

Analysis of DoS Attacks on Digital Twin-based AoI-aware Wireless Transmission Scheduling

Ahmed S. Khwaja^{*†}, Shuo Yu[‡], Waleed Ejaz[‡], Poornima S.[§], Isaac Woungang[†], Alagan Anpalagan^{*}

^{*}Department of Electrical, Computer and Biomedical Engineering, [†]Department of Computer Science,
Toronto Metropolitan University, Toronto, Canada

[‡]Department of Electrical and Computer Engineering, Lakehead University, Barrie, Canada

[§]Department of Electronics, Cochin University of Science and Technology, Kerala, India

Abstract—In this paper, we study and analyze the effects of a denial-of-service (DoS) attack by a malicious user equipment (UE) on the performance of digital twin (DT)-based age-of-information (AoI)-aware wireless uplink transmission scheduling. The malicious UE generates the packets at a high transmission rate, with the aim to disrupt the transmission of packets by a genuine UE. We first calculate an upper bound of the packet transmission loss rate (PTLR) versus varying the genuine and malicious packet generation rates. This loss rate is caused by new genuine packets overwriting the existing genuine packets that could not be transmitted in a timely manner due to the DoS attack. We also calculate upper and lower bounds of the AoI for the genuine UE in the presence of DoS attack. Subsequently, we carry out simulations to examine the scheduling performance for a genuine UE under varying genuine and malicious packet generation rates. We show that the DT-based scheduling receiving a timely information of the packet transmission request and receipt acknowledgment results in the lowest PTLR. This work provides an insight into the design of DT-based transmission scheduling systems in the presence of DoS attacks.

Index Terms—Digital twin, scheduling, denial-of-service (DoS), analysis, age-of-information (AoI)

I. INTRODUCTION

The integration of new and upcoming wireless technologies such as the fifth generation (5G) and sixth generation (6G) wireless networks with internet-of-things (IoT) devices will enable large-scale connectivity and smart applications deployment. In such setting, a digital twin (DT) is an important technology to study, analyze and plan the features offered by these networks [1]. Furthermore, service-specific DTs allow the provision of different services in cellular-supported IoT networks, such as load-balancing, user equipment (UE)-base station (BS) association, wireless transmission scheduling, to name a few [2]. However, the security of IoT devices is a concern [3] as many of these low-cost devices are not equipped sufficiently to guard against cyber attacks. Consequently, these devices can be used to introduce different types of cyber attacks in a network to disrupt its functionality.

According to [4], denial-of-service (DoS) and distributed DoS (DDoS) attacks are the most common and dangerous cyber attacks in IoT systems. In [5], DoS attacks are defined as attacks that compromise the data availability by obstructing the transmission in a network. The authors in [6] presented a design of an IoT network based on light-weight protocols and showed that a support vector machines-based classifier

trained on a DoS attack dataset outperformed other considered machine learning methods in detecting DoS attacks in this system. They also mentioned that such a detection system introduced additional delay in the network. The authors in [4] proposed the use of convolution neural networks to detect DoS and DDoS attacks, and they validated their solution using the Bot-IoT dataset [7] containing traffic from smart fridges, garage doors, weather stations, motion activated lights, and smart thermostats. In [8], the authors proposed a DDoS attack detection system for Industry 5.0 environment, making use of decision trees and DTs data to detect such an attack.

Besides, the scheduling of transmission in an IoT system is necessary to ensure a timely transmission of information from a source to a destination. In this regard, many 5G and future 6G applications require real-time updates that further increase the importance of scheduling. For instance, age-of-information (AoI) minimization is a useful tool to achieve scheduling with low computational complexity [2]. In addition, a DoS attack on an IoT system can affect the AoI and its scheduling performance by introducing delays, which can have serious consequences, for instance, in a ultra-reliable-low-latency communications system that needs to send timely updates [9]. Such attacks can also cause a packet loss prior to transmission, where new packets can overwrite the existing packets awaiting transmission in a queue.

The authors in [10] analyzed the impact of attacks on the AoI of a queuing system, considering attacks that could cause all updates in queues to be discarded. They stated that the average AoI increased in the presence of an attack where an incoming update overwrote the one being serviced. In [11], the authors considered a cyber-physical system where a DoS attack was considered as noise power injection. They showed that such an attack could increase the AoI, and considered DoS attack and defense as a game-theoretic model. Besides, they proposed a deep reinforcement learning-based solution to counter the attack, where a genuine sensor would increase its transmission power to make the transmission successful. The proposed solution was shown to attain an optimal Bayesian Nash equilibrium. In [12], the authors analyzed jamming-based DoS attacks on the status update of a remote sensing system from the perspective of game-theory. They used age-of-incorrect-information as a metric that is minimized and maximized by genuine and malicious transmitters, respectively, by

varying their transmission rates. The authors showed that a DoS attack would become less convenient as the transmission cost increased for the malicious entity.

