Security in Industry 4.0 : Cyber-attacks and countermeasures

Aziz Naanani [a], Noureddine Masaif[b]
[a,b] Laboratory of Electronic Systems, Information Processing, Mechanics and Energy, Ibn Tofail University, Kenitra, Morocco
Email:[a]aziz.naanani@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Industry 4.0 or the smart factory is a concept that aims to improve productivity and organize the means of production. Industry 4.0 introduces a new way of communication in which products and machines are connected to a computer network. Plant components can communicate locally (local area network) as they can communicate internationally (wide area network). Industry 4.0 has therefore created a globally interconnected system in which maintenance and optimization can be conducted autonomously based on artificial intelligence and the Internet of Things (IoT). While it is true that relying on computer networks in today's factories will allow them to have better control, however this will make them vulnerable to attacks that can threaten the economy or the security of a country , and here we are talking about cyber attacks . In this article we will discuss the different cyber threats to the smart factory, their impacts and possible countermeasures.

Keywords: Cybersecurity, IoT, IIoT, Industry 4.0

1. Introduction

The industry has evolved rapidly over the course of time. In its first evolution,the Industry 1.0 was known by the invention of steam engines and intense coal mining. The next revolution, the Industry 2.0 had mass production as its main feature , and it relied on oil and electricity. The third generation,the Industry 3.0, was primarily known for the emergence of new electronic and telecommunications technologies that led to the development of PLCs and information systems in factories., the Industry 4.0 has changed factories, in fact the fourth Industrial Revolution made factories more agile, more efficient and more competitive. The Industry 4.0 is based on data technologies, communicating sensors, the IIoT (Industrial Internet of Things), piloting, simulation and information processing software. Figure 1 illustrates the evolution of the industry over time.

Industry 4.0 is no longer seen as a luxury but an obligation for factories wishing to survive and promote their activities. Thanks to specialized software, plant managers can customize productions, reduce costs and energy consumption, be able to remotely control and pilot the production equipment or even virtual networks, to control physical objects, allow the production equipment to self-diagnose.

Relying on new forms of communication, in particular computer networks, new connected machines , Cloud Computing, extends the vulnerability of factories and therefore leads to vulnerability that can jeopardize the activity of the factory and the entire Supply Chain . Attacks, whether intentional or accidental, are proliferating every day and are becoming much more sophisticated. In fact, the more communicating components are added in the plant, the more the vulnerabilities associated with it are added to the list of threats. In this article we will try to classify all the vulnerabilities and possible countermeasures to put in place in order to better secure an Industry 4.0 factory.

The rest of the article is organized as follows, in the second section we will discuss the main components of Industry 4.0. In the third section we will discuss the different threats related to Industry 4.0. In the fourth section we will present the recommendations and solutions to adopt to secure your plants. Finally,the fifth section will be devoted to the conclusion.

2.. Main components of the Industry 4.0

While Industry 4.0 provides unparalleled flexibility and improvement in production, production relies on several technologies to achieve this success.

Several technologies are associated with Industry 4.0, including IIoT, cyber-physical systems, cloud computing, artificial intelligence, big data.

2.1.Industrial Internet of Thing - IIoT

IIoT is the technology that allows all workstations, lines and logistics capacities to be all linked into a network. The network components communicate with each other and each of them communicates with the production control system. Objects integrated into a manufacturing process contain data in the form of design, production, or logistics parameters. The Industrial Internet of Things enables machines and systems to manufacture products practically in an independent way.

2.2.Cyber-physical system

A cyber-physical system is a composite autonomous system, combining sensors, software that posses data processing features and communication capabilities.The cyber-physical system interacts with its environment to drive physical processes and optimize industrial production.

2.3.Industrial cloud computing

Industrial cloud computing provides the essential platform for the secure sharing of data exchanged between machines and equipment in Industry 4.0 especially in the wider perspective where the unified production platform includes several production and logistics sites.

