

Received November 5, 2021, accepted December 8, 2021, date of publication December 10, 2021, date of current version December 27, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3134671

# DDoS Attack Mitigation Based on Traffic Scheduling in Edge Computing-Enabled TWDM-PON

YAJIE LI<sup>1,2</sup>, YINGQI ZHAO<sup>1</sup>, JUN LI<sup>2</sup>, XIAOSONG YU<sup>1</sup>, (Member, IEEE),  
YONGLI ZHAO<sup>1</sup>, (Senior Member, IEEE), AND JIE ZHANG<sup>1</sup>, (Member, IEEE)

<sup>1</sup>State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

<sup>2</sup>Jiangsu Engineering Research Center of Novel Optical Fiber Technology and Communication Network, Soochow University, Suzhou 215031, China

Corresponding author: Yongli Zhao (yonglizhao@bupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China (NSFC) Project under Grant 61901053, Grant 61822105, Grant 61831003, and Grant 62101372; in part by the Fundamental Research Funds for the Central Universities under Grant 2021RC12; and in part by the Project of Jiangsu Engineering Research Center of Novel Optical Fiber Technology and Communication Network, Soochow University under Grant SDGC2117.

**ABSTRACT** Time-Wavelength Division Multiplexing Passive Optical Network (TWDM-PON) is considered as a promising solution of next generation PON (NG-PON). The integration of Edge Computing (EC) and TWDM-PON can satisfy the QoS requirements of delay-sensitive applications by providing storage, processing and caching capabilities at the network edge. However, with limited resource capacity, edge nodes in TWDM-PON are vulnerable to network attacks, e.g., Distributed Denial of Service (DDoS) attacks. Resource exhaustion in the attacked nodes easily leads to QoS degradation and even service blocking. This paper investigates how to effectively schedule traffic to mitigate the DDoS attack in EC-enabled TWDM-PON. Based on the collaboration of edge nodes, an adaptive traffic scheduling algorithm is designed to minimize the impact of DDoS attacks on delay sensitive services. The performance of the proposed algorithm is evaluated in simulation, where direct and indirect DDoS attacks are simulated. Besides, the attack duration and the number of attacked nodes are considered in the evaluation. Simulation results show that the proposed algorithm can effectively mitigate DDoS attacks in terms of reducing the QoS degradation rate and blocking rate of delay-sensitive services.


**INDEX TERMS** DDoS attack mitigation, edge computing, traffic scheduling, TWDM-PON.

## I. INTRODUCTION

With the emergence of the Internet of Things (IoT) and emerging 5G applications, a large amount of data will be generated at the edge of the network. These data will be transferred to the conventional centralized cloud for storage and processing [1]. The traditional centralized cloud has higher storage and processing capabilities, but it is far from the user terminals. Long-distance data transmission on networks with large amounts of data will cause some potential problems, such as unacceptable delays and unstable connections when transferring computing tasks to cloud computing servers [2]. These shortcomings make it difficult to meet the Quality of Service (QoS) of novel delay-sensitive applications. To address this challenge, Edge Computing (EC) has

been conducted in academia and industry [3], [4]. This technology provides cloud-like computing, storage and network functions at the edge of the network close to the user [5], thus opening the door for applications with strict latency requirements, such as Augmented Reality (AR), Virtual Reality (VR) [6].

As one of the widely deployed access technologies [7], Passive Optical Networks (PONs) have been recently receiving significant attentions in multi-disciplinary research areas. This technology can greatly alleviate the last-mile bandwidth bottleneck problem and support the time-critical services [8]. The traditional time division multiplexing PON (TDM-PON) is increasingly unable to meet the increasing bandwidth requirements of users, and the industry has begun to study next-generation PON (NG-PON) and standardization work. Time-Wavelength Division Multiplexing PON (TWDM-PON) combines the respective advantages of TDM-PON

The associate editor coordinating the review of this manuscript and approving it for publication was Tianhua Xu .

and Wavelength Division Multiplexing PON (WDM-PON), becoming the most competitive NG-PON solution [9]. In this regard, EC can be integrated with existing PONs, forming EC enabled PONs, to support the services with ultra-low latency requirements. In such EC enabled PONs, there are several ways to integrate EC with PONs, such as deploying EC nodes (e.g., cloudlet, micro data center) with Remote Nodes (RNs), Optical Network Units (ONUs) [10], or Optical Line Terminal (OLT) [11] to satisfy the latency requirements of time-critical services.

With the advantages of supporting time-critical services, EC-enabled PONs still faces with several security challenges [12]. To control network cost, each EC node usually has limited resources (i.e., computing and storage) [1]. Thus, compared with a cloud node with huge resources, EC nodes are much more sensitive to Distributed Denial of Service (DDoS) attacks [13], which disrupt legitimate services by sending a large number of malicious requests to exhaust network resources [14]. When attacked by DDoS, EC nodes are easily overloaded, which may cause the QoS degradation or even service interruption. Therefore, it is significant to investigate the mitigation of DDoS attacks to guarantee the QoS of services as much as possible.

Since load balancing is proved to be an effective method to mitigate DDoS attacks, some research has been conducted to mitigate DDoS attacks through computing offloading in edge nodes. In [15], a multi-level framework based on edge computing was designed to defend DDoS attacks for perception nodes in Industrial Internet of Things. A solution was proposed to relieve the overloaded server by redirecting incoming requests to nodes at the edge of networks in [16]. The authors in [17] proposed a novel cooperative task offloading scheme to avoid DDoS attacks in a secure and sustainable mobile Cloudlet network. In [15]–[17], edge resource was leveraged to detect and defend DDoS attacks in the cloud. However, the security of edge nodes in DDoS attacks has not been addressed.

In addition, a lot of studies have been proposed to dynamically offload computing services in the EC-deployed network [18]. For example, energy consumption or system costs can be reduced by optimizing offload decisions and effectively allocating resources [19]–[21]. By jointly optimizing the calculation and resource allocation of the load strategy, the total cost of energy, calculation and delay for all users was minimized in [19], and the energy consumption of users was minimized in [20] and [21]. The author in [22] proposed an effective distributed computing offloading algorithm to achieve the optimal offloading decision of vehicles in the vehicle network. However, these works only focus on optimizing network performance and the security of EC nodes is not considered. To the best of our knowledge, seldom works investigate how to mitigate DDoS attacks faced by EC nodes to guarantee the QoS in EC-enabled TWDM-PON.

This paper focuses on the scenario where EC nodes attached to ONUs are attacked by DDoS in TWDM-PON. The target is to minimize the impact of DDoS on the services

by optimizing the traffic scheduling. Our previous work proposed a traffic scheduling strategy based on the coordination of EC nodes [23]. This paper extends the previous work from the following three aspects.

- 1) The previous algorithm is updated by optimizing the process of traffic scheduling, including the trigger mechanism and the selection of target nodes.
- 2) Simulation is optimized by updating simulation setup and benchmark algorithms. Specifically, in the previous benchmark, EC-ONU and EC-OLT independently complete the processing of services with different delay requirements. The benchmark in this paper considers the collaboration between EC-ONU and EC-OLT to complete traffic scheduling.
- 3) As for the type of DDoS attacks, the previous work only considers one type of DDoS attack while this paper adopts two types of DDoS attack, namely direct attack and indirect attack. More simulation results are obtained to verify the proposed scheduling strategy. Simulation results show that the proposed algorithm can effectively reduce the QoS degradation rate and blocking rate of delay sensitive (DS) services.

The rest of the paper is structured as follows. Section 2 introduces the edge computing-enabled TWDM-PON, including network model and latency calculation. Section 3 describes two types of DDoS attacks and illustrates the addressed problem in this paper. Section 4 details the proposed traffic scheduling strategy, including collaborative computing offloading and resource allocation optimization schemes. Section 5 provides the setup of network simulation. The performance evaluation and analysis of the algorithm are given in Section 6. Finally, Section 7 draws conclusions.

## II. EDGE COMPUTING-ENABLED TWDM-PON

### A. NETWORK MODEL

Since the conventional dynamic bandwidth allocation (DBA) generates some latencies from the report and gate mechanism and bandwidth calculation [24], it cannot guarantee the low-latency requirement. The EC servers with computing resources are deployed on each ONU and OLT in TWDM-PON. Specifically, EC servers are connected to ONUs through fiber link. With ONUs integrated with access point or base station, end users can access ONUs by a fixed or wireless network [1], [10]. The resource capacity in the EC node connected to OLT (i.e., EC-OLT) is higher than the EC node associated with ONUs (i.e., EC-ONUs). This integration of EC and TWDM-PON allows DS services to be processed in the local EC-ONU (i.e., the nearest ONU to users) to meet strict latency requirements.

