Developing and experimenting simulation model of DDoS attacks in IIoT networks using Python

Aleksandar Hristov
Department "Information Technologies in Industry"
Technical University of Sofia
Sofia, Bulgaria
ahristov@tu-sofia.bg

Galya Pavlova
Department "Information Technologies in Industry"
Technical University of Sofia
Sofia, Bulgaria
raicheva@tu-sofia.bg

Kamelia Raynova
Department "Information Technologies in Industry"
Technical University of Sofia
Sofia, Bulgaria
kkaneva@tu-sofia.bg

***Abstract*— The DDOS attack vector on a PLC in an automated process control system is investigated and a simulation model for determining the DDOS attack vector on a PLC in an IIoT network was developed using Python. The proposed simulation model can be used for predicting the time for conducting successful DDoS attack, which allows to estimate the maximum response time of defense systems.**

Keywords—computer security, DDoS attack, defense system

I. INTRODUCTION

The number of malicious impacts that are noted in automated process control systems is increasing annually. This indicates the constant interest of attackers in such systems and the trends in the improvement of cyberattack methods. At the same time, the development of systems that protect from cyberattacks the automated control systems does not always keep the pace of the cyberattack methods [1] improvement. Programmable logic controllers (PLCs) are also at risk, as they are generally part of industrial digital equipment that interfaces with the corporate network [5]. One of the simplest and most effective cyberattacks is DDoS (Distributed Denial of Service). DDoS attacks are among the most common attacks that disrupt the synchronization of network processes. The number of DDoS attacks is continuously increasing, attacks are becoming more intense, longer lasting and involve a larger number of targets. Well-known DDoS attack patterns are often complex and require knowledge of the specifics of a particular DDoS attack and its intensity [4].

The literature review showed that many of the proposed models involve a large amount of heterogeneous input data, many of which are difficult to specify with acceptable accuracy or require configuration and use of artificial intelligence methods and tools [2,6]. This affects the computation time and the accuracy of the final results. The presented model does not address the specifics of the types of DDoS attacks, but relies only on their impact on the target host, which is characterized by the average denial-of-service time. The model in [1] is based on a stochastic network, which allows to estimate the average time of successful DDoS attack as well as the distribution function of the attack time. A DDOS attack vector is defined as a sequence of intruder actions resulting in unauthorized access to the target system and leading to a denial of service.

Determining the time needed for a successful DDoS attack is very important for building a management system, as a large number of processes being processed, many of which take place in dangerous conditions and require accurate and synchronized exchanges. Even a low-intensity DDoS attack can disrupt the synchronization of processes in the network and eventually halt communication completely, which can cause significant equipment damage [4]. Therefore, the protection systems should be designed by taking into consideration the execution time of a successful DDoS attack in order to adjust the response time. The average time needed for a successful DDoS attack can be used to estimate the required response time of cyber defense systems and could be used in embedded network-information security tools. If the response time of the defending systems and the time to take the necessary measures is less than the average time to carry out a DDoS attack, then, as a rule, the probability of a successful attack is significantly reduced. Many devices, including programmable logic controllers - PLCs, which are part of automated manufacturing process control systems, do not have sufficient built-in information security tools [5], making them extremely vulnerable to DDoS attacks. As a result, various additional protection systems, including adaptive and intelligent ones are added, eg. Secure core [6].

The aim of this paper is to develop a simulation model for determining the DDOS attack vector on a PLC in an IIoT network.

II. IMPLEMENTATION OF A DDOS ATTACK

The sequence of steps (Fig. 1) for successful implementation a DDOS attack is discussed below:

1. The attacker runs software to generate threat intelligence queries on the IIoT network. This takes a certain time, defined by its mean value, t1, and its probability distribution function P(t1).

2. The attacker scans the network to determine its topology, hosts, their software versions, open ports, and network services running. The duration of this process is defined by the mean value of the time needed for scanning the network, t2, and its corresponding probability distribution function is P(t2). The described actions of the attacker are assumed to be successful with probability P2.

3. If any of the attacker's actions in step 2 is unsuccessful, he creates a process to restart the network scanning software with probability (1 - P2). This restart takes a certain time, which is defined by its mean value - t3 and its probability distribution function P(t3).

