Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

The vulnerability of securing IoT production lines and their network components in the Industry 4.0 concept

Tibor Horak*. Zuzana Cervenanska*. Ladislav Huraj. Pavel Vazan*. Jan Janosik*. Pavol Tanuska***

**Institute of Applied Informatics, Automation and Mechatronics*
Faculty of Material Science and Technology in Trnava
Slovak University of Technology in Bratislava Trnava, Slovak Republic
(e-mail: tibor.horak@stuba.sk).
***Department of Applied Informatics, University of SS. Cyril and Methodius*
Trnava, Slovakia (e-mail:ladislav.huraj@ucm.sk)}

Abstract: IoT systems are an integral part of every modern industrial enterprise Industry 4.0. IoT is the term for modern remote devices controlled via the Internet. Internet of Things is the name of technologies that allow cheap wireless connection and communication of various sensors and devices to automate, accelerate and streamline processes. In the interconnected world of Industry 4.0, there are many potential resources existing for infiltration. Cybercriminals could take control of manufacturing industries, manipulate machines, or could do an industrial espionage. This type of attack is called Denial of Service. In the second case, the attack preserves the attacker's anonymity through an IP address by using a potentially innocent third party (a reflector) that is indirectly involved in the attack. Through this attack, the attacker forwards the flow of attacking data to the target victim. The attacker sends the packets with a fake spoof source IP address set to the victim's IP address to the reflector, thus indirectly overloading the target with the packets, or it will intrude into a network device through a faulty WPS implementation. The simulation model of the production line and the IoT security system Fibaro were used to investigate these attacks. The article demonstrates the possibility of attacks on network devices and the misuse of IoT devices in order to compromise production machines which use DRDoS and Brute-force attacks.

Keywords: Industry 4.0, IoT devices, DRDoS attacks, WPS, Production line, Simulation

1. INTRODUCTION

Industry 4.0 is a concept of philosophical principles developed by German technology companies. These companies were Siemens, Bosch, Festo, Volkswagen, and other ones included as well. Industry 4.0 marks the process of optimizing production procedures by using the most modern technology findings in order to increase the production. It describes the transformation of production from separated automated units to a fully integrated automated and continuously optimized production environment. This is achieved by creating new global networks based on the interconnection of production devices to Cyber-Physical Systems (CPS). The CPS devices are a basic building block of "intelligent factories" and are capable of autonomous exchange of information, triggering the necessary actions in response to current conditions, and mutual independent control. Sensors, machines, parts and IT systems are interconnected within the value chain. These interconnected CPS devices can interact and analyze data by using Internet-based communication protocols, they can predict possible errors or failures, and also, they can configure themselves and, in real time, they are able to adapt in changed conditions Lee et al. (2015).

IoT systems are an integral part of every modern industrial enterprise Industry 4.0. IoT is the term for modern remote devices controlled via the Internet. Internet of Things is the name of technologies that allow cheap wireless connection and communication of various sensors and devices to automate, accelerate and streamline processes, distance measurement, increase comfort, remote control, enable better quality of life, and many other uses such as agriculture, waste recycling, medical care, production of virtual real estate, or movement in the gaming industry. The most common are sensors and small devices with low data requirements and low data consumption. Sensors and devices can communicate with each other, or with central systems, via conventional or special types of wireless networks. The typical usage for monitoring and measuring are sensors, e.g. agriculture, industry, environment and households, movement tracking, transport or transportation of goods, and human or animal location Shrouf et al. (2014).

In the interconnected world of Industry 4.0, there are many potential resources existing for infiltration. Cybercriminals could take control of manufacturing industries, manipulate machines, or could do an industrial espionage. This is just a small indication of similar behavior: In May 2017, the cryptoworm Wannacry infected, among other things, the computers of the British National Health Service, Renault's car manufacturer in France, and Deutsche Bahn. This malware encrypted the systems and temporarily paralyzed them. Hackers wanted to use it to demand ransom. Therefore, the companies have to take safety into account in Industry 4.0 projects in order to protect themselves Tuptuk et al. (2018).