2.4.Artificial intelligence (AI)

Artificial intelligence (AI) enables machines to mimic forms of real intelligence, particularly the human brain, by integrating the ability to adapt its modus operandi according to external stimuli. AI in Industry 4.0 can be used to anticipate breakdowns and schedule maintenance. Thanks to its prediction assets, AI can also be used to simulate an industrial configuration by adding to the production parameters a flow of forecast data, economic, climatic and human behavior data.

2.5.Big data

Big data allows to massively collect structured or unstructured data from different sources In the context of Industry 4.0, this data can come from sensors, equipment or machines. Big data makes it possible to implement increasingly sophisticated process methods to control the quality of products along the supply chain (inventory management, transport, marketing, purchasing).

2.6.Threats related to Industry 4.0

The risks of attacks are increasing every day, critical industrial activities are now directly targeted by cyber attacks (energy and heavy production). Their identified vulnerabilities, and generally not protected, expose them to significant physical, environmental and / or financial consequences. According to the "Cisco 2018 Annual Cybersecurity Reports", almost 31% of organizations have been victims of cyber attacks related to the operational technology (OT) , while more than 38% predict the occurring of such cyber attacks. 75% of experts give top priority to cyber attack protection, only 15% believe their companies can deal with different cyber attacks.

Industry 4.0 generally has four main threats, these are denial of service, theft of intellectual property, industrial sabotage and finally the scourge of ransomware. These threats relate to attacks that can target components of the smart factory.

Figure 1 illustrates all of the cyberattacks threatening the Industry 4.0. These cyberattacks affect the hardware layer of the OSI model, especially the physical layer, layer 3 of the OSI model, the network layer and the layers 4 and 7 transport and network. In the rest of this section we will discuss the most prevalent and impacting the industry.

3.Denial of service

Denial of service is an attack that overloads equipment or services with a mass of data that they cannot process. The overload can be from a single source, in this case the attack is called DoS, or it could come from several sources, in this case the attack is called Distributed DoS ,or dDoS. In the case of the dDoS attack,a malware called botnets infects machines, then put them under the control of the hacker, who can order them to attack his victim. Since Industry 4.0 relies on a large number of interconnected devices, this attack remains very likely and can have a critical impact on the entire system. In article [1] the authors presented the Mirai botnet and its variants as well as the various damages that it can inflict upon an IoT architecture. In article [2] the authors exploited the DNP3 and Modbus protocol to inject traffic causing a denial of service. The Distributed Network Protocol (DNP3), which is used in automation systems primarily by electric utilities and water utilities. DNP3 was developed for communication between different types of control and data acquisition systems. It plays an important role in SCADA systems, and it is used by control centers, terminal units (RTU) and intelligent electronic devices (IED). The authors have shown that a simple authentication limit can lead to considerable losses. Article [3] proposed a new authentication method deployed at the IoT or IIoT level without the data being stored locally, authentication is based on challenges to verify identities. The authors of the article [4] exploited vulnerabilities in the UDP transport protocol ,and through NTP and DNS, were able to generate unusually high levels of traffic on the network to cause disruption. A new dDoS attack has been developed exploiting the MQTT protocol thus threatening the availability of the entire IoT and IIoT architecture [5]. MQTT is a Machine-to-Machine (M2M) data transfer protocol that enables SCADA systems to access IIoT data. It is considered one of

the main messaging protocols of the IIoT. In this article, the authors exploited a specific weakness in MQTT that allowed the client to configure server behavior. In order to validate the possibility of exploiting such a vulnerability, the authors proposed SlowITe, a new low rate denial of service attack aimed at targeting MQTT via low rate techniques. Specifically, the authors exploited the ability to set the Keep-Alive parameter of the server from the client itself, thus configuring the behavior of the server, in terms of connection close times, from the attacking node.