979-8-3503-0329-2/23/$31.00 ©2023 IEEE

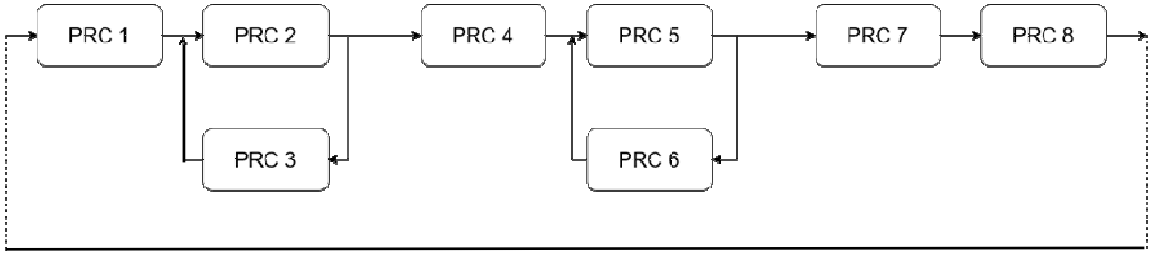

Fig. 1. Steps of successful DDOS attack

4. Upon successful completion of the process in step 2, the attacker analyzes the collected data, looking for hosts with available vulnerabilities. The process in this step has a duration defined by its mean time t4 and a distribution function P(t4).

5. Upon successful completion of the process in step 4, the attacker creates a process to initiate a connection to the target host. This process has a mean time t5 with the corresponding distribution function. The probability of successfully connecting to the attacked host is characterized by the probability P5.

6. If the connection process (step 5) is unsuccessful, i.e., with probability (1-P5), the attacker initiates a process that prepares his system for another attempt to connect to the attacked host. The process in step 6 on has mean duration t6 with its corresponding probability distribution function.

7. If the connection process (the process in step 5) completes successfully, the next process is initiated in which the attacker receives a confirmation of successful connection. The mean time for this step is t7 and there is has probability distribution function P(t7).

8. If all previous processes are successfully executed, the attacker initiates the last process, i.e. a direct DDoS attack, by sending UDP requests to the attacked host. The result of the attack occurs after mean time t8, which has a probability distribution function P(t8).

The probability of successful completion of a process Pj of step j (j=1,2...8) can be set according to specific threat models or, as in [1], their probabilities may take values in the range [0.7, 1] with a predefined step.

Below, the DDOS attack vector on a PLC in an automated process control system is investigated. The model is based on the queuing systems and allows estimation of the mean time for a successful DDoS attack as well as the distribution function of the attack time.

The model is a closed queue system in which the elements corresponding to the processes from the steps above PROC[j] j={1,2,4,5,7,8} are sequentially connected.

Figure 2 shows the Q-diagram and its corresponding GPSS (IBM General Purpose Simulation System code [2,3]) segment for process PROC[j]. The PROC[j] process has an input from the previous process (PROC[j-1]), and an output towards the next process(PROC[j+1]). Processes PROC[2] and PROC[5] which have probabilities P2 and P5 are assumed to have output towards to the next processes (PROC[3] and PROC[6] respectively) with probability (1-P2) and (1-P5), respectively (See TRANFER PROBj,,LABi form Fig. 2). Process PROC[3] output is input of process PROC[2], while process PROC[6] output is input of process PROC[5].

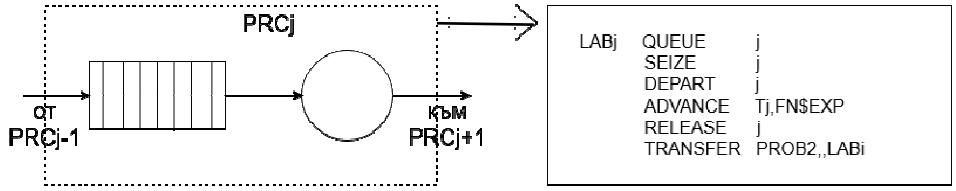

Fig. 2. Q-diagram its corresponding GPSS segment

Note that for each pass through the model (via the GPSS operators TABLE, MARK, TABULATE) the time is saved and tabulated. The resulting histogram is given in Fig. 5.