Similar to [12], the authors in [9] considered jamming attacks on a status update wireless system. They calculated the analytical expressions of the average AoI under high- and low-power jamming, and showed that an increase in the jamming power could increase the average AoI. The authors in [5] showed that the status-updating systems operating on age-of-incorrect-information were less susceptible to jamming attacks. They further provided an optimal jamming policy that balanced the system's performance degradation and attacker's energy consumption.

On another note, the vulnerability of IoTs to cyber attacks makes DTs susceptible to different types of cyber attacks. In [13], it was stated that DTs could be a target of DoS attacks as they continuously exchange the data with the physical world, and a random forest-based approach to detect DoS attacks in IoT-enabled DTs was proposed. In [14], the authors proposed a review of security attacks and possible solutions in a DT-enabled wireless system. The authors identified the physical interaction layer in a DT-enabled wireless network as susceptible to DoS attacks, and they further stated that an attack could be detected and categorized in the DT space by analyzing the abnormal value of the throughput and AoI, followed by the anti-jamming action.

In this paper, we investigate and analyze the effects of DoS attacks on the performance of a DT-based uplink transmission scheduling system. Here, a DoS attack is considered as a generation of packets by malicious IoT UEs to obstruct the transmission of genuine packets. Given that DoS-attack detection mechanisms based on machine learning algorithms could introduce additional delays or require training datasets [4], [6], [8], [11], [13], we consider a low-complexity AoI-based-DT system for scheduling, and study the effects of varying the genuine and malicious packets generation rates on the performance of this system. We calculate an upper bound of the genuine packet transmission loss ratio (PTLR) as well as the best- and worst-case AoI bounds of genuine UEs with respect to varying genuine and malicious packet generation rates. Through simulations, we show how AoI-based scheduling and benchmark random scheduling would perform in the presence of DoS attack. To the best of our knowledge, this is the first time that PTLR and AoI bounds for genuine UEs in the presence of a DoS attack are provided, and the performance of DT-based AoI-leveraged packet transmission scheduling has been investigated. The insights gained from the work in this paper can be used to design DT-based transmission scheduling systems that are robust to DoS attacks.

The rest of this paper is organized as follows: Section II presents the system model. In Section III, the bounds of PTLR and AoI for genuine UEs in the presence of a DoS attack are analyzed and calculated. Section IV shows the simulation results of the benchmark and AoI-leveraged scheduling techniques under a DoS attack. Section V concludes this paper.

II. SYSTEM MODEL

A cellular wireless network is considered, which consists of IoT UEs, a main base station (MBS) that can cater to a large number of UEs, and a number of small base stations (SBSs) that can allow up to $U_{max} \approx 30$ UEs to connect to each one of them. We consider an uplink communication scenario. The MBS hosts a DT server that provides separate association and low-complexity scheduling service DTs, which associate each UE to either the MBS or one of the SBSs, and once it is complete, the packet transmission is scheduled from each UE to its associated BS in a real-time manner.

Each SBS is connected to the MBS via a fiber-optic link for timely relaying of information relating to the transmission requests from the UEs and the acknowledgment of packets received at the SBS. As our goal in this paper is to study the impact of a DoS attack on the UE-base station (BS) packet transmission scheduling, we consider all UEs to have already been associated with one of the BSs. Subsequently, we consider the effect of DoS attack on the UE transmissions to the associated BS. In this paper, we consider the transmission and scheduling between the UEs and an SBS; however, this analysis and its results are equally applicable to the transmission between the UEs and an MBS.

Consider the s^{th} SBS, to which a total number of U_s UEs have been associated. A time-division multiple access system operates on a time-slot of duration Δt , where only one UE can transmit per time-slot. Each UE connected to the SBS generates the packets at a rate of $\lambda_{u_s \in \mathbf{u}_s}^s$ packets/second, where $\mathbf{u}_s = \{1, 2, \dots, U_s\}$. The UE has a single buffer to store a newly generated packet, and the UE sends its transmission request to the SBS via a dedicated orthogonal wireless channel. This request is also conveyed to the DT server located at the MBS via the fiber-optic link. The scheduling service DT located at the DT server decides which UE should transmit according to a pre-defined scheduling policy based on the AoI. The scheduling decision is sent to the SBS via the fiber-optic link, which then selects the corresponding UE for transmission.