3.1. Data tampering and identity theft

Data tampering is an attack that involves altering data in transit between one node and another. This falsification can be carried out by interception during the transfer or by identity theft. Identity theft allows an attacker to get through the a node or a machine in the plant, thus making it possible to receive all the information that is generated at the plant, and to possibly respond instead of the legitimate machine. This attack is known as the Man in the Middle (MITM). These kinds of threats are very common in Industry 4.0 due to vulnerable identification mechanisms. The Transport Layer Security TLS protocol was developed to add a layer of security , by first of all authenticating communicating machines and verify the integrity of authenticated exchanges. However, this TLS protocol can be vulnerable to identity theft attack, the intruding machine can take the role of the server to participate in the challenge and recover the machine's authentication data and intercept its data and possibly modify them, without having the possiblity to intercept the intrusion. Article [6] proposed an effective new model to avoid this manipulation exploiting identity theft when establishing a TLS secure channel. The proposed authentication mechanism is based on the SISCA mechanism which is proposed in article [7] and relies on "ID-based Channel" authentication and server invariance. With the emergence of IoT technologies, the block chain has become essential. The block chain is a cryptography-based computer protocol used to secure data transferred digitally from a single source to a single recipient. Finally, the block chain brings confidence in the data through the non-centralization of authorizations, and authentication. All of these processes are "distributed" over a network which reduces the risk of errors or corruption. Thus this new technology makes it possible to solve genuineness problems related to a given data. Through article [8], the authors proposed a secure wireless mechanism using Block Chain technology that stores the extorted procedures of each record in a number of blocks. The blockchain scheme is typically used to extort information from the sensors and further preserve it in the blockchain to ensure security and provide transparency between users in various locations.

Table 1 illustrates a summary of the most prominent cyberattacks in the Industry 4.0

Table 1 List of the most prominent cyber attacks in Industry 4.0

Year	Virus	Function	Affected sector	Impact
2009	Night dragon	Distribute RAT- Remote Administration Torjans. The virus allowed a remote takeover of infected systems by the attackers.	Fossil fuel	hijack Scada systems operating diagrams, as well as data
2010	Stuxnet	A computer worm used to spy on and reprogram industrial systems at Iran's Natanz nuclear site.	Nuclear	Destruction of nuclear centrifuges in Iran
2014	Havex	scans the local network for servers that collect data from industrial equipment, then routes that data to a Command & Control server.	-	industrial espionage and data hijacking
2015	Black Energy	When opening the document, a dialog box appears recommending that the user enable macros so that they can view the content. Enabling macros triggers infection by the BlackEnergy malware.	Industrial Control Systems (ICS), Energy, Government and Media in Ukraine	Industrial sabotage

2016	Mirai	Mirai identifies vulnerable IoT objects with a default ID and password table and then simply logs in to install the malware	Deutsche Telekom (DEU)	Failure at Deutsche Telekom
2017	WannaCry	WannaCry targets computers that use the Microsoft Windows operating system. It encrypts the data and demands the payment of a ransom in cryptocurrency (bitcoins) for it to be returned.	Renault, FedEx, Spanish telecom operator Telefonica, German railway company Deutsche.	Loss of data
2019	Ransomware	Baltimore's computer network has been infected with ransomware. The city remained paralyzed for several weeks. The damage is estimated at 18 million USD.	U.S.A	loss of production

4. Countermeasures

As a response to the various IIoT cyberattacks, several solutions and equipment can be put in place to guarantee the availability, confidentiality, integrity, authentication and non-repudiation of data.

4.1.Encryption

It is important to ensure that production facilities are safe for people, the environment and the data and information they contain. Data must therefore be absolutely protected against misuse and unauthorized access. The first risk concerns industrial espionage, in fact, a low level of encryption in the cloud environment is a major problem because a hacker, or an organization, can bring down many factories and not just a single site. The use of VPN (Virtual Private Network) solves several problems mainly of availability, confidentiality, integrity and authentication of data.

4.2.Firewall

Preventing unsolicited connections can reduce but not negate the risk of infection with viruses and malware. A firewall is a device that can authorize or prohibit a flow according to its attributes. The latter, in a factory is often configured in different zones at least three; the Inside zone, the Outside zone and the DMZ demilitarized zone. Communication between these zones is governed by security levels, in which the Inside zone is level 100,and the outside zone is 0 , while the DMZ zone is between 0 and 100. Communication between a higher level to a lower level is allowed while the reverse is not , only after a manual authorization has been granted by the administration. Most often, any connection from the outside is redirected to the DMZ which can tolerate failure or else it does not contain confidential information.