A Python application has been developed that offers the user a convenient graphical interface (Fig. 3) for entering the model parameters: the duration of each process Tj (j = 1,2...8) and the probabilities P2 and P5. These parameters are used for creating the GPSS model, which will be used for the experiment.

In order to obtain numerical results from the execution (conducting the experiment) of the simulation model thus created, it is necessary to run the GPSS interpreter. There are various licensed and free versions of GPSS interpreters available which require knowledge of their interface and ways to work with them, which makes it difficult for the user to experiment with the proposed above simulation model. For this purpose, an open-source GPSS code interpreter has been integrated in the developed application, by using the package gpss.py [8].

The programming implementation of the GPSS code interpreter is given in [9]. The Python code of the GPSS interpreter is given in [7]. The user-friendly form (Fig. 3) for users unfamiliar with the GPSS simulation system has been additionally created.

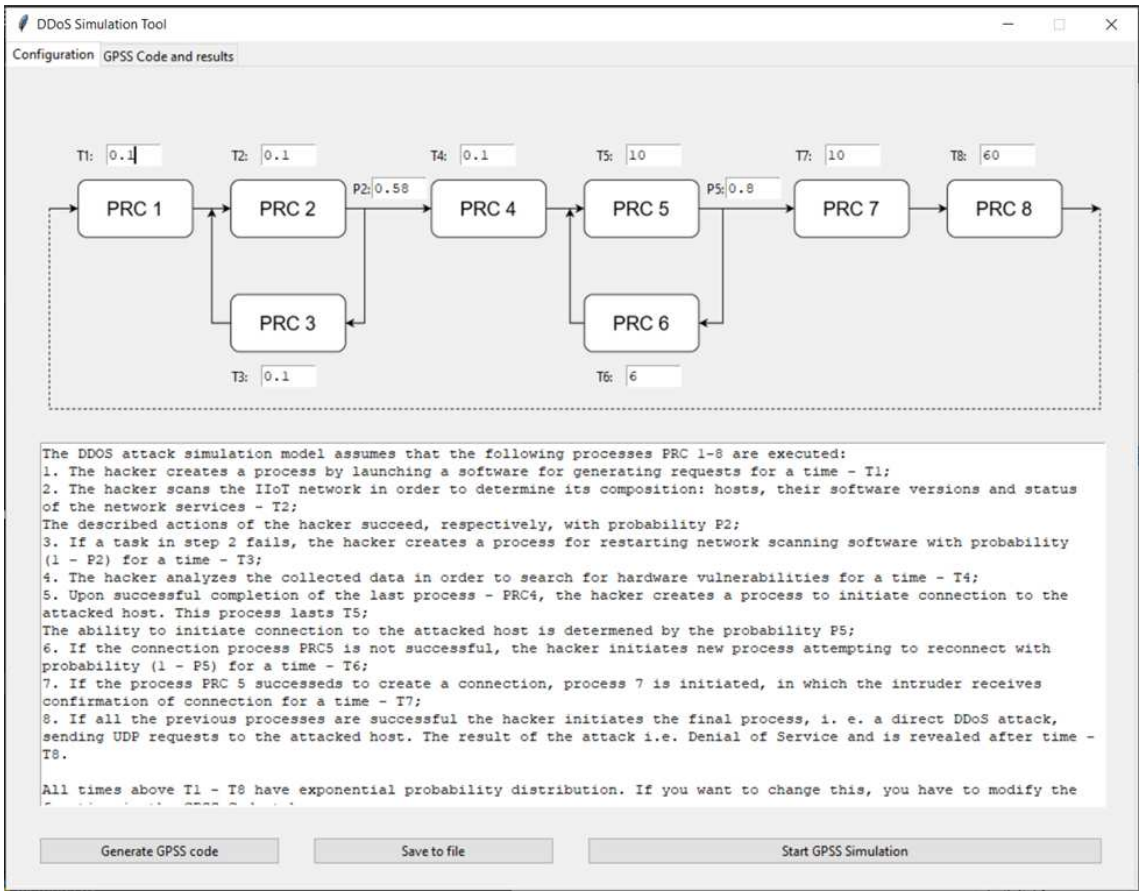

Fig. 3. A screenshot of the developed Python application

III. EXPERIMENTAL RESULTS

In order to verify the proposed simulation system, here as in [1], the mean values of step (1-8) durations are chosen as follows: T1 = T2 = T3 = T4 = 0.1, T5 = 10, T6 = 6, T7 = 10, T8 = 60.