In this paper, considering heavy traffic load under DDoS attacks, two transmission mechanisms are available to support the communication among EC-ONUs. The first case is to direct the traffic from one EC-ONU node to another via direct looping at a RN with an additional control wavelength ( $\lambda_3$  in Fig. 1) [8]. With a fiber Bragg grating deployed near the RN, this wavelength is selectively reflected back

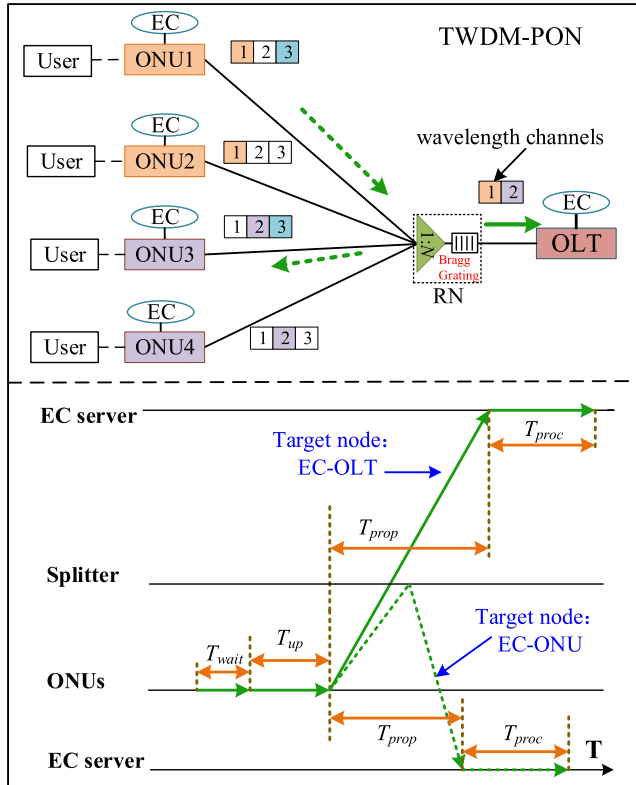


FIGURE 1. Edge computing-enabled TWDM-PON.

to the ONUs. As a decentralized DBA, this control wavelength enables ONUs to take turns transmitting, according to a pre-defined sequence. In the second case, the traffic needs to be transmitted via OLT using the existing wavelengths for upstream ( $\lambda_{u1} - \lambda_{u2}$ ) and downstream ( $\lambda_{d1} - \lambda_{d2}$ ) of TWDM-PON. Thus, two mechanisms do not affect each other by using different wavelengths. For simplicity, only the former method is shown in the network model in Fig. 1.

Due to the coexistence of two communication mechanisms, two transmitters need to be deployed at each ONU. Under normal circumstances, DS services will only be processed in the local EC-ONU, and delay tolerant (DT) services will be transmitted to EC-OLT for being processed. Therefore, only one transmitter needs to be activated. When the ONU is attacked by DDoS, another wavelength ( $\lambda_3$ ) transmitter will be used for scheduling services to other ONUs. This scenario will increase the cost and energy consumption, but can greatly improve the flexibility of traffic scheduling under high load.

### B. LATENCY CALCULATION

The total time  $T$  for services includes four parts [25]: waiting latency  $t_w$ , upload latency  $t_{up}$ , propagation latency  $t_{prop}$  and processing latency  $t_{proc}$  in Fig. 1.

#### 1) WAITING LATENCY

The waiting latency is also known as the queuing latency, which is caused by the mechanism of time division

multiplexing transmission in TWDM-PON in this paper. For example, there are  $m$  ONUs in TWDM-PON,  $n$  wavelength channels on the uplink. For simplicity, we only consider the case where  $m/n$  is an integer.  $m/n$  ONUs will share a wavelength channel in the communication process, then the waiting delay is equal to the total waiting time of the first  $(m/n-1)$  ONUs. In other words, the  $(m/n)^{th}$  ONU needs to wait until all the other ONUs have completed transmission. Therefore, the waiting latency of  $t_w$  in Eq.(1) equals to the total transmission latency of the former  $(m/n-1)$  ONUs, which denotes the waiting latency of all ONUs to get the available time slots.

$$t_w = \sum_{i=m/n-1} t_s^i \quad (1)$$

where  $m/n$  is the number of ONUs sharing a wavelength channel, and  $t_s^i$  indicates the transmitting latency of the  $i^{th}$  ONU.

#### 2) UPLOAD LATENCY

The upload latency is mainly related to the uplink rate in the PON. The current uplink rate of TWDM-PON is basically 10Gbps. Thus, the upload latency can be basically regarded as a constant or even negligible when the data volume is small.

$$t_{up} = B_i^j / r_d \quad (2)$$

where  $r_d$  is the upstream data rate and  $B_i^j$  defines the size of the input data of the computation task from the  $i^{th}$  ONU at the  $j^{th}$  EC server.

#### 3) PROPAGATION LATENCY

The propagation latency is generated by the transmission of optical signal in the fiber, which is indicated as  $t_{prop}$ . With  $5 \mu s$  each kilometer, the propagation latency is commonly linear with the physical transmission distance. Note that  $t_{prop}$  is considered as the main bottleneck of the one-way transmission latency [26].

$$t_{prop} = S_p \times L \quad (3)$$

where  $S_p$  is propagation delay on the fiber, and  $L$  is the propagation distance.

#### 4) PROCESSING LATENCY

In this study, the processing latencies in the EC-enabled TWDM-PON is mainly the processing latency of the EC servers, indicated as  $t_{proc}$ . Each EC server is considered as one entity to handle traffics from the ONUs. In detail,  $t_{proc}$  commonly includes the computing latency and other execution latencies from the EC servers.  $c_i^j$  defines the complexity of the input data of the computation task from the  $i^{th}$  ONU at the  $j^{th}$  EC server. The computing resources (i.e., CPU cycles per second) required by the services can be obtained by multiplying  $B_i^j$  and  $c_i^j$ .  $R_a$  indicates the computing resources allocated by the  $j^{th}$  EC server to each service. According to the service delay requirements, EC servers will allocate the required computing resources to process the input data

from ONUs. The calculation formula of  $R_a$  will be explained in detail in the next section, and the computing latency of the required computation task of the  $i^{th}$  ONU by  $j^{th}$  EC server is formulated as Eq. (4)

$$t_{proc} = B_i^j \times c_i^j / R_a \quad (4)$$

In addition, there are some other execution latencies executed by the EC server, e.g., the time overhead for services forwarded to other ONUs via EC-OLT, and queuing latency. Since these are much smaller than the computing latency, these small latencies are neglected in  $t_{proc}$ .

### III. PROBLEM DESCRIPTION

#### A. DDOS ATTACK MODEL

Since EC-ONUs are responsible for processing DS services, the DDoS attacks on EC-ONUs will cause severe effects on users. This paper only considers the network scenario where EC-ONUs are attacked by DDoS. Note that compared with DoS, DDoS refers to the distributed DoS attacks, where multiple nodes are attacked in the network. Here, we consider two kinds of DDoS attacks in TWDM-PON, which cause the resource exhaustion of EC-ONU nodes [27].

- 1) Indirect DDoS attack. External attackers may maliciously modify the attributes of services and increase the demand of computing resources for the selected services. Thus, the computing resources will be overused than normal cases, which leads to the overloading of some nodes.
- 2) Direct DDoS attack. The attacker can directly obtain the management and control privilege of the target server. By modifying the server resource configuration (e.g., CPU), the target server can't provide adequate computing resources for the services in a certain period of time.

#### B. PROBLEM DEFINITION

According to the above DDoS attack models, when EC-ONUs are attacked, the DS services may suffer from QoS degradation or interruption due to insufficient resources. Fig. 2 shows different traffic scheduling schemes for DS services under DDoS attacks. When EC-ONU2 is attacked by DDoS, the usage of computing resources will be overloaded. If the DS services continue to be processed on the local EC-ONU, the QoS will be degraded since the delay requirement is not satisfied [28]. In this case, we can achieve resource sharing through the coordination of edge nodes to schedule services.

Two traffic scheduling schemes are depicted to schedule DS services in Fig. 2. Scheme 1 adopts the shortest delay policy and all the EC-ONUs and EC-OLT are traversed to calculate the total delay of each candidate path. With the shortest delay  $t_1$ , the DS service is offloaded to the node EC-ONU4. However, this scheduling policy might easily lead to the high computing load in the offloading node, e.g., EC-ONU4, which affects the processing of upcoming DS services. In contrast, scheme 2 jointly considers the

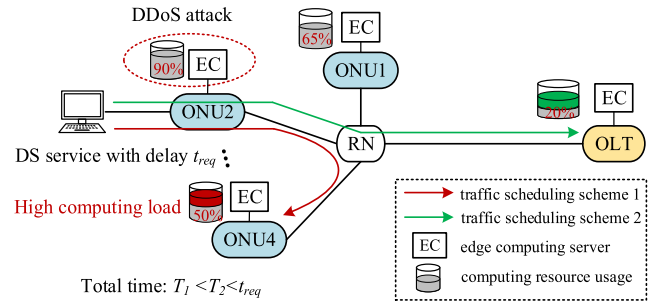


FIGURE 2. Traffic scheduling for DS services under DDoS attacks.