2. ATTACKS IN IOT ENVIROMENT A COMPUTER NETWORKS

Many attackers focus exclusively on IoT devices because it is, both, users and manufacturers that are underestimated by the security of IoT devices that the attacker takes control of and can remotely order, for example, to request a specific website. If the attacker has many similar devices available, he can disable any website by using any of these available devices. It redirects so many requests to it that the server cannot handle them, and it stops communicating
Nowadays, the field of security is becoming increasingly more important and every data processing system has to count on it from the very first design. The industry linked to the Internet of Things already understands the need to prevent cyber attacks in the near future Bertino et al. (2016).
A DDoS attack is being led by multiple sources simultaneously, while attacking devices are sending either a large number of small requests to the target service, server, or network to disrupt service delivery by overloading primary resources (CPU overload, RAM overload) or large amounts of application data, in this case with the potential to completely overload the network infrastructure of the service provider.
A Distributed Reflection Denial of Service (DRDoS) attack maintains an attacker's anonymity through an IP address using a potentially innocent third-party (reflector) that is indirectly involved in the attack and through which the attacker forwards the flow of attacking data to the target victim. The attacker sends packets to the reflector's devices with a false source IP address set to the victim's IP address, thus indirectly overloading the target with packets. Therefore, it is difficult to identify real attackers and block their services. The reflector may be a regular, legitimate device, for example, IoT device, while it did not have to come to its compromise. If the amount of reflected packets is extremely large, the victim's network may be flooded. The advantage of DRDoS attack is that while tracing the source of the attack, the packets are not sent directly to the attacker, but only to the reflector, which is a device that forwards packets Xu et al. (2019).

WPS security is implemented by deterring network devices such as routers and access points. WPS has begun to be implemented in networking devices around 2010. Already in 2011, a way to break this security has been revealed and, at the same time, to reveal the secret key WPA2-PSK. This is a brute-force attack that targets an 8-digit PIN, which is actually a 7-digit PIN, since the last digit represents the checksum of the previous digits. Essentially, an attacker only needs to know the PIN to successfully authenticate against the network, so this request is prone to brute-force attacks. Later, the manufacturers of devices introduced the possibility of blocking an attacker for 60 seconds in case of three unsuccessful attempts to guess the correct PIN code. But this is only a small thing for this great lack of WPS security, because they only delay the time to get the PIN code. Later, WPS 2.0 version was developed, but only in version 2.0.2 was implemented permanent blocking of the attacker after 10 unsuccessful attempts to guess the correct PIN code. Even this latest version did not solve the wrong WPS structure, because an experienced attacker can write a script which defines that after 8 unsuccessful attempts to log off and change the MAC address, and so it can continue to attack with multiple devices until it detects the PIN code. About the WPS 2.0.2, there is a very little information offered, very difficult to find, so only few people know about this upgrade to version 2.0.2, and therefore, mainly use WPS 1.0, which is implemented on most devices, and turned on by default, so the device is then a threat to a large number of users, although it is also currently equipped with WPA2-PSK security Zhang et al. (2014).

3. EXPERIMENT DESIGN

3.1 Network topology

An experimental network was set up to carry out the attack. It also includes the ASUS-RT-AC66U high-speed router, which is capable of handling data rates of up to 1.75 Gbps, IoT Fibaro security. This router is designed to protect the enterprise from intrusion by unwanted people and bad weather conditions such as fires and floods. Another network forming device is simulation model of the production line As shown in (Fig.1) a simple star topology was used. The computer, which served as a packet generator, was connected wirelessly with an IoT security device with 54Mbps transfer rate, and the simulation of the production line was connected to the network via a 100Mbps LAN cable.

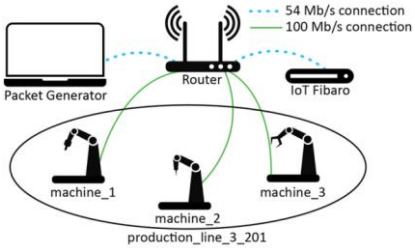

Fig.1. The topology of the testing network

3.2 Simulation model of the production line

An intention of this section is to present the impact of attack described above to the production performance indicators of hypothetic IoT aided manufacturing system with partially interchangeable workplaces. We simulate the shutdown of machine which is a part of a smart job-shop production system and observe an effect on the system behaviour and its dynamics in time. The investigation is conducted via the performance of a discrete-event simulation model adapted from Vazan et al. (2019). The chosen tested system is deterministic, of one-piece flow type with no random breakdowns. Also no random variation of operation times and setup times of machines are allowed. All these attributes were under consideration how to ensure easier direct studying the system behaviour.
The production line generates four types of products, each of them has a specified definition of the sequence of operations. The system includes six workplaces, partially interchangeable Table 1. presents the interchangeability of machines in the system. Operation times of machines are modified in the

relation to the type of processing operation. Also, all machines are setup when the type of operation is changed. The sequence of operations (that cannot be interchanged) and operation time for each operation are defined in Table 2. and Table 3. Own input and output buffers where priority rule FIFO is implemented are disposed to each of workplaces.