4.3.Antivirus and Malwares

More than filtering, it's about inspecting. Because most viruses hide behind authorized traffic, deep packet analysis systems can analyze signatures and determine the type of virus. In Operational Technology - OT, it is impossible to control computers because they can be embedded inside PLCs and you cannot install an antivirus on them. To protect themselves from infected USB keys, factories can install electronic customs posts that materialize the separation between the OT and the IT. This is a secured USB port that allow only signed files to be transfered . Likewise, installing an antivirus has side effects on the performance of the machine on which it is installed. The Norman Shark ICS Protection solution allows a workstation to accept a USB key only if it has been scanned and guaranteed to be virus-free. In addition, with its Trend Micro Portable Security 2 solution, the eponymous publisher offers its antivirus in the form of a USB key to scan equipment on which it is not possible to install software.

Table 2 illustrates all of the work carried out in relation to cyber attacks on industrial networks.

Table 2 Liste of cyber attacks and their solutions

Title	Problem	Existing solutions	Reference
A machine learning based approach for intrusion prevention using honeypot interaction patterns as	resolve network intrusion	Machine learning:Using honeypot interaction patterns as training data	[9]

training data			
Explorative Techniques and VulnerabilityAssessment on Automotive Networks	ECU: automated vulnerability due to standard commands and brute-force possibility	filtering by the CGM.	[10]
Extend Your Car's Attack Surface Through Smart Devices	OBD-II attack by GSM owner (long range)	OBD-II dongle+custombuilt framework for performing penetrations tests on OBD-IIdongles will be the major goal	[11]
Classification and Analysis of Communication Protection Policy Anomalies	detection of anomalies(classified in two taxonomies) that can arise during the implementation of communication protection policies	using FOL formulas	[12]
Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat	resolve the activeMITM attack	use strong mutual authentication techniques, encryption and decryption algorithm, proper configuration of client and server handshake mechanism to reduce this attack.	[13]
Detection of Address Resolution Protocol Attacks	detect malicious activities against the Address Resolution Protocol, and anomalies originating from its different implementations.	network flow monitoring and extended IP flows	[14]
Android Malware Detection Using Network Behavior Analysis And Machine Learning Classifiers	detection of botnets malware from benign applications and in then classification of malwares dataset on a base of family.+performed an analysis of Android botnets that employ HTTP traffic for their communications	using machine learning : 1-networklevel behavioral malware classification system that focuses on HTTP-based malware and classification malware samples based on a notion of statistical similarity between the malicious HTTP traffic they generate. 2-the samples belonging to the same malware family have structural similarity between HTTP malicious traffic traces.	[15]
Computer and Network Forensics: investigating network traffic	what and if any content can be revealed while someone investigates network traffic, meaning doing packet sniffing, with a special monitoring and analyzing tool, Wireshark.	encryptation	[16]
ENERGY-GRID THREAT ANALYSIS USING HONEYPOTS	cyber threats to smart energy grids	a high-interaction honeypot that simulates a grid named GridPot	[17]
Securing Web Applications: Web Application Flow Whitelisting to Improve Security	It targets two of OWASP's top ten web vulnerabilities; A4: Insecure Direct Object References and A7: Missing Function Level Access Control.	web application flow whitelisting	[18]
NETWORK FORENSICS ANALYSIS	detection of stealthy TCP, ICMP, UDP packets which are malicious in snort.		[19]
Security Threats and Countermeasures for Connected Vehicles	identification of 25 services that connected vehicles can provide	TLS based connection from TCU to remote servers to ensure communication's authenticity, integrity, and	[20]