The processes described are performed on a digital equipment and their behavior indicates that they are more likely to complete in a short period of time, whence the durations for successful completion of the processes in steps (1-8) are assumed to have an exponential distribution y=1-e^(λt).

It is also assumed that the probabilities used, P2 and P5, take values in the interval [0.7, 1] with step 0.1.

TABLE I. TABLE 1 MEAN TIME AND STANDARD DEVIATION OF SUCCESSFUL EXECUTION OF DDOS ATTACK IN IIOT NETWORK

Probability	0.7	0.8	0.9	0.9999
Mean	88.01	83.83	81.61	79.97
Std Dev	65.19	62.26	62.35	60.75

Fig. 4 shows the loading and execution of the model for DDoS attack in IIoT network using GPSS simulation application.

As it was mentioned above, by using the operators TABLE, MARK and TABULATE the time for which DDoS attack is conducted in IIoT network is saved and tabulated. The resulting histogram for P5 = 0.8 is given in Fig. 5. For the other values of this probability P (see Table 1), the type of histograms is similar and due to the limited size of the paper, are not applied here.

The results achieved with the proposed application and with inputs discussed above are given in Table 1. The obtained indexes match perfectly with the numerical values calculated mathematically [1] for the probability of conducting a successful DDoS attack in an IIoT network at F(t) = 0.63. For the rest of the values, the differences are insignificant. This can be considered as a verification of the proposed simulation model and GPSS simulation application.

IV. CONCLUSION

The proposed simulation model of DDoS attacks in IIoT networks can be used for predicting the time for conducting successful DDoS attack, which allows estimating the maximum response time of defense systems. If the reaction time of the defense systems plus the time for performing protective actions is less than the simulated average time for conducting a successful DDoS attack, then the probability of occurrence of significant consequences from DDoS attacks significantly reduces.