Once a packet from the selected UE is transmitted, its buffer becomes empty. A high channel signal-to-noise ratio is considered in this study, so that once a packet is transmitted, it is received successfully at the SBS. If a new packet is generated by a UE before the previous one in the buffer has been transmitted, it overwrites the existing packet in the buffer. This phenomenon is measured by means of the overall PTLR for the s^{th} SBS, denoted by $PTLR_s$. It is defined as the ratio of the total number of genuine packets overwritten in all UEs associated to the s^{th} SBS to the total number of genuine packets generated by all these UEs.

Each transmitted packet is considered to reach its associated SBS within the duration of Δt . Once a packet is received at the SBS, an acknowledgment of receipt is transmitted and received instantly by a dedicated orthogonal control channel at the transmitting UE, and the scheduling service DT is informed as well via the fiber-optic link. Each generated packet has the timestamp of its generation, which is also conveyed to the DT

server to update the AoI, denoted by $AoI_{u_s}^s$ for the u_s^{th} UE associated to the s^{th} SBS. The DT server maintains a record of AoI of each UE, which is used by the service DT to schedule the UEs for packet transmission. If no packet from a UE is received at the SBS in a time-slot, the AoI corresponding to the UE is increased by Δt ; otherwise, it is equal to the sum of the time spent by the packet in the UE's buffer prior to transmission and the time taken by the packet to reach the SBS after transmission.

Among U_s UEs connected to the s^{th} SBS, there can be U_m malicious UEs. The packet generation rates of the malicious nodes are denoted by $\lambda_{u_m \in \mathbf{u}_m}^s$, where $\mathbf{u}_m = \{1, 2, \dots, U_m\}$. The SBS does not have any prior identification information about malicious and genuine UEs. A malicious UE generates the packets at a high rate, attempting to induce the scheduling service DT to schedule the genuine UEs for transmission less frequently. This, in turn, will reduce the timeliness of the transmission and increase the $PTLR_s$. Consequently, the AoI of a genuine UE, denoted by $AoI_{u_g \in \mathbf{u}_g}^s$, where $\mathbf{u}_g = \mathbf{u}_s \setminus \mathbf{u}_m$, may increase as a malicious UE may be prioritized for transmission. We study the effects of malicious traffic generated by the malicious UEs on the scheduling of genuine uplink traffic generated by genuine UEs to their associated SBS. For this purpose, we analyze the effect of malicious packet generation on the $PTLR_s$ and $AoI_{u_g}^s$ in Section III.

III. ANALYSIS OF A DOS ATTACK

We consider a single SBS denoted by s^1 . All the UEs associated to it generate the packets at varying rates $\lambda_{u_s \in \mathbf{u}_s}$, which are then stored in their buffers, awaiting for transmission. As long as the sum of the packet generation rates of all the UEs assigned to the SBS is less than $\frac{1}{\Delta t}$, the $PTLR_s$ will be minimum, and it will increase as this sum starts to exceed $\frac{1}{\Delta t}$. This can be expressed by the following expression:

$$PTLR_s \rightarrow \begin{cases} \approx 0, & \text{if } \sum_{u_s=1}^{U_s} \lambda_{u_s}^s < \frac{1}{\Delta t} \\ > 0, & \text{otherwise,} \end{cases} \quad (1)$$

Once a malicious UE is associated with the s^{th} SBS, it will generate the packets at a high rate, attempting to surpass the limit in (1) to increase the $PTLR_s$ and/or $AoI_{u_g}^s$. As the fiber-optic connection between the SBS and DT server protects it against wireless cyber attacks, a DoS attack can be carried out on the scheduling service DT indirectly by frequently generating the packets and sending numerous transmission requests to the SBS.

Next, we study the effects of increasing the malicious packet generation rate on the $PTLR_s$ and provide a conservative upper bound for it. We first consider the scenario where the sum of genuine packet transmission rate is slightly less than $\frac{1}{\Delta t}$, i.e., $\sum_{u_g \in \mathbf{u}_g} \lambda_{u_g}^s < \frac{1}{\Delta t}$. Without the loss of generality and to facilitate the analysis, we represent all genuine UEs transmitting at varying rates $\lambda_{u_g}^s$, $u_g \in \mathbf{u}_g$ by a single equivalent UE that has a packet generation rate of $\lambda_g^s =$

$\sum_{u_g \in \mathbf{u}_g} \lambda_{u_g}^s$. Similarly, all malicious UEs are represented by an equivalent single malicious UE, which tries to disrupt the genuine packet transmission by generating the packets at a high packet generation rate of $\lambda_m^s = \sum_{u_m \in \mathbf{u}_m} \lambda_{u_m}^s$. We first consider the malicious packet generation rate to be also equal to $\frac{1}{\Delta t}$. To calculate an upper-bound of $PTLR_s$, we consider a totally random scheduling (TRS) strategy as a benchmark, where the scheduling service DT selects each associated UE for transmission with an equal probability, irrespective of whether it has a packet to transmit or not. This strategy is selected as a benchmark because it assumes that a DT has no information regarding the transmission behavior of UEs.