Table 1. Interchangeability of machines

Machine No.	Available Operations
1	A, C, D
2	A, F, G
3	B, C
4	D, E, G
5	B, F, C
6	E, G

Table 2. Definition of order operations for entering parts

Part No.	Operations Order
1	A, G, B, F
2	C, B, D, F
3	D, F, G, E
4	G, E, A, C

Table 3. Time operation for part related to operation order

Part No.	Operation Time Regarding Operation Order [min]
1	4, 6, 5, 3
2	5, 4, 3, 4
3	3, 3, 5, 3
4	5, 3, 4, 4

Conveyors including sensors that allow to identify every approaching part provide the parts transportation between buffers. If the appropriate part attribute has been detected, then this part is accepted for the following processing. The discrete-event simulation model is shown in (Fig.2). Simulation model is created in software Witness Horizon.

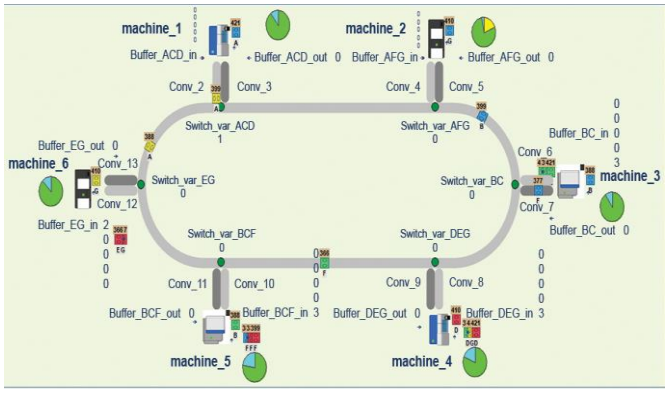

Fig.2. Simulation model of the investigated smart production line (Vazan et al. 2019)

The algorithm implemented into the simulation model ensured a right allocation on the base of the information on loading parts to the next location just after a performed operation in production process. The control system determines the subsequent machine that could perform the following operation and setup the attribute which fully identified the next machine. Implemented smart conveyor sensor system recognizes the attribute value and the part is conveyed to the input buffer of the allocated machine. The processing data acquired via simulation are automatically written into Excel sheet for the subsequent analysis.

All necessary simulation experiments related to the production line operation in a stable and normal status were performed under the identical simulation parameters, such as simulation run length 1440 minutes and the warm-up period 90 minutes. Production data were obtained in two forms: as the statistics outputs at the end of the simulation run and as the reports to Excel sheet, being written for each of parts in one minute period. On the base of these data, the total number of shipped products was 399, the total number of W.I.P. pieces was 109, and the average flow time was 170.30 minutes. Machine utilization after simulation run length 1440 minutes. The total average machine utilization is 85.63 % and the average number of parts related to the work in progress is 27.25 pcs.

As for the dynamics with which the machines operate, plots in (Fig.3) indicate the stabile throughput for every single machine in selected time range 100 minutes.

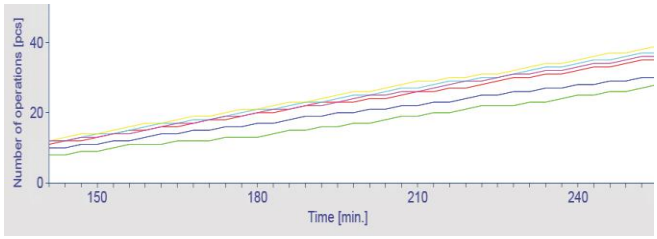

Fig.3. Simulation model output from Witness - the total number of operations for each of six machines vs. simulation time

4. ILLUSTRATION OF ATTACK

The attacks were performed in the following order, as our network infrastructure is equipped with a router which is equipped with WPA2-PSK security, and WPS 1.0 was performed by a brute-force attack to verify a faulty implementation of WPS 1.0. This implementation is used by majority of routers. Another attack was aimed at securing IoT security equipment Fibaro. This equipment has the task of protecting the company with motion sensors and sensors against floods and fires. With the help of DRDoS attack, the security of the Fibaro device will be verified, and this device will be misused in the attack to compromise the production line, and also the production process.