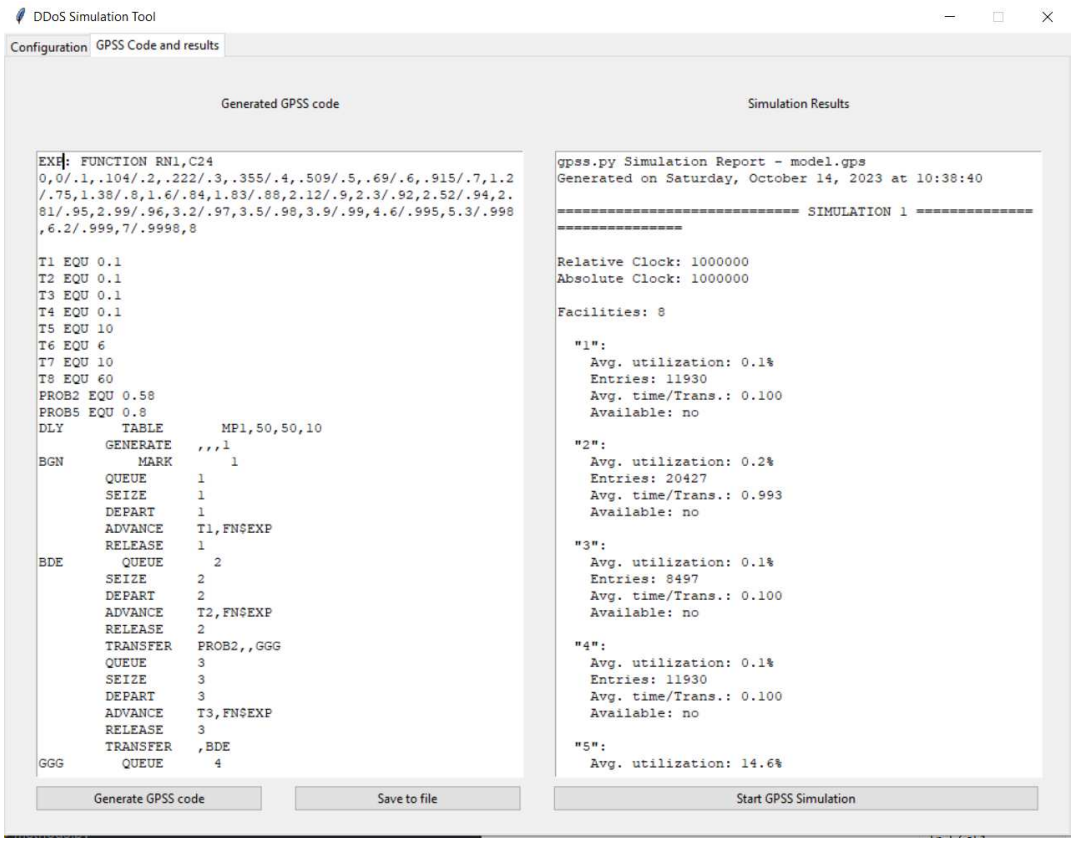

Fig. 4. Loading and execution of the model for DDoS attack in IIoT networ

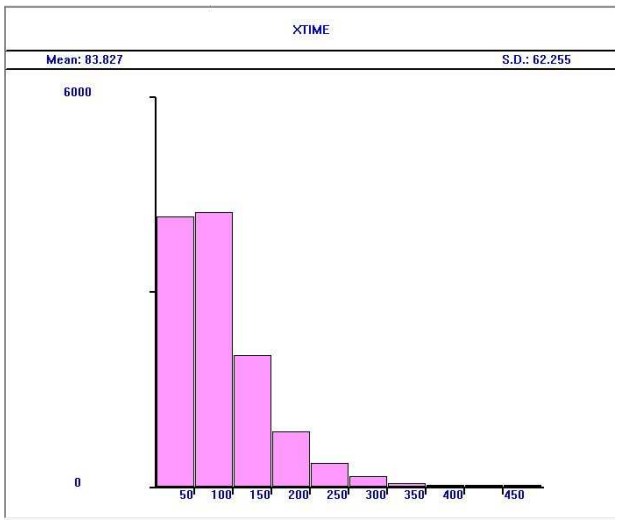

Fig. 5. Histogram of the distribution of times for successful DDoS attack in IIoT network

ACKNOWLEDGMENT

The presented research is funded by National Science Fund under the Ministry of Education and Science in Bulgaria with contract КП-06-Н 47/7 entitled “Possibility Investigation of Increasing the Cybersecurity of the Systems in Industry 4.0 using Artificial Intelligence”

REFERENCES

[1] Boger A. , Sokolov A. Mathematical model of the vector of a DDOS attack on the ICS using the method of topological transformation of stochastic networks, BKC , no. 4, 2023, pp. 72-77 (in Russian)

[2] HRISTOV, V. A visual environment for simulation of 802.11n wireless networks, BJED, ISSN 1313-7530, no. 10, 2012, pp. 37-44 (in Bulgarian)

[3] Mitrev, R. Computer modeling and Simulation, Propeler, Sofia, 2021 (in Bulgarian)

[4] Balarezo, J., et al. A survey on DoS/DdoS attacks mathematical modelling for traditional, SDN and virtual networks, Engineering Science and Technology, an International Journal, no. 31/2022.

[5] DDoS attacks in the second quarter of 2022 //Securelist by Kapersky, online available: https://securelist.ru/ddos-attacksin-q2-2022/105674/

[6] Chien-Ying Chen et al. Securing Real-Time Internet-of-Things, J. Sensors, no. 18, 2018, 4356

[7] Hristov, A. GPSS Simulation Tool online available: https://github.com/sashkinaaa/gpssGUI

[8] Documentation of gpss.py package online available: https://github.com/martendo/gpss.py

[9] Hristov, A. Using Python for development of an application for building and experimenting with GPSS simulation model, "TELECOM 2023" (IEEE Conference record # 59629), Sofia, 16 – 17 November 2023, submitted