As the packet transmission rates are approximately equal to $\frac{1}{\Delta t}$, both the malicious and genuine packets will be generated with a probability of 1 at each time-slot, i.e., the UEs will be generating a packet in each time-slot. As there is an equal chance of selecting either of the UE, the probability of selection of each UE is $\frac{1}{2}$. Thus, at every alternate time-slot, a packet will be missed from the genuine UE and overwritten by a new packet, i.e., half of the genuine packets will be overwritten by a new packet, resulting in $PTLR_s$ of $\frac{1}{2}$.

Now, consider an equivalent sum of genuine packet arrival rate equal to $\frac{1}{2\Delta t}$, while the malicious packet generation rate is still $\frac{1}{\Delta t}$. In this case, the probability of generating a genuine packet in each time-slot is equal to $\frac{1}{2}$, while the probability of generating a malicious packet is still equal to 1. Thus, a genuine packet generated has the current time-slot and the next time-slot over which it can be selected for transmission, and the chance that a packet in the buffer of a genuine UE will be transmitted is equal to $\frac{2}{3}$. As the probability of a buffer of the genuine UE being full is $\frac{1}{2}$, $PTLR_s$ is equal to $\frac{1}{2} \times \frac{2}{3} = \frac{1}{3}$. Similarly, if the sum of genuine packet transmission rates is equal to $\frac{1}{3\Delta t}$, $PTLR_s$ is equal to $\frac{1}{3} \times \frac{3}{4} = \frac{1}{4}$. Based on the aforementioned discussion, $PTLR_s$ is equal to $\frac{1}{n+1}$ for a genuine packet generation rate of $\frac{1}{n\Delta t}$, i.e.,

$$PTLR_s \left(\lambda_g^s = \frac{1}{n\Delta t} \right) = \frac{1}{n+1} \quad (2)$$

where $n \geq 1$ is used to represent λ_g^s as a fraction $\frac{1}{n}$ of the maximum packet generation rate of $\frac{1}{\Delta t}$.

Fig. 1a shows the $PTLR_s$ calculated based on the aforementioned explanation, where on the x-axis, the genuine packet generation rate λ_g^s is varied as a proportion of $\frac{1}{\Delta t}$. It can be observed that the $PTLR_s$ increases as λ_g^s increases, and this rate of increase decreases slightly once λ_g^s surpasses $\frac{0.5}{\Delta t}$. Note that as this is a conservative $PTLR_s$ estimate calculated based on the TRS, it is unaffected even if the malicious packet generation rate changes. Consider the case where the malicious packet generation rate λ_m^s decreases to $\frac{1}{2\Delta t}$. In this case, when the genuine packet generation rate varies as $\frac{1}{2\Delta t}$, $\frac{1}{3\Delta t}$ or $\frac{1}{4\Delta t}$, $PTLR_s$ will be $\frac{1}{2}$, $\frac{2}{3}$ or $\frac{1}{4}$, respectively, as each slot is selected with an equal probability and no other information is considered for selecting a UE.

Next, we consider the effect of a DoS attack on AoI_g^s . For that, we first consider a best-case AoI bound, where a packet is transmitted as soon as it is generated. Given that the genuine

¹Note that the results of this study can be generalized to other SBSs as well as the MBS.

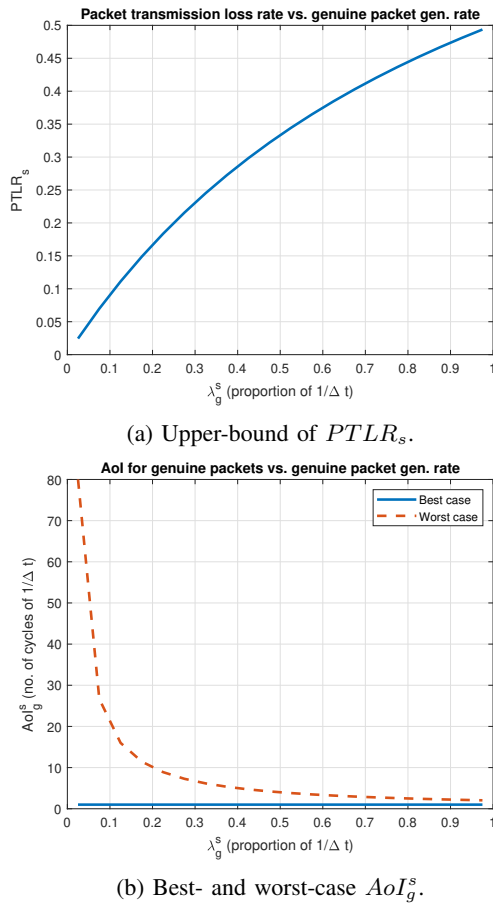


Fig. 1: Calculated bounds versus varying genuine packet generation rates.