TABLE 1. Notations description.

Notations	Description
$S_i$	The $i^{th}$ service, $i \in [1, N]$
$\mu_i$	Scheduling decision (0, 1, -1)
$T_{k,j}^i$	Total delay of offloading the $i^{th}$ service from EC-ONU $_k$ to EC-ONU $_j$
$T_{k,OLT}^i$	Total delay of offloading the $i^{th}$ service from EC-ONU $_k$ to EC-OLT
$C_{ONU}^n$	Resource utilization of the $n^{th}$ EC-ONU
$C_{OLT}$	Resource utilization of EC-OLT
$CU_{ONU}^n$	Computing resources of the $n^{th}$ EC-ONU
$CU_{OLT}$	Computing resources of EC-OLT
$\tau_i$	The final scheduling path of the $i^{th}$ service
$t_r^i$	Delay requirement for the $i^{th}$ service

QoS requirement and computing resource usage during the traffic scheduling. With the premise of ensuring QoS requirement, EC-OLT is finally selected as offloading target and the total delay is denoted as  $t_2$ . We can see that both schemes can satisfy the delay requirement of DS services. Although  $t_1 < t_2$ , scheme 2 can effectively balance the network resource usage and QoS requirement. Therefore, both QoS requirement and resource usage should be considered when designing traffic scheduling strategies, so as to minimize the impact of DDoS attack on DS services.

### IV. ADAPTIVE TRAFFIC SCHEDULING ALGORITHM

This section introduces a novel Adaptive Traffic Scheduling (ATS) algorithm to schedule DS services under DDoS attacks. Considering DS services generally bring more benefits than DT services, this algorithm aims to minimize the impact of DDoS attacks on DS services. The traffic scheduling problem is divided into two sub-problems, that is, route scheduling and resource allocation, which are detailed in Sections 4-A and 4-B, respectively. Finally, the details of ATS scheme are described and its complexity is analyzed in Section 4-C.

#### A. ROUTE SCHEDULING

To simplify the algorithm description, some symbols are predefined as follows. Let  $S_i$  denote the set of computation



tasks,  $i \in [1, N]$ . The scheduling decision of  $S_i$  is denoted as  $\mu_i \in \{0, 1, -1\}$ , where  $\mu_i = 0, 1, -1$  indicates that the task  $S_i$  is processed in the local EC-ONU, other EC-ONUs, and EC-OLT, respectively. Without DDoS attacks, the value of  $\mu_i$  for DS and DT services is 0 and  $-1$ , respectively. When DDoS attacks EC-ONUs nodes, the  $\mu_i$  of DT services in the attacked node is still  $-1$ . However, the value of  $\mu_i$  for DS services is modified according to ATS algorithm in this paper.

From the analysis of latency calculation in Section 2-B, the delay of scheduling services to other nodes is composed of four parts, while that of services processed in the local EC-ONU is equals to processing latency. This means that the performance of a few DS services with strict delay requirements will be degraded if they are scheduled to other nodes. This type of services can meet delay requirements only if the local EC-ONU has sufficient resources.

---

#### Algorithm 1 Adaptive Traffic Scheduling (ATS) Algorithm

---

**Input:** Topology ( $m$  EC-ONUs, OLT), service request  $S_i$  arriving at the attacked node EC-ONU $_k$

**Output:** offloading target, scheduling path  $\tau_i$

```

1: for request  $s \in S_i$  do
2:   if  $s$  is DT service then
3:     select EC-OLT as destination
4:   else if  $s$  is DS service
5:     traverse all the edge nodes, calculate  $T_{k,OLT}^i$  and  $T_{k,ONU}^i$ 
6:     if  $\min\{T_{k,ONU}^i, T_{k,OLT}^i\} > t_r^i$  then
7:       select local EC-ONU $_k$  as destination
8:     else
9:       if  $CU_{ONU}^n \times (1 - C_{ONU}^n) \leq CU_{OLT} \times (1 - C_{OLT})$ 
then
10:        select EC-OLT as destination
11:      else
12:        select the EC-ONU with the lowest resource
utilization
13:        select transmission mechanism with minimum
 $t_w$  as  $\tau_i$ 
14:      end if
15:    end if
16:  end if
17: if  $T_n^i \geq \alpha \times t_r^i$  then
18:    $s$  will be discarded
19: else if  $T_n^i \geq t_r^i$ 
20:   QoS of  $s$  will be degraded
21: end if
22: update the network status and usage of edge nodes
23: end for

```

---

The processing flows of the proposed ATS algorithm are described as follows. For simplicity, we focus on the network scenario where one EC-ONU is attacked by DDoS since the case of multiple attacked nodes can be analyzed similarly. When the node EC-ONU $_k$  is attacked, the other  $m-1$  EC-ONUs will be traversed to calculate the total delay of offloading the service  $S_i$ , which are denoted as  $T_{k,ONU}^i = \{T_{k,j}^i\}, j \in [1, k) \cup (k, m]$ . In addition, the delay of offloading service  $S_i$

at EC-OLT is expressed as  $T_{k,OLT}^i$ . The total delay is the duration from the arrival of a service to the end of being processed in the target edge node. Only if  $\min\{T_{k,ONU}^i, T_{k,OLT}^i\} > t_r^i$ , the service will attempt to be processed in the EC-ONU $_k$ . Otherwise, the service  $S_i$  will be scheduled to other EC-ONUs or EC-OLT for being processed, that is,  $\mu_i$  of  $S_i$  changes from 0 to 1 or  $-1$ .

When the service is offloaded to other nodes, it is necessary to calculate the optimal offloading target node at this time. Among all the paths that meet the delay requirements, the node with the lowest utilization of computing resources is selected as the target node. It is worth noting that if the target node is other EC-ONUs, two transmission mechanisms are available to enable the traffic offloading between EC-ONUs. In this case, the transmission mechanism with the shorter queuing time will be selected for the service. Note that each task consists of multiple packets and each packet can carry 1518 bytes at most. Here the queuing time is divided into two parts. First, the task must wait for transmission according to the granted polling cycle. Second, multiple polling cycles may be required to schedule the service with large size of data. Thus, the queuing time depends on not only the data size of the service, but also the number of polling cycles granted by different transmission mechanisms.

#### B. ALLOCATION OF COMPUTING RESOURCES

The value of  $R_a^i$  for each service is calculated according to the delay requirement  $t_r^i$ . The delay requirement here is not the traditional round-trip time. Due to the small amount of data in the task calculation result, the downlink time can be ignored. Therefore, we only consider the uplink time, that is, the time from the service arriving at the ONU to the end of being processed. The allocated resources are given as:

$$R_a^i = (B_i^j \times C_i^j) / (\alpha t_r^i - t_{prop}^i - t_w^i - t_{up}^i) \quad (5)$$

$R_{a1}^i$  and  $R_{a2}^i$  can be obtained when  $\alpha = 1$  and  $\alpha = 10$ , respectively, and the specific resource allocation depends on the remaining idle resources  $R_{re}^m$  in the node.

Therefore, the latency requirements can be satisfied only if the remaining resources  $R_{re}^m$  in the target node are higher than  $R_{a1}^i$ . When  $R_{re}^m$  is less than  $R_{a2}^i$ , the total delay of the service is longer than  $10t_r^i$ , which is far beyond  $t_r^i$ . In this case, the service will be directly blocked. If  $R_{re}^m$  is between  $R_{a1}^i$  and  $R_{a2}^i$ , the total time will exceed the latency requirement, which leads to QoS degradation of the service  $S_i$ .

#### C. ANALYSIS OF TIME COMPLEXITY

The time complexity of the proposed algorithms is analyzed as follows. Since we need to consider all nodes in the proposed algorithm, we must traverse the entire solution space and enumerate all the possible offloading decisions of the service for comparison. Therefore, the time complexity for proposed algorithm ATS is  $O(N \times m \times 2)$ , where  $N$  is the number of computing tasks that arrive, and  $m$  is the number of edge nodes in TWDM-PON. In addition, there are

**TABLE 2.** Simulation parameters.

Simulation Parameters	Value
Services number	50000
Simulation times	20
Data size of services	[300, 800] KB
Complexity level of services	[1,2,3,4]
Delay requirements of DT services	[50,200] ms
Delay requirements of DS services	[5,50] ms
DT/DS services	1:1
Computation capacity of EC-ONU	2GHz
Computation capacity of EC-OLT	16GHz
Cycle duration of ONU-OLT	2ms
Cycle duration among ONUs	0.5ms
Propagation delay on the fiber	5us/km

two transmission mechanism options for services scheduled to other EC-ONUs.