		confidentiality. IPsec is selected for in-vehicle communication with the Time-based One-Time Password algorithm to allocate secret keys. Biometric authentication would make this process easier.	
Internet Censorship: An Integrative Review of Technologies Employed to Limit Access to the Internet, Monitor User Actions, and their Effects on Culture	Demactaratization of internet	vpn+liberal proxys(TOR...)	[21]
An Interception System for ISPs (ISISP)	network intrusions	Low level packet sniffing. Good tool for memory management(C#).	[22]
Enabling Auditing and Intrusion Detection of Proprietary Controller Area Networks	Cyber attacks against passenger vehicles	automation of lexical and semantic analysis for Cyber-Physical System (CPS)	[23]
Formal Network Behaviour Analysis using Model Checking	Designing and configuring individual network devices to function correctly as per specifications, such as protocol standards or security policies	with mathematical rigour it's possible in a corporate environment to mitigate network-based information leakage.	[24]
A three-layered robustness analysis of cybersecurity:Attacks and insights	Wireless communication networks attack (in the physical layer, the data-link layer, and the network layer)	new network's access points that can maintain connectivity in the advent of an also optimal jamming attack	[25]
Denial of service attacks – an updated perspective	prevent to DoS	presented various attack vectors,attack tools, trends in detection and mitigation mechanisms.	[26]
Comparative Analysis Based on Sur e Analysis Based on Survey of DDOS A y of DDOS Attacks' ttacks' Detection Techniques at Transport, Network, and Application Layers	detecting attacks on Network, Transport, and Application Layers	machine learning solution	[27]
Detection of Address Resolution Protocol Attacks	detecting ARP attacks from network flow data and to implement a proof-of-concept tool	network flow monitoring+flow measurements	[28]
The Post-GIG Era:From Network Security to Mission Assurance	cybersecurity through network defense, to mission assurance through information assurance	composing timely assurance out of untrusted components, and a shift towards commercial cloud solution.	[29]
DATA COMMUNICATIONS AND APPLICATION DEVELOPMENT OF A FULL-POWER CONVERTER IN WIND POWER SYSTEMS	implementation of a parameter exchange functionality between the cabinet automation logic and primary controls, and a supervision functionality for the power module cooling fans+keep the DC-link capacitors at optimal temperature	Opening some of the essential parameters to the customer makes the "FPC+ product"+ supervision functionality	[30]

THREAT MITIGATION IN INDUSTRIAL INTERNET: CASE VARIABLE-FREQUENCY DRIVE	cybersecurity industrial devices :case study and the target device was variable-frequency drive (VFD)	prioritisation method was Weighted Shortest Job First (WSJF)+Secure Boot, Endpoint and Configuration Control and Remote and Automated Endpoint Update.	[31]
INTEGRATING ELECTRIC VEHICLES INTO SMART GRID USING IEC 61850 AND ISO/IEC 15118 STANDARDS	uncontrolled charging of electric vehicle would cause a significant impact on the grid operations and planning.	computer program for simulate the charging process between the vehicle and the charging post+ based on IEC 61850 for monitoring and controlling of electric vehicle.	[32]
PACKET FILTER APPRO TER APPROACH TO DETECT DENIAL OF SER AL OF SERVICE ATTACKS	Denial of service attacks	neural networks	[33]
A Scenario Based Performance Analysis of VANET Protocols	analysing the performance of several VANET protocols for real scenarios	provided a realistic model for Auckland and evaluate VANET protocols in different areas of Auckland to see which protocol works better for each area. The routing protocols we investigated include AODV, DSR, OLSR, DSDV, GPSR, CBRP, and ZRP. Using Nakagami as the propagation model.	[34]
CYBERGAME SECURE APPLICATION DELIVERY	ready framework for a web application called Cybergame by implementing secure and optimized application delivery features.	knowledge of F5 ADCs	[35]
NAVAL CYBER WARFARE: ARE CYBER OPERATORS NEEDED ON WARSHIPS TO DEFEND AGAINST PLATFORM CYBER ATTACKS?	exploration of the general vulnerabilities of the computer networks on modern warships	update ICS, navigation systems and CMS. (navy specific cyber operators)	[36]
Multidimensional Intrusion Detection System for IEC 61850 based SCADA Networks	intrusion detection for IEC 61850 based substations is lacking. In particular, published literature lacks validation of solutions using data from real electrical substations. Furthermore, and as a result, many published approaches do not focus on providing solutions that are truly tailored to practical implementation at the physical application layer	novel use of configuration information from the SCD file in order to automatically configure the deployed IDS to the substation where the IDS is installed. The proposed solution also adopts detection appraches based around expert knowledge such as GOOSE and SMV parameter configuration data	[37]
Multi-Channel Security through Data Fragmentation	security architects to develop a secure, multi-channel communication system	increasing the number of channels utilized	[38]
Intrusion Detection for Smart Grid	vulnerabilities associated to the smart grid.	anti jamming and spofing using algorithms	[39]