packet generation rate is λ_g^s , and it takes a duration of Δt for a packet to arrive at its destination, this best-case AoI bound, denoted by $\underline{AoI}_g^s$ is obtained as

$$\underline{AoI}_g^s \approx \Delta t \quad (3)$$

To calculate the worst-case bound for AoI_g^s , we consider that the packet transmission from the genuine UE is delayed due to a malicious packet transmission. This packet in the buffer of the genuine UE is transmitted just before a new genuine packet is generated, and the new packet is generated as late as possible, i.e., if the first genuine packet is generated at 0 s, the second genuine packet would be generated just before $\frac{2}{\lambda_g^s}$ s. This scenario would occur if the gap between the generation time of the new packet and the most recent packet in the buffer is equal to $\frac{2}{\lambda_g^s} - \Delta t$. In this case, when the packet arrives at the destination, the worst-case AoI bound, denoted by $\overline{AoI}_g^s$ becomes

$$\overline{AoI}_g^s \approx \frac{2}{\lambda_g^s} \quad (4)$$

Fig. 1b shows the calculated best- and worst-case AoI_g^s bounds as a function of varying λ_g^s . It can be observed that $\overline{AoI}_g^s$ decreases rapidly as λ_g^s increases, and the difference between

$\underline{AoI}_g^s$ and $\overline{AoI}_g^s$ estimates decreases with the increasing genuine packet generation rate.

In the next section, we compare the performance of the following three scheduling strategies via simulations: 1) Benchmark TRS. 2) Partially informed scheduling (PIS), where the scheduling service DT does not have the information of UE transmission requests, and only receives a real-time acknowledgment once a transmitted packet reaches the SBS. It select a UE with the highest AoI for transmission, irrespective of whether it has a packet to transmit or not. 3) Fully informed scheduling (FIS), where the scheduling service DT receives real-time transmission requests from the UEs, as well as the acknowledgment of the packet receipt at the SBS. Among all UEs requesting transmission of their packets, it selects the one with the highest AoI. These three scheduling strategies involve usage of an increasing amount of information by the scheduling service DT, where the TRS has neither any information regarding the transmission requests nor the acknowledgment of packet reception, and the FIS has the complete information. This performance comparison would help evaluate the DT-based scheduling design in the presence of DoS attacks.

IV. RESULTS

In this section, we carry out simulations to obtain the $PTLR_s$ values versus varying λ_g^s and λ_m^s , and compare them to the bounds calculated in the previous section. We consider $\Delta t=1\text{ms}$ and the simulation is run over 360,000 cycles, equal to six minutes. We also determine the average AoI values of the genuine and malicious UEs in the presence of DoS attack, denoted by $\widehat{AoI}_g^s$ and $\widehat{AoI}_m^s$, respectively. We consider a genuine UE whose packet generation rates vary as $\lambda_g^s = 999, 450$ and 333 packets/s, respectively. We also consider a malicious UE, whose packet generation rates vary as $\lambda_m^s = 1000, 500$ and 333 packets/s, respectively. Note that if different packet generation rates are defined as $\frac{1}{n\Delta t}$, the aforementioned λ_m^s values correspond to $n = 1, 2$ and 3 , respectively. We first consider simulation results for the benchmark TRS, where each of the malicious and genuine UEs is selected randomly with a probability of 0.5, without considering any other information. For reference, we also provide the results for the case where the malicious UE does not transmit any packets.

The corresponding $PTLR_s$ results calculated from simulations are shown in Fig. 2a, for different combinations of λ_g^s and λ_m^s . It can be observed that in the absence of malicious packet generation, $PTLR_s$ is equal to 0.5. This is the best possible value of $PTLR_s$ under TRS. Next, we fix $\lambda_m^s=1000$ packets/s and vary λ_g^s as 999, 450 and 333 packet/s. It can be observed that the corresponding $PTLR_s$ is again 0.5 at $\lambda_g^s = 999$ packets/s and it decreases for $\lambda_g^s=450$ and 333 packets/s. This decrease is consistent with (1) and the calculations obtained using (2). The aforementioned results are repeated when λ_m^s is changed to 500 and 333 packet/s. It can be observed that $PTLR_s$ follows the same behavior with decreasing λ_m^s for all values for λ_g^s , as in this case, it is independent of the malicious packet generation rate as explained in the previous section.

