G-EPON with Sleep-Aware MAC Control and Scheduling,” *IEEE Commun. Mag.*, vol. 49, no. 2, pp. 33–38, Feb., 2011.

[5] A. F. Pakpahan and I.-S. Hwang, “Adaptive ONU Energy-Saving via Software-Defined Mechanisms in TDMA-PON,” in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2018, pp. 137–142.

[6] D. P. Van *et al.*, “Energy-saving framework for Passive Optical Networks with ONU sleep/doze mode,” *Optics express*, vol. 23, no. 3, pp. A1–A14, 2015.

[7] M. Fiammengo, “Sleep mode scheduling technique for energy saving in TDM-PONs,” M.S. thesis, KTH, School of Information and Communication Technology, Stockholm, Sweden, 2011.

[8] I.-T. G.987.3, “10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification,” Geneva, Jan., 2014.

[9] A. Yin and Y. Ding, “Design of a mutual authentication based on NTRUsign with a perturbation and inherent multipoint control protocol frames in an Ethernet-based passive optical network,” *Optical Engineering*, vol. 53, no. 11, p. 115101, 2014.

[10] A. Yin, Q. Li, and M. Zhu, “Secure authentication scheme for 10 Gbit/s Ethernet passive optical networks,” *Optik*, vol. 125, no. 20, pp. 5947–5951, 2014.

[11] L. C. Paolo de Lutiis, Roberta D’ amico, “Next Generation Access Network (in)security,” in *4th ETSI Security Workshop*. Telecom Italia Group, 2009.

[12] S. Gorshe *et al.*, *“Broadband access: Wireline and Wireless-Alternatives for Internet Services”*. John Wiley & Sons, 2014.

[13] H. Ujikawa, T. Yamada, and N. Yoshimoto, “Demonstration of timer-based ONU deep sleep for emergency communication during power failure,” in *2013 IEEE Global Commun. Conf.*, 2013, pp. 2413–2417.

[14] X. Zeng, M. Zhu, L. Wang, and X. Sun, “Optimization of sleep period in watchful sleep mode for power-efficient passive optical networks,” *Photonic Network Communications*, vol. 35, no. 3, pp. 300–308, 2018.

[15] L. Wang, Z. Zhu, Z. Wang, and D. Meng, “Analyzing the security of the cache side channel defences with attack graphs,” in *2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2020, pp. 50–55.

[16] Z. Sun, Y. Ma, F. Sun, and Y. Wang, “Access Control For Distribution Automation Using Ethernet Passive Optical Network,” in *Power and Energy Engineering Conference (APPEEC), Asia-Pacific*. IEEE, 2010, pp. 1–4.

[17] N. Alexiou, S. Basagiannis, and S. Petridou, “Formal security analysis of near field communication using model checking,” *Computers & Security*, vol. 60, pp. 1–14, 2016.

[18] W. L. Bo Gao, “Method and apparatus for authentication in passive optical network and passive optical network thereof,” German Patent EP 2 426 866 B1, September 04, 2013.

[19] M. Kwiatkowska, G. Norman, and D. Parker, “Probabilistic model checking: Advances and applications,” in *Formal System Verification*. Springer, 2018, pp. 73–121.

[20] S. Basagiannis, S. Petridou, N. Alexiou, G. Papadimitriou, and P. Katsaros, “Quantitative analysis of a certified e-mail protocol in mobile environments: A probabilistic model checking approach,” *Comput. & Security*, vol. 30, no. 4, pp. 257–272, Jun 2011.