To attack a router in the infrastructure with WPA2-PSK security and WPS implementation. To perform the attack, the USB network card called Alfa network AWUS036NH was used. This network card supports monitoring mode and is equipped with an additional antenna for the best signal needed to successfully handle the brute-force attack. Last but not least, the Kali Linux testing version, which has to be equipped with the Reaver utility, has to be installed.

The whole wrong implementation is that the exchange of EAP messages during the authentication process is divided into 2 parts, in which the first and second parts of the PIN code, which the attacker compares with the PIN code stored in the router, are gradually compared. The messages during

this EAP are called M1-M8. If WPS authentication fails at any point, the router sends an EAP-NACK message to the attacker. It implies that if the attacker receives the EAP-NACK after sending an M4 message, the first half, 4 characters of the PIN code, was incorrect. If the attacker receives the EAP-NACK after sending an M6 message, then the other half of the PIN code, 3 characters, is incorrect.

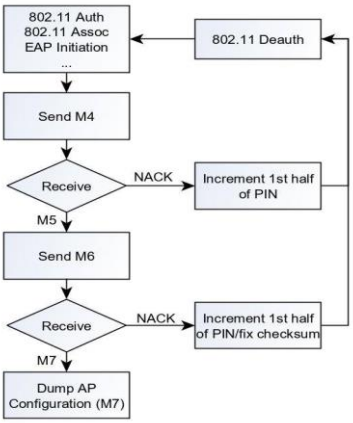

Fig.4. Flowchart on how brute force attack works on WPS PIN attack (Rianto 2019).

The shortcomings, shown above, imply that the number of attempts to guess the PIN code decreases when the brute-force attacks are used. From the original 10^8 to 10^4+ 10^3 attempts, since the last eight digit represents only the checksum. The maximum number of attempts, needed to break the PIN code, is 11000. The average number is 5500. The design error reduced the order by 4 numbers (from 8 to 4) in the number of attempts to gain the access to WPS secured by WLAN Rianto 2019.

The whole attack works the way that the router confirms the correctness of the first half of the eight-digit PIN code, regardless of whether the rest agrees or not. It is done by the so-called Reaver utility, which is implemented for brute-force attack, or, in other words, by brute force. Thus, in the first phase, the Reaver sequentially tests all possibilities ranging from 0000yyyy to 9999yyyy. For a PIN code of about 3 to 5 seconds, it is clear that a PIN code that starts with number 9 will take an attack, performed by brute force, for much longer than about 12 hours than with a PIN code that starts with a unit, in which case it takes up to maximally an hour or two.

The attack was successfully performed in about 4 and half hours by using utility River commands. After the PIN code was detected, the WPA2-PSK password was revealed as well. Therefore, a combination of running security is very dangerous. Although some manufacturers already implement toward WPS for 60 seconds attacker block after three unsuccessful authentication attempts; however, the real shortage does not just eliminate the attack time. In this case if such blocking is enabled, the attack would take approximately 70 hours. Even the upgrade to WPS 2.0.2 will not avert the threat because it only implemented only blocking after 10 unsuccessful attempts. It would be very easy for an experienced attacker to write just one script, which after 9 failed attempts, will log off and change the MAC address, and it will proceed further even with multiple devices at once, since the maximum number of comparison attempts is 11000, which is an average of 5500 Zhang et al. (2014).

After a successful attack on the router in this infrastructure, other DRDoS attacks were demonstrated, which were aimed to abuse the IoT Fibaro security equipment and individual production line machines to compromise the production line, respectively, the production process. A TCP, UDP, and ICMP infiltrations were performed by using Kali Linux via the hping3 tool. The Hping3 tool supports TCP, UDP, ICMP protocols. The settings and the packets generation are performed via the command line. These tools are also used by security analysts to verify the security of managed infrastructures.

In order to perform attacks, an ICMP type of an attack was used. This type of the attack is considered to be one of the invasive attacks oriented to the OSI network layer model. The attacker overloads targeted system by ping packets (ICMP Echo requirements), what gradually increases the urge of victim's response to them.