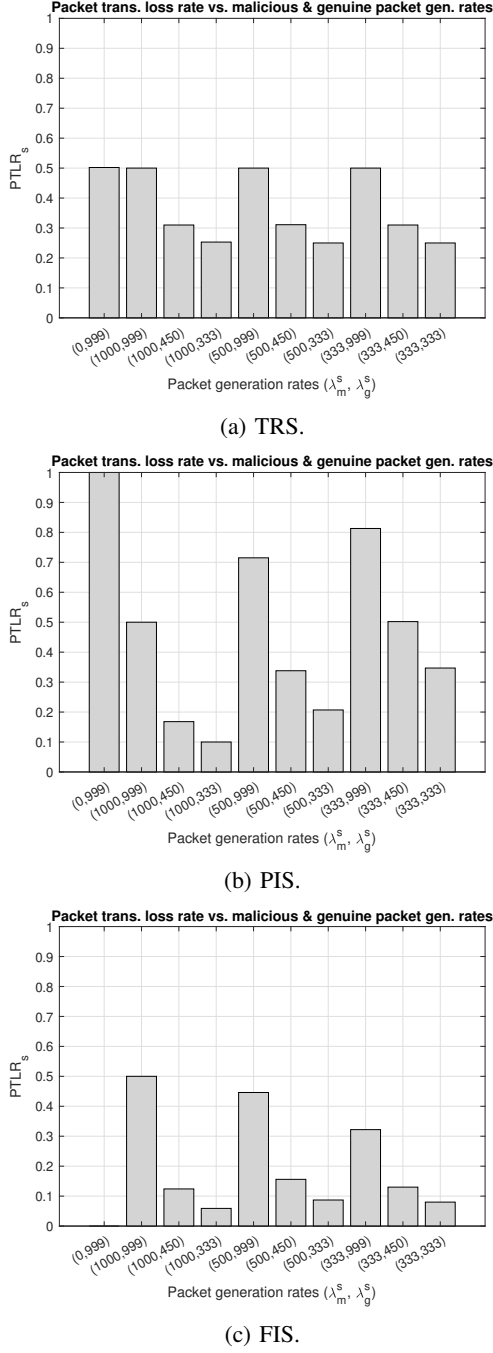


Fig. 2: Packet transmission loss rate versus different combinations of malicious and genuine packet generation rates.

These results confirm the correctness of the $PTLR_s$ behavior expressed in (1) and (2).

We also show the results with other types of scheduling strategies in increasing order of information usage. Fig. 2b shows the results with PIS, which always chooses the UE with the highest AoI, irrespective of whether it has the packet to transmit or not. Note that in this case, when $\lambda_m^s=0$, the scheduling would fail as due to a lack of arrival of any packet

from the malicious UE, it would have the highest AoI and hence would always be selected. This signifies that if PIS is used, a malicious UE could induce a $PTLR_s$ increase by reducing λ_m^s . We note that for a fixed λ_m^s and decreasing λ_g^s , $PTLR_s$ decreases. This is because if $\lambda_g^s < \lambda_m^s$, the AoI of the genuine UE would increase, causing the scheduler to select it more frequently for packet transmission. Furthermore, as λ_m^s decreases, the corresponding $PTLR_s$ increases compared to a higher λ_m^s with the same λ_g^s value. This is because due to the lower packet generation rates, the malicious UE would maintain a higher AoI, causing it to be selected for transmission more frequently. The $PTLR_s$ with PIS at $\lambda_m^s=1000$ packets/s is equal to or less than the corresponding $PTLR_s$ with TRS. As λ_m^s decreases, the $PTLR_s$ increases and is almost the same or surpasses those of the TRS for all λ_g^s values. This shows that the lack of availability of transmission request information causes the scheduling to perform equal to or worse than random scheduling without information.

Next, in Fig. 2c, we show the $PTLR_s$ values obtained using the FIS strategy, where a scheduler considers only the UE that has a packet to transmit, and selects the one with the highest AoI. In the absence of any malicious packet generation, $PTLR_s=0$, i.e., all the generated genuine packets are transmitted. It can be observed that for a fixed λ_m^s , $PTLR_s$ decreases as λ_g^s decreases. This is because as λ_g^s decreases, the corresponding AoI increases, causing more frequent selection of genuine UE for packet transmission. A noticeable decrease in $PTLR_s$ compared to TRS and PIS can be noticed for $\lambda_g^s = 450$ and 333 packets/s with $\lambda_m^s = 1000$ packets/s, as well as for all λ_g^s values with $\lambda_m^s = 500$ and 333 packets/s. However, for $\lambda_g^s = 999$ packets/s with $\lambda_m^s=1000$ packets/s, the $PTLR_s$ values are the same for all scheduling strategies. Thus, it is challenging to deal with a DoS attack where λ_g^s and λ_m^s are both approximately equal to $\frac{1}{\Delta t}$.