## V. SIMULATION SETUP

In this section, simulation is conducted to analyze the performance of the traffic scheduling strategy based on edge computing when EC-ONUs are attacked by DDoS.

### A. PARAMETER SETUP

We consider a 100 km long reach PON (LR-PON) consisting of an OLT and 16 ONUs. Note that the number of ONUs in LR-PON can be set to different values. In the simulation, the split ratio does not affect the performance evaluation of the proposed algorithm. The RN is assumed to be located 90 km away from the OLT and ONUs are placed randomly in the last 10 km of the 100 km network span. Four upstream transmission wavelengths are used and the bit rate of each channel is 10 Gb/s. Other simulation parameters are depicted in Table 2. The boundary of distinguishing DS services and DT services is 50 ms. The arrival process of services in the network is subject to Poisson distribution. It should be noted that the proposed algorithm is not constrained to a certain distribution of service arrival. Meanwhile, the data size of services is hundreds of kilobytes ranging from 300 to 800 KB, which is applicable to the EC applications in IoT scenario [10].

### B. SIMULATION OF DDoS ATTACK

The details of simulating two types of DDoS attacks in Section 2 are given as follows.

- 1) In indirect attack case, the attributes of DS services will be modified by the attacker. Specifically, the computation complexity of DS services is maliciously increased. To ensure the QoS requirements, more computing resources are occupied in the EC-ONUs, leading to the significantly higher usage or the exhaustion of computing resources. In this case, EC-ONU nodes are considered as the attack target. Since DS services generally require more computing resources than DT services, this method causes severer resource exhaustion, which brings more benefits for the attacker. In the

simulation, the computation complexity is increased by 6 times for 20% DS services.

- 2) In direct attack case, the computing resource configuration in EC servers are directly changed by the attackers. The attack is assumed to last for a period of time, which is from the arrival of the  $x^{th}$  service request to the arrival of  $y^{th}$  service request. In more details, the available computing resources in the attacked server will be directly reconfigured to a low level when the  $x^{th}$  service request arrives. The original resource configuration will be recovered until the  $y^{th}$  service arrives. It means that the duration of DDoS attack is  $T_{x-y}$ . In the simulation, the available computing resources of the attacked server is reconfigured to 60% during the attack.

## C. BENCHMARK ALGORITHMS

To evaluate the effectiveness of ATS algorithm, we conduct a comparison with the following two approaches, traffic scheduling-OLT (TS-OLT) and traffic scheduling-ONU (TS-ONU). The former prefers to offload DS services to EC-OLT for processing. EC-ONUs can also server as offload targets only if computing resources are not available in EC-OLT. On the contrary, the latter gives a priority to EC-ONUs during the selection of offloading target. The DS services will be offloaded to EC-OLT unless the resources become insufficient in EC-ONUs. With a low time calculation complexity, TS-OLT algorithm can avoid affecting other DS services due to traffic scheduling. In contrast, TS-ONU algorithm can greatly reduce the transport bandwidth in TWDM-PON.

## D. PERFORMANCE METRICS

The performance of the proposed algorithm is evaluated in terms of two kinds of metrics, including the ratio of affected services and resource utilization in EC-ONUs and EC-OLT. Meanwhile, regardless of DT or DS services, the affected services in DDoS attack consist of blocking and QoS degradation. As mentioned in Section IV-B, the time threshold of service blocking is ten times the threshold of QoS degradation. Resource utilization refers to the ratio of the occupied computing resources to the total computing resources in EC-ONUs and EC-OLT. With dynamic traffic, the resource utilization varies with time during the simulation. The average resource utilization and real-time resource utilization are considered in indirect and direct DDoS attacks, respectively. Specifically, in indirect DDoS attack, we record the resource utilization when each service leaves. Thus, with 50000 services in total, resource utilization is the average value of all samples when all services leave in simulation. In contrast, the real-time resource utilization is recorded in the case of direct DDoS attack.

## VI. RESULT ANALYSIS

### A. INDIRECT DDoS ATTACKS

Two cases are considered in the scenario of indirect DDoS attacks, including the variation of traffic load and different

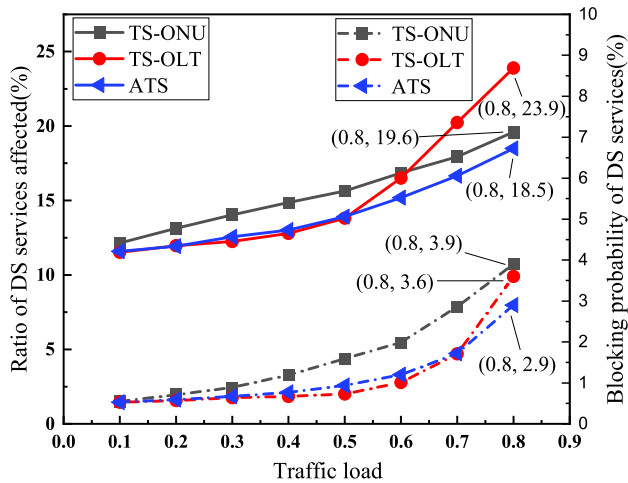


FIGURE 3. Ratio of DS services affected vs. traffic load.

number of attacked nodes. The resource occupancy threshold is set to 60%. It means that traffic scheduling is carried out once resource utilization ratio in EC-ONUs is higher than 60%.

### 1) VARIATION OF TRAFFIC LOAD

In this case, six ONUs are attacked by indirect DDoS. To ensure that node overload is caused by DDoS attack instead of high traffic load, traffic load should be set in an appropriate range in simulation. The range of traffic load is from 0.1 to 0.8.

Fig. 3 shows the proportion of affected DS services under different traffic loads. The six curves in the figure respectively represent the blocking probability and the ratio of affected DS services with three scheduling strategies. It can be seen that the blocking rate and the ratio of affected DS services increase with the growth of traffic load under the three strategies. When the traffic load is between 0.1 and 0.5, the blocking rate and the ratio of affected DS services in TS-ONU are the highest, followed by ATS strategy. When the traffic load is higher than 0.5, the ratio of affected DS services in TS-OLT increases rapidly. In particular, the ratio of affected DS services reaches 23.9% when traffic load is 0.8, which is 4.3% and 5.4% higher than TS-ONU and ATS strategy, respectively. However, the increase of blocking rate under TS-OLT is relatively flat, which means that QoS degradation rate of DS services increases rapidly in this traffic load range.

When the traffic load is between 0.1 and 0.5, the ratio of affected DS services in TS-ONU is the highest. The reason is that the DS services scheduled to other EC-ONUs does not meet the delay requirement, or the traffic scheduling affects other DS services that should be processed in the offloading target. The ratio of affected DS services in ATS and TS-OLT strategy is similar, which indicates that there are a lot of idle resources in EC-OLT. Meanwhile, ATS strategy also gives priority to scheduling most services to EC-OLT for processing. When traffic load is higher than 0.5,

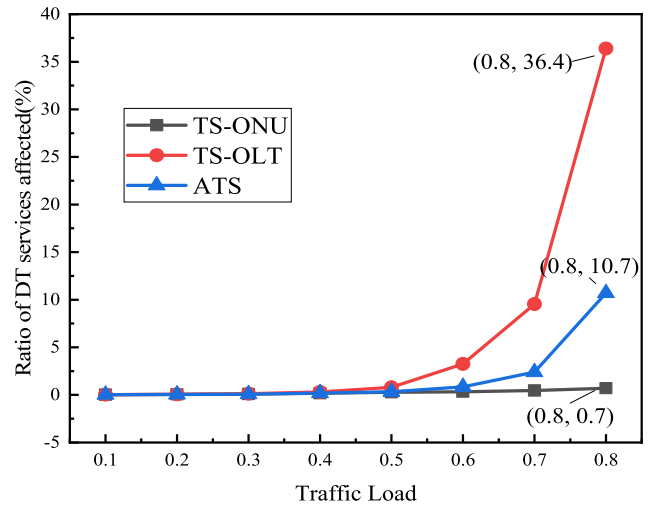


FIGURE 4. Ratio of DT services affected vs. traffic load.

the available resources in EC-OLT become insufficient, leading to the increase of QoS degradation for DS services in TS-OLT. In contrast, the QoS degradation of DS services in ATS does not change much since some services are scheduled to other EC-ONUs according to the network resources and delay requirements.

Fig. 4 shows the ratio of affected DT services. Since the blocking probability of DT services is very low, the blocking probability and QoS degradation of DT services are not separately shown. As traffic load increases, the ratio of the affected DT services also increases. When the traffic load is between 0.1 and 0.9, the number of the affected DT services under TS-ONU is basically unchanged. This is because almost all DS services are scheduled to other EC-ONUs, which will not affect the DT services that are processed in EC-OLT. When traffic load is less than 0.5, the DT services under TS-OLT are almost unaffected. It means that the idle resources in EC-OLT are sufficient to process DT services and the scheduled DS services at the same time. However, when traffic load is higher than 0.5, the number of the affected DT services begins to grow rapidly, which indicates that the resources in EC-OLT are becoming insufficient. Specifically, when the traffic load is 0.8, the number of affected DT services accounts for 36.4% in TS-OLT. Considering all the edge nodes, the services in ATS can be adaptively scheduled to EC-OLT or other EC-ONUs according to the resource usage. Therefore, the ratio of DT services affected in ATS is between TS-OLT and TS-ONU.