Communication Systems			
Firewalls: A study on Techniques, Security and Threats	network intrusions	using firewalls	[40]
DESIGNING A PROTOCOL AGNOSTIC RULE ENGINE FOR A CROSS-DOMAIN SOLUTION	designing the core component of the CDS	using protocols: ASTERIX and the HLA	[41]

5.Conclusion

Through this article we have discussed the role of Industry 4.0, its components and the associated cyber attacks. Although Industry 4.0 has become a necessity to increase production and ensure efficient communication between different machines, the latter is seen as an active field for cyber attacks. Protection against cyber attacks on an industrial network does not stop with the deployment of the most sophisticated solutions, but also to the awareness of users because most attacks can exploit the naivety of employees or the neglect of the impact of the cyberattack on the continuity of production.

References

1. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.
2. Gao, W., Morris, T., Reaves, B., & Richey, D. (2010, October). On SCADA control system command and response injection and intrusion detection. In 2010 eCrime Researchers Summit (pp. 1-9). IEEE.
3. M. N. Aman, K. C. Chua and B. Sikdar, "A Light-Weight Mutual Authentication Protocol for IoT Systems," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8253991.
4. V. Borgiani, P. Moratori, J. F. Kazienko, E. R. Tubino and S. E. Quincozes, "Towards a Distributed Approach for Detection and Mitigation of Denial of Service Attacks within Industrial Internet of Things," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3028652.
5. Vaccari, I., Aiello, M., & Cambiaso, E. (2020). SlowITe, a Novel Denial of Service Attack Affecting MQTT. Sensors, 20(10), 2932.
6. Karapanos, N., & Capkun, S. (2014). On the Effective Prevention of {TLS} Man-in-the-Middle Attacks in Web Applications. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (pp. 671-686).
7. Esfahani, A., Mantas, G., Ribeiro, J., Bastos, J., Mumtaz, S., Violas, M. A., ... & Rodriguez, J. (2019). An efficient Web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain. IEEE Access, 7, 58981-58989.
8. Rathee, G., Balasaraswathi, M., Chandran, K. P., Gupta, S. D., & Boopathi, C. S. (2020). A secure IoT sensors communication in industry 4.0 using blockchain technology. JOURNAL OF AMBIENT INTELLIGENCE AND HUMANIZED COMPUTING.
9. Zammit, D. (2016). A machine learning based approach for intrusion prevention using honeypot interaction patterns as training data. University of Malta, 1-55.
10. CALIN, L. R. (2018). Explorative techniques and vulnerability assessment on automotive networks.
11. Hackenberg, R., Weiss, N., Renner, S., & Pozzobon, E. (2017). Extend Your Car's Attack Surface Through Smart Devices.
12. Valenza, F., Basile, C., Canavese, D., & Lioy, A. (2017). Classification and analysis of communication protection policy anomalies. IEEE/ACM Transactions on Networking, 25(5), 2601-2614.
13. Alwazzeh, M., Karaman, S., & Shamma, M. N. (2020). Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat. Journal of Cyber Security and Mobility, 449-468.
14. Hijazi, S., & Obaidat, M. S. (2019). Address resolution protocol spoofing attacks and security approaches: A survey. Security and Privacy, 2(1), e49.
15. Amos, B., Turner, H., & White, J. (2013, July). Applying machine learning classifiers to dynamic android malware detection at scale. In 2013 9th international wireless communications and mobile computing conference (IWCMC) (pp. 1666-1671). IEEE.
16. Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. digital investigation, 7(1-2), 14-27.
17. Kendrick, M. M., & Rucker, Z. A. (2019). Energy-Grid Threat Analysis Using Honeypots. Naval Postgraduate School Monterey United States.