In the second attack, 2 DRDoS reflected attacks were performed, where the packets were generated for two minutes. Sending of the packets was set to the highest possible speed. The first attack was an ICMP echo Flood, in which an attacker sent the packets to IoT Fibaro security device on a non-existent port 350. The IoT Fibaro, with a false report, reflected these packets to a false set address that the machine_1 had, as can be seen in (Fig.5) and (Fig.6) After this attack, the machine_1 was permanently decommissioned for approximately 24 seconds.

The second attack was basically the same where the attacker sent ICMP echo packets to the machine (machine_3) of the production line, with forged machine_2 IP address (spoof) in the production line to which machine_3 reflected the error message packets of machine_2, where for approximately 12 seconds, the machine_2 of the production line stopped communicating permanently on the network even after the attack has ended.

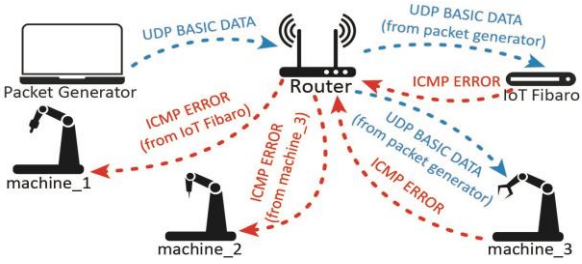

Fig.5. Visual illustration of the attack

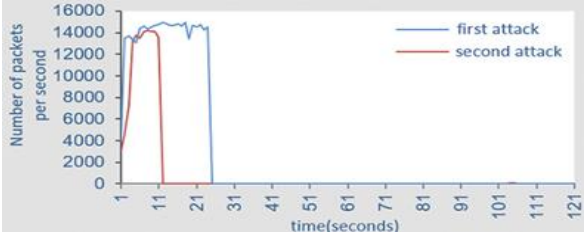

Fig.6. Number of reflected packets per second transmitted to the network by the IoT device and machines

4.1 The results of the first type of attack (shutdown of a single machine)

The response of the production system, after machine_1 failure had occurred, was monitored during simulation by tracking of the selected production data. In addition, the resulting status of processing, when simulation for 1440 minutes was performed, was checked too. Fig. 7 shows the change of the regular production process due to machine_1 failure in the term of total number of operations for six machines.

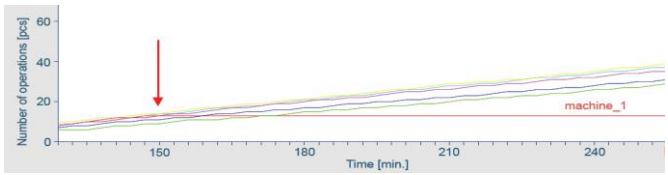

Fig.7. Witness output of the simulation model with the modelling of machine_1 failure vs. simulation time. A red arrow shows the moment of failure.

Table 4. shows the overall productivity of system with machine_1 failure after simulation 1440 minutes for four produced products. Now, the total number of shipped products falls down, the total number of W.I.P. pieces growths, the average flow time increases. Machine utilization is shown in Table 5. Due to the machine_1 failure, the average machine utilization decreases to 70.88 % and, on the other hand, the average number of parts related to the work in progress increases up to 41.5 pcs.

Table 4. Characteristics of the Processing with machine_1 failure (simulation run length 1440 min)

Product	No. Entered	No. Shipped	No. Rejected	W.I.P.	Avg. W.I.P.	Avg. Time
Product_1	86	76	41	10	18.95	297.53
Product_2	128	78	0	50	29.97	316.10
Product_3	127	84	0	43	23.11	245.61
Product_4	126	63	0	63	37.80	404.99

Table 5. Values of machine utilization with machine_1 failure (simulation run length 1440 min)

Machine Status	m_1	m_2	m_3	m_4	m_5	m_6
% Idle	0.01	1.26	0.00	0.00	0.00	0.00
% Busy	3.77	86.30	85.85	80.52	82.37	86.44
% Blocked	0.00	0.00	0.00	0.00	0.00	0.00
% Setup	0.52	12.44	14.15	19.48	17.63	13.56
% Broken Down	95.70	0.00	0.00	0.00	0.00	0.00
No. Of Operations	13	269	256	313	300	287

4.2 The results of the second type of attack (shutdown of two partially interchangeable machines sequentially)

Table 6. shows the performance of system with both machine_1 and machine_2 failure after simulation 1440 minutes for four produced products. In this case, the total number of shipped products decreases to 188, the total number of W.I.P. pieces increases to 224, the average flow time increases up to 477.1 minutes. The machine utilization is shown in Table 7. Due to both of machines failure, the average machine utilization decreases to 51.2 % and the average number of parts related to the work in progress increases to 56 pcs.