In Fig. 3, when the traffic load is 0.8, the affected DS services under ATS algorithm is 1.1% and 5.5% lower than that under TS-OLT and TS-ONU respectively. However, in Fig. 4, the ratio of affected DT services under ATS algorithm is higher than that of TS-ONU. Obviously, in order to reduce the ratio of affected DS service as much as possible, ATS inevitably sacrifices the QoS of some DT services. In general, DS services can bring more benefits for network operators than DT services.

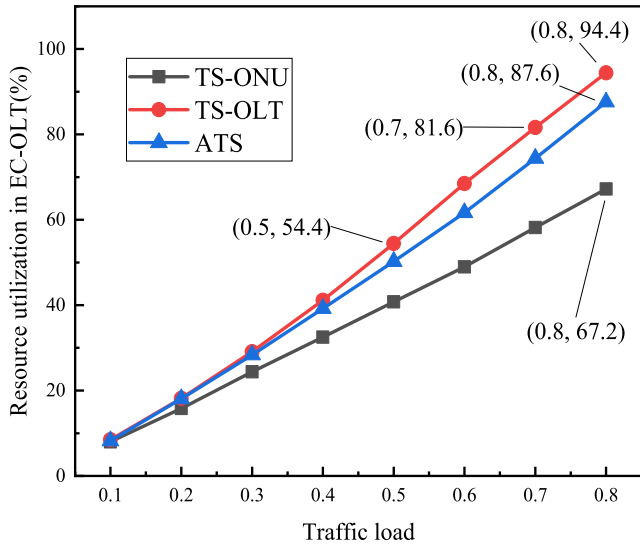


FIGURE 5. Resource utilization in EC-OLT vs. traffic load.

The resource utilization of EC-OLT and EC-ONU can further explain the above results when nodes are attacked by DDoS under different traffic load. As shown in Fig. 5 and Fig. 6, when the traffic load is 0.1, the resource utilization rates of three algorithms are basically the same, which indicates that traffic scheduling is not triggered at this time. With the increase of traffic load, the resource utilization ratio of nodes begins to show differences. Fig. 5 shows the change of resource utilization in EC-OLT as the traffic load increases. Under DDoS attacks, resource utilization in EC-OLT is about 10% when the traffic load is 0.1. With the increase of traffic load, TS-OLT and TS-ONU give a priority to scheduling services to EC-OLT and EC-ONU respectively. Therefore, TS-OLT has the highest resource utilization in EC-OLT and TS-ONU has the lowest. When the traffic load is 0.5 and 0.7, the resource utilization in EC-OLT has reached 54.4% and 81.6% respectively under TS-ONU. Thus, the idle resources are not enough to handle DS and DT services at the same time. This explains why the QoS degradation of DS services and the ratio of affected DT services in Fig. 3 and Fig. 4 increase significantly.

Similarly, the average resource utilization of EC-ONUs under different traffic loads is shown in Fig. 6. The performance comparison of three strategies in this figure is just opposite to that in Fig. 5. When the traffic load is 0.8, the average resource utilization of EC-ONUs under TS-ONU is the highest, but less than 50%. However, the blocking probability of DS services under TS-ONU in Fig. 3 has reached 3.9%. It can be obtained that the scheduling strategy of TS-ONU will seriously affect the DS services that should be processed in the offloading target.

## 2) DIFFERENT NUMBER OF ATTACKED NODES

The traffic load is fixed at 0.6 in this case and the number of attacked ONU nodes ranges from 2 to 12.

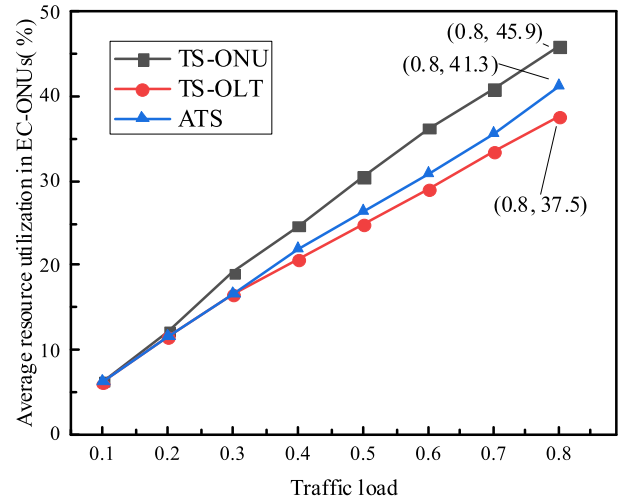


FIGURE 6. Average resource utilization in EC-ONUs vs. traffic load.

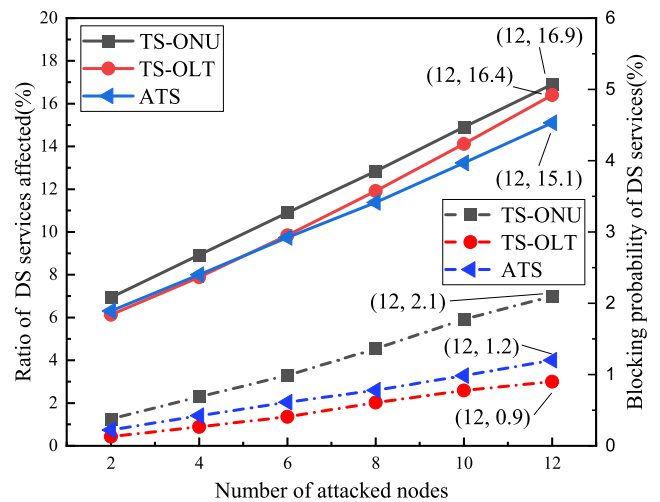


FIGURE 7. Ratio of DS services affected vs. number of attacked nodes.

Fig. 7 illustrates the proportion of affected DS services under different numbers of attacked nodes. Obviously, the higher number of attack nodes, the more DS services will be affected. When the number of attack nodes is less than 12, ATS achieves the best performance among the three strategies. Specifically, when the number of attack nodes is smaller than 6, the ratio of the affected DS services under TS-OLT and ATS is roughly the same. This means that when the number of attack nodes is small, ATS will schedule most of the services to EC-OLT for processing. When the number of attack nodes is higher than 6, the ratio of affected DS services under TS-OLT is higher than that under ATS. Specifically, with 12 nodes attacked by DDoS, the ratio of affected services in TS-OLT is very close to that in TS-ONU. This shows that an increasing number of DS services are scheduled to EC-OLT and the available resources in EC-OLT become insufficient, which leads to the QoS degradation of DS services. In addition, with 12 nodes attacked, the ratio of affected DS services in ATS is 1.3% lower than TS-OLT while the blocking rate



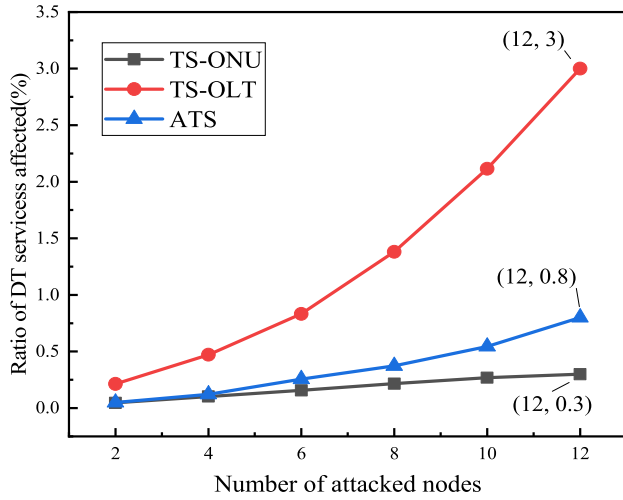


FIGURE 8. Ratio of DT services affected vs. number of attacked nodes.

is 0.3% higher than that in TS-OLT. Thus, the QoS degradation rate in ATS is 1.6% lower than that in TS-OLT. The reason is that ATS will adaptively schedule DS services to other EC-ONUs or EC-OLT according to network resource usage, leading to a lower ratio of affected DS services.