18. Alabdulrazzaq, H. (2017). Securing Web Applications: Web Application Flow Whitelisting to Improve Security.
19. Corey, V., Peterman, C., Shearin, S., Greenberg, M. S., & Van Bokkelen, J. (2002). Network forensics analysis. IEEE Internet Computing, 6(6), 60-66.
20. Luo, F., & Hou, S. (2019). Cyberattacks and countermeasures for intelligent and connected vehicles. SAE International Journal of Passenger Cars-Electronic and Electrical Systems, 12(07-12-01-0005), 55-66.
21. Hyland, J. (2020). Internet Censorship: An Integrative Review of Technologies Employed to Limit Access to the Internet, Monitor User Actions, and their Effects on Culture.
22. Bader, A. A. A. E., & Mikki, M. An Interception System for ISPs (ISISP).
23. Stone, B. C. (2018). Enabling Auditing and Intrusion Detection of Proprietary Controller Area Networks.
24. Brown, D. G. (2016). Formal network behaviour analysis using model checking (Doctoral dissertation, Queensland University of Technology).
25. Schweitzer, D. (2019). A Three-Layered Robustness Analysis of Cybersecurity: Attacks and Insights. Mississippi State University.
26. Kumar, G. (2016). Denial of service attacks–an updated perspective. Systems science & control engineering, 4(1), 285-294.
27. Kolandaisamy, R., Md Noor, R., Ahmedy, I., Ahmad, I., Reza Z'aba, M., Imran, M., & Alnuem, M. (2018). A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks. Wireless communications and mobile computing, 2018.
28. Abad, C. L., & Bonilla, R. I. (2007, June). An analysis on the schemes for detecting and preventing ARP cache poisoning attacks. In 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07) (pp. 60-60). IEEE.
29. Jabbour, K. (2019). The Post-GIG Era. The Cyber Defense Review, 4(2), 117-128.
30. Salokanto, T. (2016). Data communications and application development of a full-power converter in wind power systems (Master's thesis).
31. Kankaanranta, A. (2018). Threat mitigation in industrial internet: Case variable-frequency drive (Master's thesis).
32. Gasto, A. L. (2016). INTEGRATING ELECTRIC VEHICLES INTO SMART GRID USING IEC 61850 AND ISO/IEC 15118 STANDARDS.
33. Muharish, E. Y. M. (2016). Packet filter approach to detect denial of service attacks.
34. Alobaidi, N. (2017). A scenario based performance analysis of VANET protocols (Master's thesis).
35. Järviö, J. (2017). Cybergame secure application delivery.
36. Andress, J., & Winterfeld, S. (2013). Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier.
37. Yang, Y., Xu, H. Q., Gao, L., Yuan, Y. B., McLaughlin, K., & Sezer, S. (2016). Multidimensional intrusion detection system for IEC 61850-based SCADA networks. IEEE Transactions on Power Delivery, 32(2), 1068-1078.
38. Hayden, M., Graham, S., Betances, A., & Mills, R. (2020, March). Multi-Channel Security through Data Fragmentation. In International Conference on Critical Infrastructure Protection (pp. 137-155). Springer, Cham.
39. Chatfield, B. (2017). Intrusion Detection for Smart Grid Communication Systems.
40. Neupane, K., Haddad, R., & Chen, L. (2018, April). Next generation firewall for network security: A survey. In SoutheastCon 2018 (pp. 1-6). IEEE.
41. Holmala, O. (2019). Designing a Protocol Agnostic Rule Engine for a Cross-Domain Solution (Master's thesis).