Table 6. Characteristics of the Processing with both machine_1 and machine_2 failure

Product	No. Entered	No. Shipped	No. Rejected	W.I.P.	Avg. W.I.P.	Avg. Time
Product_1	31	9	96	22	19.62	854.36
Product_2	128	84	0	44	16.35	172.40
Product_3	127	90	0	37	22.30	237.01
Product_4	126	5	0	121	60.17	644.73

Table 7. Values of machine utilization with both machine_1 and machine_2 failure

Machine Status	m_1	m_2	m_3	m_4	m_5	m_6
% Idle	0.01	0.76	35.96	0.00	0.00	15.70
% Busy	3.77	3.33	51.37	79.26	85.93	83.56
% Blocked	0.00	0.00	0.00	0.00	0.00	0.00
% Setup	0.52	0.07	12.67	20.74	14.07	0.74
% Broken Down	95.70	95.83	0.00	0.00	0.00	0.00
No. Of Operations	13	9	200	317	288	250

Fig.8. shows the change of the regular production process due to both machine_1 and machine_2 failure in the term of total number of operations for six machines.

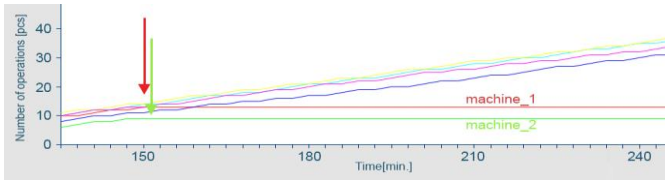

Fig.8. Witness output of the simulation model with the modelling of both machine_1 and machine_2 failure vs. simulation time

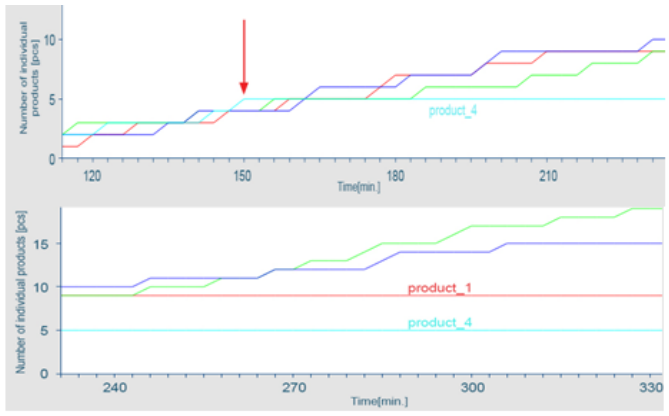

Fig.9 Witness output of the simulation model with the modelling both machine_1 and machine_2 failure - the number of shipped parts for each of four produced products.

A situation in the simulation model with both the machine_1 and machine_2 failure in simulation time 1440 minutes is depicted in Fig. 10.

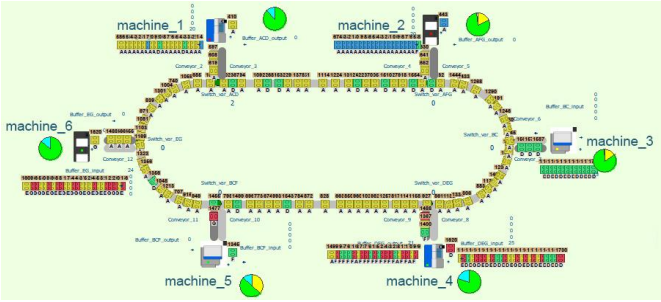

Fig.10. A status of the simulation model with both the machine_1 and machine_2 failure in simulation time 1440 minutes

5. DISCUSSION OF SIMULATION RESULTS AND ATTACKS

Applying the discrete-event simulation, we try to model the situation when one and more of the partially interchangeable workplaces are out of control because of shutdown caused by attacks DRDoS. The consequences are observed for both cases. When comparing the simulation results ofter 1440 minutes run for normal conditions of the production system, and results in Tables 4. and 5. related to the failure conditions of the investigated production line, we can see the strong negative effect of shutdown to the performance of the production system. In regards to the interchangeability machines in the production line, other four machines (except the machine_6) shoulder the processing of all products with operations A, D and G partially. In spite of the increasing number of operations (both machine_2 and machine_3), the outage of machine_1 causes less produced products, the longer average flow time and higher number of parts in process. The production of all four products is ensured but it is only in three quarters level related to the production under normal conditions.