The proportion of affected DT services under different numbers of attacked nodes is shown in Fig. 8. Similarly, the blocking probability and QoS degradation rate are not separately depicted. The number of the affected DT services increases with the number of attack nodes and TS-OLT has the highest value. When the number of attacked nodes is more than 6, similar to Fig. 7, the ratio of the affected DT services increases significantly, which further indicates that the resources in EC-OLT are insufficient. When the number of attack nodes is 12, the proportion of affected DT services under TS-OLT reaches 3%. In contrast, the values of the other two strategies are less than 1%. Meanwhile, the ratio of affected DT services in ATS is 0.5% higher than that in TS-ONU. As discussed in Fig. 7, the ratio of affected DS services in ATS is 1.8% lower than that in TS-ONU. Therefore, the reduction of the affected DS services in ATS is at the expense of QoS degradation of some DT services.

Fig. 9 and Fig. 10 show the resource utilization in EC-OLT and EC-ONUs with different numbers of attacked nodes respectively. A higher number of attack nodes leads to the increase of resource utilization in both EC-OLT and EC-ONUs. When the number of attacked nodes is 2, the resource utilization of EC-OLT under three strategies are different, indicating that traffic scheduling has been triggered.

Similarly, TS-ONU schedules most of the services to other EC-ONUs first, which leads to the highest resource utilization in EC-OLT. When 6 nodes are attacked, the resource utilization in EC-OLT under TS-ONU reaches 60.9%. This explains the significant increase of the affected DS and DT services under TS-OLT. In addition, when the number of attack nodes is greater than 6, the resource utilization in EC-OLT under

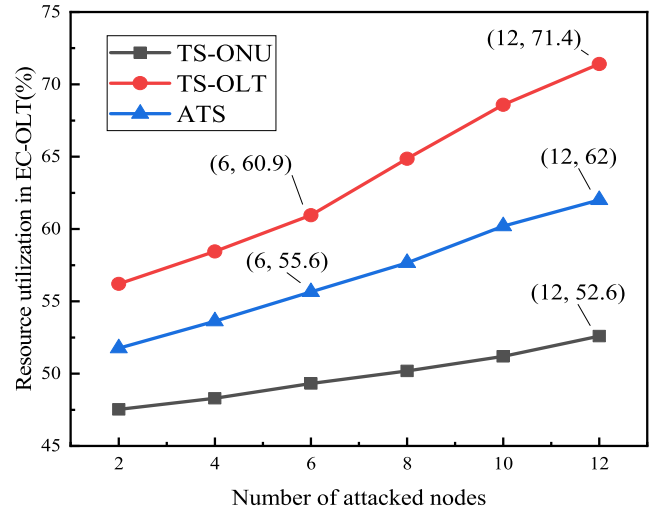


FIGURE 9. Resource utilization in EC-OLT vs. Number of attacked nodes.

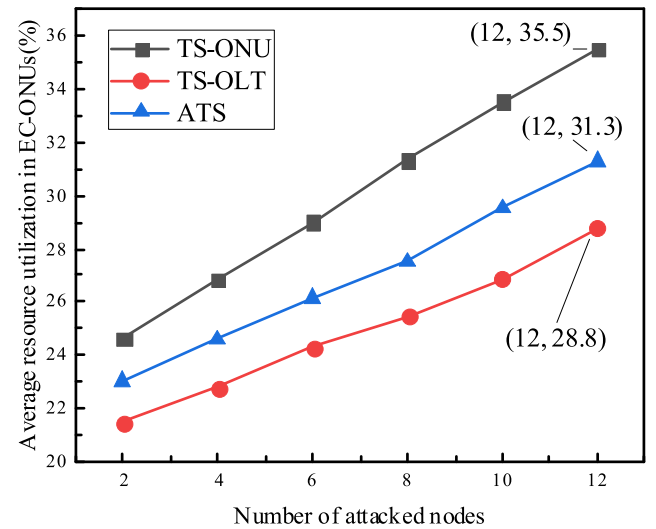


FIGURE 10. Average resource utilization in EC-ONUs vs. Number of attacked nodes.

ATS is higher than 55.6%, which leads to an increase of affected DT services under ATS in Fig. 8.

In Fig. 10, the average resource utilization of EC-ONUs under TS-ONU is the highest, which can explain the highest ratio of the affected DS services and blocking rate under TS-ONU in Fig. 7. In addition, we can see that the average resource utilization of EC-ONUs under ATS is 31.3%, when the number of attacked nodes is 12. We can see that with the same number of attacked nodes, the resource utilization in EC-ONUs under TS-ONUs is the highest while the value under TS-OLT is the lowest. The reason is that TS-OLT and TS-ONU prefer to schedule DS services to EC-OLT and EC-ONUs, respectively.

### B. DIRECT DDoS ATTACKS

In direct DDoS attacks, the performance of ATS algorithm is evaluated in two cases, i.e., the variation of attack duration and different number of attacked nodes.

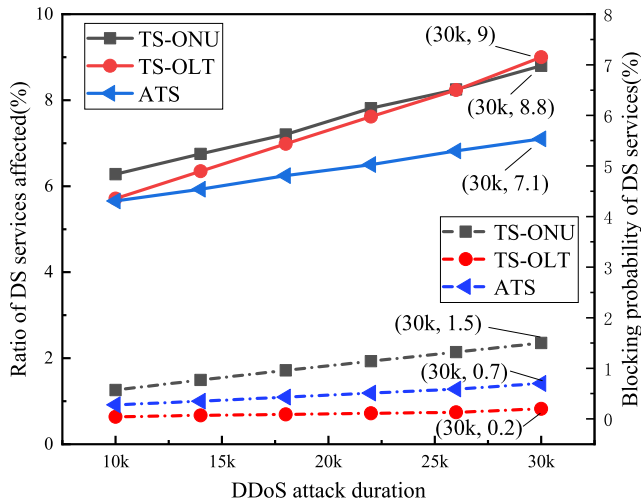


FIGURE 11. Ratio of DS services affected vs. DDoS attack duration.

1) VARIATION OF ATTACK DURATION

As mentioned in Section 5, the duration of DDoS attack is denoted as  $T_{x-y}$ , that is, from the arrival of the  $x^{th}$  service to the arrival of the  $y^{th}$  service. With 50k services in total, for simplicity, the sum of  $x$  and  $y$  is set to 50k. It means that the start and end time of a DDoS attack are symmetric about the arrival of 25k<sup>th</sup> service.

Fig. 11 and Fig. 12 show the ratio of the affected DS and DT services under different DDoS attack durations, respectively. At this time, the traffic load is 0.6 and the number of attack nodes is 8. Note that the attack duration  $T_{x-y}$  is simplified as the difference of  $y$  and  $x$  (i.e.,  $y-x$ ) in the horizontal axis of these two figures. For example, the duration  $T_{20k-30k}$  and  $T_{10k-40k}$  are denoted as 10k and 30k, respectively. Obviously, the longer the duration of DDoS, the more services will be affected.

Fig. 11 shows the ratio of the affected DS services under different DDoS attack durations. When the attack duration is 10k, the ratio of the affected DS services in TS-OLT and ATS is similar. Since EC-OLT has more resources than other EC-ONUs, ATS schedules most of DS services to EC-OLT. When the duration of DDoS attack is less than 25k, the strategy of TS-ONU will affect the DS services in other nodes that have not been attacked, resulting in the highest ratio of affected DS services. When the duration is longer than 25k, the ratio of affected DS services under TS-OLT is the highest. It means that the resources in EC-OLT are becoming scarce so that the QoS of DS services cannot be guaranteed. In addition, with different attack durations, the blocking rate of DS services under TS-OLT is the lowest. The reason is that both TS-ONU and ATS will schedule some services to other EC-ONUs, affecting the DS services that should be processed in offloading nodes. When DDoS attack duration is 30k, the ratio of affected DS services in ATS is improved by 1.7% and 2% compared to TS-ONU and TS-OLT respectively.

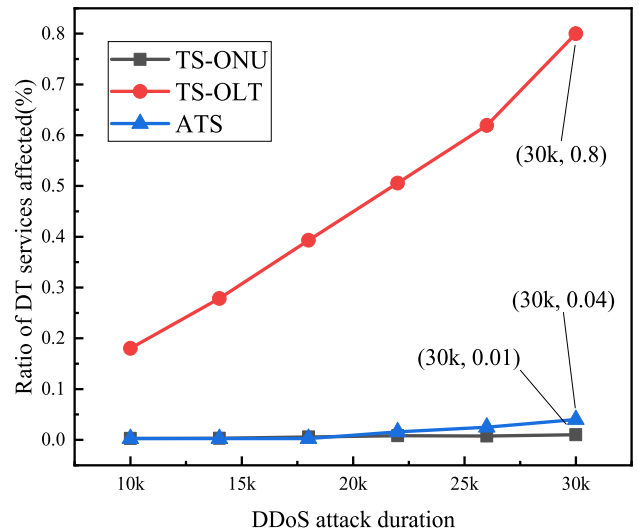


FIGURE 12. Ratio of DT services affected vs. DDoS attack duration.