For $\lambda_m^s=500$ packets/s and $\lambda_g^s=450$ and 333 packets/s, the $PTLR_s$ values for FIS slightly increase compared to those with $\lambda_m^s=1000$ packets/s, and then decrease again when $\lambda_m^s=333$ packets/s. Unlike the PIS, this is a smaller increase and may be caused by the increase in AoI of the malicious UE due to its lower packet generation rate. It shows that unlike the PIS, the FIS is robust against DoS attacks with a reduced malicious packet generation rate. This is because the timely knowledge of the UE transmission requests ensures that genuine packets are transmitted frequently. For reference, the results of the average AoI values calculated over the complete simulation run are shown in Table I, including $\widehat{AoI}_g^s$ and $\widehat{AoI}_{gr}^s$. It can be observed that for all scheduling strategies, $\widehat{AoI}_g^s$ increases for a fixed λ_m^s and decreasing λ_g^s . The values of $\widehat{AoI}_g^s$ are between the upper and lower bounds of AoI_g^s calculated in (3) and (4) and shown in Fig. 1b, and this trend is independent of the value of $\widehat{AoI}_m^s$.

For TRS, $\widehat{AoI}_g^s$ is generally equal to or higher than that for FIS, except for $\lambda_m^s = 1000$ packets/s and $\lambda_g^s = 333$ packets/s, where it is slightly lower. On the other hand, $\widehat{AoI}_g^s$ for TRS is slightly lower than that for PIS, except for $\lambda_m^s=1000$ packets/s

TABLE I: Average AoI (no. of cycles of $1/\Delta t$) for TRS, PIS and FIS versus different malicious and genuine packet generation rates. “-” means that no transmission takes place, resulting in maximum average AoI value.

Scheduling	λ_m^s, λ_g^s	0,999	1000,999	1000,450	1000,333	500,999	500,450	500,333	333,999	333,450	333,333
TRS	$\widehat{AoI}_g^s$	2.008	2.003	3.645	4.791	2.001	3.635	4.743	2.003	3.640	4.752
	$\widehat{AoI}_m^s$	-	2.003	2.003	2.000	3.332	3.319	3.332	4.761	4.760	4.785
PIS	$\widehat{AoI}_g^s$	-	1.501	3.399	4.906	2.862	3.719	4.929	4.434	4.689	5.457
	$\widehat{AoI}_m^s$	-	1.499	2.180	2.902	2.932	3.259	3.846	4.898	4.928	5.161
FIS	$\widehat{AoI}_g^s$	1.002	1.501	3.307	4.854	1.557	3.288	4.742	1.395	3.285	4.736
	$\widehat{AoI}_m^s$	-	1.499	1.447	1.359	2.878	2.900	2.910	4.882	4.821	4.790

and $\lambda_g^s = 999$ and 450 packets/s. Thus, compared to TRS and PIS, FIS can achieve timely generation of genuine packets in the presence of a DoS attack. For TRS and FIS, $\widehat{AoI}_m^s$ remains almost the same irrespective of λ_g^s , and increases as λ_m^s decreases. For PIS, it increases as λ_m^s and λ_g^s decrease. Comparing this AoI behavior with that shown in Fig. 2 for $PTLR_s$, it can be concluded that with a lower λ_m^s , the performance of the PIS is the most affected. This is because of incomplete information availability, causing the PIS to often select the malicious UE even if it does not have a packet to transmit because the $\widehat{AoI}_m^s$ will be lower due to a lower λ_m^s .

For all scheduling methods, $\widehat{AoI}_m^s \leq \widehat{AoI}_g^s$, except for the combinations of $\lambda_m^s = 500$ packets/s with $\lambda_g^s = 999$ packets/s, and $\lambda_m^s = 333$ packets/s with all values of λ_g^s due to the lower malicious packet generation rate.² A higher λ_m^s and a lower λ_g^s means a lower $\widehat{AoI}_m^s$ due to frequent packet generation, which makes the FIS especially more robust against DoS attacks since it selects the UEs that have a higher AoI. However, as Fig. 2c shows, FIS also deals with lower malicious packet generation rates better than other scheduling methods as it achieves a lower $PTLR_s$.