In the case of the outage of two partially interchangeable machines, (Fig.8) and (Fig.9) confirm that the product 1 and subsequently also product 4 cannot be produced at all then. As can be seen in (Fig.10) conveyors and buffers are little by little filling up, they become the bottlenecks, the transport is partially blocked and therefore all production is slow down.

The results (Fig.6) clearly demonstrated how dangerous DRDoS attacks are and can cause major problems and damage to network infrastructures and production line, and therefore, it is important to ensure their safety.

Defense against a DDoS attack is not easy, and that is why it is necessary to divide the security activities carried out into several phases containing a number of other countermeasures, procedures, and defense mechanisms. The first phase is prevention, which is the basic and necessary part of the defense against the DDoS attack. It is based on the use of globally unified filters designed to stop or limit the number of attack packets. These unified filters can be further divided into ingress filtering, egress filtering, route based distributed packet filtering, history based IP filtering, secure overlay services, load balancing, and honeypot. The second phase is detection. It consists of recognition of defined patterns and anomalies in behavior, which are characteristic for DDoS attack. The best known detections are: behavioral anomalies detection and detection of designed patterns. The third phase is reaction. Once an attack or attempt is detected, it is necessary to identify as quickly as possible and then block the source of the attack. The best tools to use are: IP Traceback, ICMP Traceback, Link testing Traceback, Probabilistic packet marking, Hash based IP Traceback, Center Track, and Blackholing. For IoT devices, to reduce the security risk of connected devices, it is still necessary to check the login and access passwords, change the factory settings to new ones, and check all security features Tuptuk et al. (2018). When using routers with implemented WPS method, it is best to disable this security and not to use it as it becomes a potential threat for attacks. Many authors have warned about WPS threats for IoT, e.g. Nikolov (2018), but none addressed the impact of this vulnerability on the production line. It was not possible to disable this security for some brands of routers. In this case it will be the best to look for an upgrade of the firmware router to a higher version Zhang et al. (2014).

6. CONCLUSIONS

On the basis of the results, it was possible to point out exactly the behavior of the production line in case of compromising by a misused IoT security device. Based on these facts, certain methods, on how to prevent demonstrated attacks, have been described because attackers are able to misuse even the smallest security gap. Another direction will be the development of their own defense mechanisms and their testing of effectiveness against DRDoS attacks on IoT devices and production lines.

ACKNOWLEDGMENT

This work was written with the financial support of VEGA agency within the project 1/0232/18 “Using the methods of multi-objective optimization in a production processes control. “

REFERENCES

Bertino,E.; Raymond, K.; et al., (2016). Special Issue on Internet of Things (IoT): Smart and Secure Service Delivery, *ACM Transactions on Internet Technology*, Volume 16, pp. 22-28

Lee, J.; Behrad, B.; Hung-A. K.; (2015). Cyber-Physical Systems architecture for Industry 4.0 - based manufacturing systems. *Manufacturing Letters,* Volume 3, pp 18-23

Rianto, I.; (2013). Anticipating wps pin vulnerability to secure wireless network. *ComTech 2013,* Volume 4 pp. 1116-1121

Shrouf,F.; Ordieres,J.; Miragliotta, G.; (2014). Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. *IEEE International Conference on Industrial Engineering and Engineering Management,* 10.1109/IEEM.2014.7058728

Tuptuk, N.; Hailes, S.; (2018) Security of smart manufacturing systems. *Journal of Manufacturing Systems* , vol. 47, pp. 93-106.

Vazan, P.; Cervenanska, Z.; et al.; (2019) The impact of selected priority rules on production goals, *20th International Carpathian Control Conference* pp. 1-6. doi: 10.1109/CarpathianCC.2019.876592

Zhang, Y. et al., (2014) Attack and Analysis on the Vulnerability of Tenda Wireless Routers, *Applied Mechanics and Materials*, Volume. 556-562, Pages 5316-5320.

Xu, R.; Cheng, J.; Wang, F.; Tang, X.; Xu, J. A DRDoS Detection and Defense Method Based on Deep Forest in the Big Data Environment. *Symmetry 2019*, 11, 78.

Nikolov, L. G. (2018). Wireless network vulnerabilities estimation. *Security & Future 2*, 80-82.