The ratio of the affected DT services under different DDoS attack durations is shown in Fig.12. It can be seen that when the duration of DDoS attack is 10k, DS services under TS-OLT are scheduled to EC-OLT, which affects the QoS of DT services. As the growth of attack duration, the number of affected DT services also increases. When the duration is 30k, the ratio of affected DT services under three strategies is less than 1%, which indicates that the impact of traffic scheduling on DT services is not significant in different attack durations.

Fig. 13 and Fig. 14 show the real time resource utilization of EC-OLT and EC-ONUs through the simulation, respectively. With 0.6 traffic load, the duration of DDoS attack is set to  $T_{10k-40k}$  and the number of attack nodes is 8. Note that the results in Fig. 13 are the average values of real-time resource utilization for all the EC-ONUs. For simplicity, the resource utilization of each node is recorded every 500 services. Thus, with 50k services in total, each curve in Fig. 15 and 16 consists of 100 record points.

Fig. 13 reflects the real time average resource utilization of EC-ONUs through the simulation. We can see that without DDoS attacks, there is almost no difference about the resource utilization for three strategies. During the DDoS attack, the average resource utilization of EC-ONUs under the three strategies are different. Specifically, TS-OLT has the lowest resource utilization in EC-ONUs while TS-ONU achieves the highest. These results are consistent with the principles of three scheduling algorithms, since TS-ONU and TS-OLT prefer to schedule services to EC-ONUs and EC-OLT, respectively. In contrast, the proposed ATS algorithm can optimize the decisions of traffic scheduling based on the resource utilization in both EC-ONUs and EC-OLT. In addition, since direct DDoS attacks instantly change the resource configuration of EC-ONUs, the average resource utilization of EC-ONUs under three strategies will sharply change at the starting and ending of DDoS attacks.

Fig. 14 also shows the variation of real time resource utilization in EC-OLT under three strategies. The highest

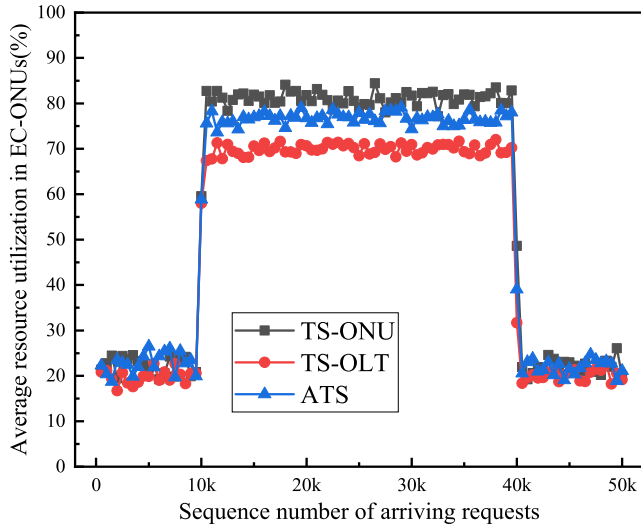


FIGURE 13. Average resource utilization in EC-ONUs vs. request services.

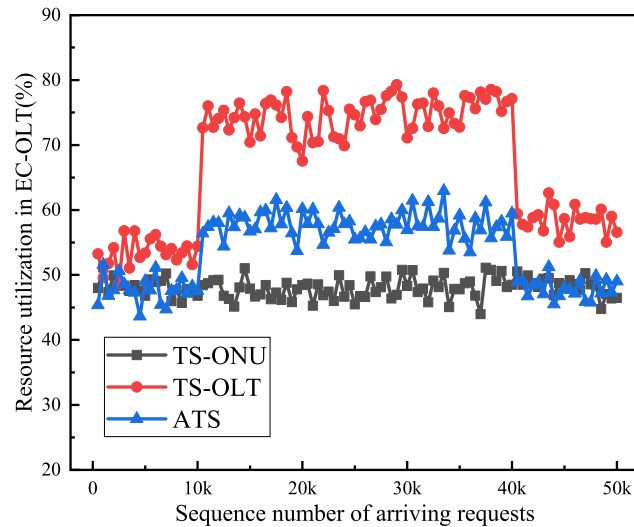


FIGURE 14. Resource utilization in EC-OLT vs. request services.

resource utilization is TS-OLT while the lowest resource utilization is TS-ONU. We can see that the resource utilization under TS-OLT and ATS has sharp changes at the starting and ending of DDoS attacks, depending on the number of DS services scheduled to the EC-OLT. The reason why the values of TS-ONU do not change sharply is that DS services are hardly scheduled to EC-OLT under this scheduling strategy.

2) DIFFERENT NUMBER OF ATTACKED NODES

We also record the ratio of affected DS services under different numbers of attacked nodes. DDoS attack duration is set to  $T_{10k-30k}$ . In Fig. 15, when the number of attacked nodes is less than 6, the ratio of the affected DS services under three strategies has little difference. When the number of attacked nodes is higher than 6, the number of affected DS services in TS-OLT increases rapidly. However, the blocking probability of DS services is always very low, which indicates

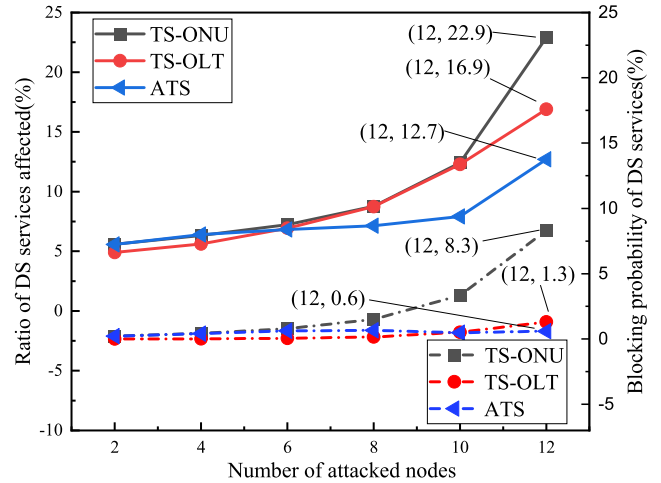


FIGURE 15. Ratio of DS services affected vs. number of attacked nodes.

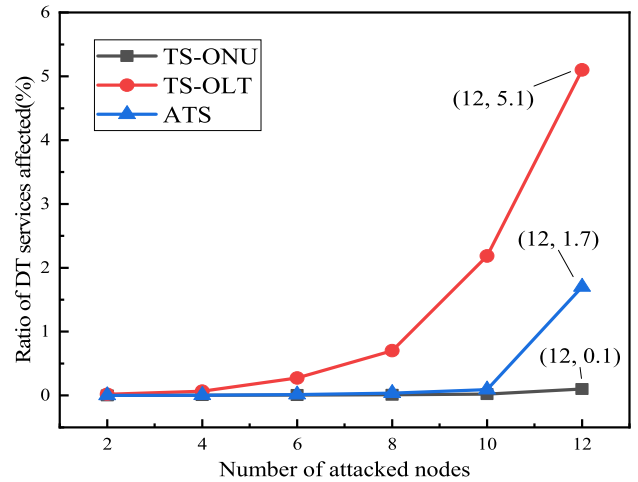


FIGURE 16. Ratio of DT services affected vs. number of attacked nodes.

that the QoS degradation of DS services increases under this strategy. In TS-ONU, when the number of attacked nodes is higher than 8, both blocking rate and the ratio of the affected DS services increase significantly. It means that scheduling services to other EC-ONUs will affect other DS services. In contrast, the proposed ATS can achieve the lowest ratio of affected DS services. For instance, when the number of attacked nodes is 12, the ratio of affected DS services is respectively reduced by 4.2% and 10.2%, compared with TS-OLT and TS-ONU.

Fig. 16 shows the ratio of the affected DT services under different number of attacked nodes. When two nodes are attacked, there is almost no difference in the number of the affected DT services under three strategies. When the number of attacked nodes is higher than 2, the TS-OLT scheme schedules the services to EC-OLT for being processed, which will affect some DT services. If the number of attacked nodes is not higher than 10, the ratio of the affected DT services under TS-ONU and ATS is close to 0. Based on the analysis in Fig. 15, when the number of attacked nodes is greater than 10,

the affected DS and DT services under ATS will increase at the same time. However, the blocking rate of DS services is extremely low, which means that ATS attempts to avoid the blocking of DS services as much as possible, at the cost of part DT services being affected by DDoS attacks.

## VII. CONCLUSION

This paper focuses on the problem of traffic scheduling to mitigate the DDoS attacks in EC-enabled TWDM-PON. The optimization target is to minimize the impact of DDoS attack on DS services. Based on the collaboration of EC-ONUs and EC-OLT, an ATS algorithm is designed to adaptively schedule traffic during DDoS attacks. With DS and DT services in dynamic traffic, the performance of ATS algorithm is evaluated through simulation. Specifically, direct and indirect DDoS attacks are considered and two benchmarks are adopted in simulation. Meanwhile, the performance of ATS algorithm is analyzed in different network scenarios, including different attack duration, traffic loads and different number of attacked nodes. Simulation results verify the effectiveness of the proposed ATS algorithm in terms of reducing the QoS degradation rate and blocking rate of DS services. The proposed algorithm can be combined with the existing mitigation solutions at higher network layer to further enhance the security. As our future work, we plan to further investigate the overhead caused by traffic schedule and PON framing in edge computing-enabled TWDM-PON. In addition, the implementation of control plane enabling traffic scheduling is also significant to be investigated.