V. CONCLUSIONS

In this paper, we studied and analyzed the effects of a DoS attack by a malicious UE on the performance of a DT-based uplink transmission scheduling in an IoT system. We first calculated an upper bound of the PTLR in the presence of DoS attack. These calculations correspond to a benchmark TRS strategy, where scheduling is carried out randomly without using any information about the transmission request and the acknowledgment of the packet receipt. We also calculated the best- and worst-case bounds of the AoI for a genuine UE. Simulation results confirmed the correctness of these calculations. We also compared the performance of PIS and FIS strategies, which used partial and full information regarding the packet transmission requests and arrivals, respectively. We showed that the FIS outperformed both the TRS and PIS, whereas the PIS mostly performed worse than the TRS. These results led to the conclusion that the use of partial information was counter-productive compared to the TRS, and a fully-informed DT was more suitable for transmission scheduling in the presence of DoS attack. This study could be extended to the design of service DTs that are robust against DoS attacks.

²The only exception to this trend is the PIS for both λ_m^s and $\lambda_g^s = 333$ packets/s.

Future work would involve considering the effects of low channel signal-to-noise ratios on the AoI and PTLR in the presence of DoS attacks. Furthermore, the analysis presented in Section III could be extended by considering individual multiple malicious and genuine UEs.

REFERENCES

- [1] M. Sanz Rodrigo, D. Rivera, J. I. Moreno, M. Álvarez Campana, and D. R. López, “Digital twins for 5g networks: A modeling and deployment methodology,” *IEEE Access*, vol. 11, pp. 38 112–38 126, 2023.
- [2] A. Shaharyar Khwaja, N. Tri Vo, W.-P. Nwadiugwu, I. Woungang, and A. Anpalagan, “Digital twin-assisted load-balanced user association and aoi-aware scheduling in iot networks,” *IEEE Access*, vol. 13, pp. 95 888–95 910, 2025.
- [3] P. Sitaraman, “Enhancing dos attack recovery in mqtt brokers for iot systems through efficient scheduling algorithms,” in *IEEE MIT Undergraduate Research Technology Conference (URTC)*, 2023, pp. 1–4.
- [4] I. Jemal, O. Cheikhrouhou, and M. A. Haddar, “Iot dos and ddos attacks detection using an effective convolutional neural network,” in *International Conference on Cyberworlds (CW)*, 2023, pp. 373–379.
- [5] S. Kriouile, M. Assaad, D. Gündüz, and T. Soleymani, “Optimal denial-of-service attacks against status updating,” in *IEEE International Symposium on Information Theory (ISIT)*, 2024, pp. 1373–1378.
- [6] R. N. Bhai and M. S. Patil, “Machine learning based detection of dos attacks in integrated mqtt-coap heterogeneous iot network,” in *5th International Conference for Emerging Technology (INCET)*, 2024, pp. 1–5.
- [7] N. Moustafa, “The bot-iot dataset,” 2019. [Online]. Available: <https://dx.doi.org/10.21227/r7v2-x988>
- [8] A. Gaurav, B. B. Gupta, K. Tai Chui, V. Arya, and E. Benkhelifa, “A ddos attack detection system for industry 5.0 using digital twins and machine learning,” in *IEEE 12th Global Conference on Consumer Electronics (GCCE)*, 2023, pp. 1019–1022.
- [9] H. Xu, Y. Yang, J. Pan, and Y. Xu, “On the information freshness under random jamming attacks,” *IEEE Wireless Communications Letters*, vol. 14, no. 10, pp. 3373–3377, 2025.
- [10] J. Doncel and M. Assaad, “Optimizing age of information with attacks,” in *Network Games, Artificial Intelligence, Control and Optimization*, H. Le Cadre, Y. Hayel, B. Tuffin, and T. Chahed, Eds. Cham: Springer Nature Switzerland, 2025, pp. 3–13.
- [11] Z. Hang, X. Wang, F. Li, Y.-a. Ren, and H. Li, “Learning-based dos attack game strategy over multi-process systems,” *Mathematical Modelling and Control*, vol. 4, pp. 424–438, 01 2024.
- [12] V. Bonagura, L. Badia, F. Pascucci, and S. Panzieri, “A denial of service game for age of incorrect information in cyber-physical systems,” in *IEEE 20th International Conference on Automation Science and Engineering (CASE)*, 2024, pp. 1270–1275.
- [13] N. Alhamam, M. M. H. Rahman, and A. Aljughaiman, “Twinguard: A supervised machine learning framework for dos attack detection in iot-enabled digital twins using random forest and feature selection optimization,” *IEEE Access*, vol. 13, pp. 190 872–190 889, 2025.
- [14] W. Wang, Y. Yang, L. U. Khan, D. Niyato, Z. Han, and M. Guizani, “Digital twin for wireless networks: Security attacks and solutions,” *IEEE Wireless Communications*, vol. 31, no. 3, pp. 278–285, 2024.