## REFERENCES

- [1] B. P. Rimal, D. P. Van, and M. Maier, "Mobile-edge computing versus centralized cloud computing over a converged FiWi access network," *IEEE Trans. Netw. Service Manage.*, vol. 14, no. 3, pp. 498–513, Sep. 2017.
- [2] B. P. Rimal and M. Maier, "Workflow scheduling in multi-tenant cloud computing environments," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 1, pp. 290–304, Jan. 2017.
- [3] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.
- [4] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," *ETSI White Paper*, vol. 11, no. 11, pp. 1–16, Sep. 2015.
- [5] Y. Zhao, W. Wang, Y. Li, C. C. Meixner, M. Tornatore, and J. Zhang, "Edge computing and networking: A survey on infrastructures and applications," *IEEE Access*, vol. 7, pp. 101213–101230, 2019.
- [6] E. E. Haber, T. M. Nguyen, C. Assi, and W. Ajib, "Macro-cell assisted task offloading in MEC-based heterogeneous networks with wireless backhaul," *IEEE Trans. Netw. Service Manage.*, vol. 16, no. 4, pp. 1754–1767, Dec. 2019.
- [7] G. Kramer, M. De Andrade, R. Roy, and P. Chowdhury, "Evolution of optical access networks: Architectures and capacity upgrades," *Proc. IEEE*, vol. 100, no. 5, pp. 1188–1196, May 2012.
- [8] A. Helmy and A. Nayak, "Toward parallel edge computing in long-reach PONs," *J. Opt. Commun. Netw.*, vol. 10, no. 9, pp. 736–748, Sep. 2018.
- [9] C. Song, M. Zhang, L. Guan, L. Zhang, D. Wang, Y. Zhan, S. Cao, S. Wu, and J. He, "Load-aware dynamic traffic migration enabling low latency in hierarchical edge cloud-based 5G fronthaul," in *Proc. Opt. Fiber Commun. Conf. Exhib. (OFC)*, Mar. 2019, pp. 1–3.
- [10] H. Guo, J. Liu, and H. Qin, "Collaborative mobile edge computation offloading for IoT over fiber-wireless networks," *IEEE Netw.*, vol. 32, no. 1, pp. 66–71, Jan./Feb. 2018.

- [11] W. Wang, Y. Zhao, M. Tornatore, H. Li, J. Zhang, and B. Mukherjee, "Coordinating multi-access edge computing with mobile fronthaul for optimizing 5G end-to-end latency," in *Proc. Opt. Fiber Commun. Conf. Expo. (OFC)*, Mar. 2018, pp. 1–3.
- [12] H. Liu, F. Eldarrat, H. Alqahtani, A. Reznik, X. de Foy, and Y. Zhang, "Mobile edge cloud system: Architectures, challenges, and approaches," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2495–2508, Sep. 2018.
- [13] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019.
- [14] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Washington, DC, USA, Jun. 2019, pp. 82–90.
- [15] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level DDoS mitigation framework for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, Feb. 2018.
- [16] A. T. Al-Hammouri, Z. Al-Ali, and B. Al-Duwairi, "ReCAP: A distributed CAPTCHA service at the edge of the network to handle server overload," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 4, p. e3187, Apr. 2018.
- [17] N. Yang, X. Fan, D. Puthal, X. He, P. Nanda, and S. Guo, "A novel collaborative task offloading scheme for secure and sustainable mobile cloudlet networks," *IEEE Access*, vol. 6, pp. 44175–44189, 2018.
- [18] J. Zhao, Q. Li, Y. Gong, and K. Zhang, "Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7944–7956, Aug. 2019.
- [19] J. Zhang, W. Xia, F. Yan, and L. Shen, "Joint computation offloading and resource allocation optimization in heterogeneous networks with mobile edge computing," *IEEE Access*, vol. 6, pp. 19324–19337, 2018.
- [20] C. You, K. Huang, H. Chae, and B.-H. Kim, "Energy-efficient resource allocation for mobile-edge computation offloading," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1397–1411, Mar. 2017.
- [21] P. Zhao, H. Tian, C. Qin, and G. Nie, "Energy-saving offloading by jointly allocating radio and computational resources for mobile edge computing," *IEEE Access*, vol. 5, pp. 11255–11268, 2017.
- [22] Q. Liu, Z. Su, and Y. Hui, "Computation offloading scheme to improve QoE in vehicular networks with mobile edge computing," in *Proc. 10th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Hangzhou, China, Oct. 2018, pp. 1–5.
- [23] Y. Zhao, Y. Li, J. Li, M. Liu, Y. Niu, Y. Zhao, and J. Zhang, "Traffic scheduling strategy for mitigating DDoS attack in edge computing-enabled TWDM-PON," in *Proc. Opto-Electron. Commun. Conf. (OECC)*, Taipei, Taiwan, Oct. 2020, pp. 1–4.
- [24] R. Butt, S. Idrus, K. Qureshi, N. Zulkifli, and S. Mohammad, "Improved dynamic bandwidth allocation algorithm for XGPON," *J. Opt. Commun. Netw.*, vol. 9, no. 1, pp. 87–97, Jan. 2017.
- [25] X. Wang, Y. Ji, J. Zhang, L. Bai, and M. Zhang, "Joint optimization of latency and deployment cost over TDM-PON based MEC-enabled cloud radio access networks," *IEEE Access*, vol. 8, pp. 681–696, 2020.
- [26] X. Wang, Y. Ji, J. Zhang, L. Bai, and M. Zhang, "Low-latency oriented network planning for MEC-enabled WDM-PON based fiber-wireless access networks," *IEEE Access*, vol. 7, pp. 183383–183395, 2019.
- [27] S. Simpson, S. N. Shirazi, A. Marnerides, S. Jouet, D. Pazaros, and D. Hutchison, "An inter-domain collaboration scheme to remedy DDoS attacks in computer networks," *IEEE Trans. Netw. Service Manage.*, vol. 15, no. 3, pp. 879–893, Sep. 2018.
- [28] M. S. Elbamy, M. Bennis, and W. Saad, "Proactive edge computing in latency-constrained fog networks," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Oulu, Finland, Jun. 2017, pp. 1–6.



**YAJIE LI** received the Ph.D. degree in communication and information system from the Beijing University of Posts and Telecommunications (BUPT), in 2018. From October 2016 to December 2017, he was a Visiting Ph.D. Student at the KTH Royal Institute of Technology. He is currently working as an Associate Researcher with the BUPT. His research interests include edge computing, secure optical communications, and 5G optical transport networks.





**YINGQI ZHAO** received the B.S. degree from the Wuhan University of Technology (WUT), Wuhan, China, in 2018. She is currently pursuing the M.S. degree in information and communication engineering with the Beijing University of Posts and Telecommunications (BUPT). Her research interests include edge computing and optical access networks.



**JUN LI** received the Ph.D. degree from the KTH Royal Institute of Technology, Sweden, in 2019. From September 2018 to March 2019, he was also a Visiting Ph.D. Student at Princeton University. He was a Postdoctoral Researcher at the Chalmers University of Technology, Sweden. He is also a Lecturer with Soochow University. His research interests include fog/edge computing, optical access networks, and distributed machine learning.



**XIAOSONG YU** (Member, IEEE) received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), China, in 2015. From September 2013 to September 2014, he was a Visiting Scholar at the UC Davis. He is currently with the State Key Laboratory of Information Photonics and Optical Communications (IPOC), BUPT. His research interests include optical network security, elastic optical networks, and software defined optical networks.



**YONGLI ZHAO** (Senior Member, IEEE) received the B.S. degree in communication engineering and the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications (BUPT), in 2005 and 2010, respectively. He is currently a Professor with the Institute of Information Photonics and Optical Communications, BUPT. He has published over 150 journal articles and conference papers. His research interests include software-defined optical networks, flexi-grid optical networks, and network virtualization.



**JIE ZHANG** (Member, IEEE) received the bachelor's degree in communication engineering and the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications (BUPT), China. He is currently a Professor and the Dean of the School of Electronic Engineering, BUPT. He has published over 300 technical articles. He has authored eight books, submitted 17 ITU-T recommendation contributions, and six IETF drafts. He holds 17 patents. His research interests include architecture, protocols, and standards of optical transport networks. He has served as a TPC Member for a number of conferences, such as ACP, OECC, PS, ONDM, COIN, and ChinaCom.

...