POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)

URL: http://dergipark.org.tr/politeknik

Security implications of underlying network technologies on industrial internet of things

Temel ağ teknolojilerinin endüstriyel nesnelerin interneti üzerindeki güvenlik etkileri

Yazar(lar) (Author(s)): *İsmail BÜTÜN*

ORCID: 0000-0002-1723-5741

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Bütün İ., "Security ımplications of underlying network technologies on ındustrial ınternet of things", ***Politeknik Dergisi***, 25(1): 223-229, (2022).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: 10.2339/politeknik.724656

Security Implications of Underlying Network Technologies on Industrial Internet of Things

Highlights

- *Industrial IoT is on the rise and expected to replace lots of wired and wireless components of industrial sites in the near future.*
- *It is projected that Intrusion Detection System (IDS) to be one of the key security components of the IIoT.*

Graphical Abstract

Industrial IoT systems security is and will be a prime concern of the network implementer and operators, as the issues and problems are not yet completely addressed and solved. Hence, this work sheds light into those mentioned topics.

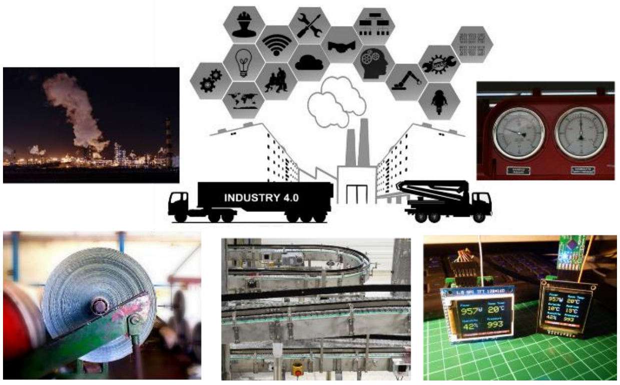


Figure An illustration of a typical Industrial IoT application.

Aim

This paper provides possible threats posed by security related vulnerabilities and stresses the importance of cyber-security measures to protect the property and life in the of Industrial IoT networks and thereby industrial facilities.

Design & Methodology

In order to increase security of Industrial IoT networks; pro-active defense mechanisms (such as hard-ware based security) or re-active defense mechanisms (such as IDS) should be employed in a coordinated and planned manner.

Originality

In this article, security implications of Industrial IoT are discussed, especially those related to the underlying network technologies; such as BACnet, LoRa, Modbus, PROFIBUS, PROFINET, WirelessHART, etc IIoT networks

Findings

It is important to mention that some of the wired industrial communication technologies, i.e. PROFIBUS, HART, and Modbus rely on closed network architecture and do not consider security as an enhanced threat for the operational safety by design.

Conclusion

Among those presented Industrial IoT enabling technologies, by possessing embedded and mandated security functions/features, LoRa and WirelessHART seems to be promising solutions in terms of security.IIoT networks

Declaration of Ethical Standards

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Security Implications of Underlying Network Technologies on Industrial Internet of Things

Araştırma Makalesi / Research Article

İsmail BÜTÜN [1 2 *]

[1]Department of Computer Engineering, Konya Food and Agriculture University, Turkey
[2]Department of Computer Engineering, Chalmers University of Technology, Sweden

(Geliş/Received : 21.04.2020 ; Kabul/Accepted : 15.12.2020 ; Erken Görünüm/Early View : 18.12.2020)

ABSTRACT

Application of Industrial Internet of Things (IIoT) network is expanding in accordance with the proliferation of Industry 4.0. As in any kind of network, security should be one of the main concerns apart from the safety of the individuals or the equipment. Yet any weaknesses in the security measures can directly affect the safety of the network components and also operators around them. Therefore, in this article security implications of IIoT are discussed, especially those related to the underlying network technologies; such as BACnet, LoRa, Modbus, PROFIBUS, PROFINET, WirelessHART, etc. Furthermore, the security implications of fog computing - IIoT integration are also evaluated and presented. Finally, future directions are provided for the researchers in the field.

Keywords: Fieldbus, HART, PROFIBUS, PROFINET, modbus, intrusion, fog, IoT, IIoT, mirai, torii, botnet.

Temel Ağ Teknolojilerinin Endüstriyel Nesnelerin İnterneti Üzerindeki Güvenlik Etkileri

ÖZ

Nesnelerin İnterneti (IIoT) ağının uygulanması, Endüstri 4.0'ın yaygınlaşmasına uygun olarak genişlemektedir. Her türlü ağda olduğu gibi, güvenlik, bireylerin veya ekipmanın güvenliği dışında ana endişelerden biri olmalıdır. Yine de güvenlik önlemlerindeki herhangi bir zayıflık, ağ bileşenlerinin ve ayrıca bunların etrafındaki operatörlerin güvenliğini doğrudan etkileyebilir. Bu nedenle, bu makalede, özellikle de altta yatan ağ teknolojileri ile ilgili olanlar olmak üzere, IIoT'nin güvenlik üzerindeki etkileri tartışılmaktadır; BACnet, LoRa, Modbus, PROFIBUS, PROFINET, WirelessHART, vs. gibi. Ayrıca, sis (fog) hesaplama - IIoT entegrasyonunun güvenlik üzerindeki etkileri de değerlendirilip ve sunulmuştur. Son olarak, alanda çalışan araştırmacılara yönelik gelecek çalışmalar önerilmiştir.

Anahtar Kelimeler: Fieldbus, HART, PROFIBUS, PROFINET, modbus, IoT, IIoT, mirai, torii, yetkisiz erişim.

1. INTRODUCTION

In technology, it is now the era of smart things, called the Internet of Things (IoT). The world is becoming more connected, as the IoT expands beyond the office and home to manufacturing at the factory floor. Smart and connected requirements of Industry 4.0 are fulfilled by the Industrial Internet of Things (IIoT) dedicated applications. For instance, IIoT can improve and improvise manufacturing as in the case of automotive sector, where Schaeffler Inc. has already started partnerships with IoT platform suppliers such as IBM's Watson, with an expectation to extend its business model to provide cognitive solutions to its products [1].

More examples of IIoT implementations and installations might include [2]:

- Optimizing maintenance in wind energy production, digitized monitoring and optimization of railway trains, connected vehicles, mechanized and robotized machine tools for Industry 4.0, connected equipment operations centers, etc.
- The factory of the future defined by Airbus Inc. is as follows: A worker on the factory floor equipped with a tablet or smart glasses/helmet assesses tasks and then sends the resulting outcome (command or sensory data) to an automated tool (robotic, AI, or similar) that finally accomplishes the task by executing the command or for instance displaying the achieved metric result.
- Caterpillar Inc. projects benefiting from vast deployment of IIoT: They want to enable their customers and vendors with the insight necessary to shift from a re-active `repair after failure' mode to a pro-active `repair before

**(Corresponding Author (Sorumlu Yazar)*
e-mail (e-posta) : ismail.butun@chalmers.se

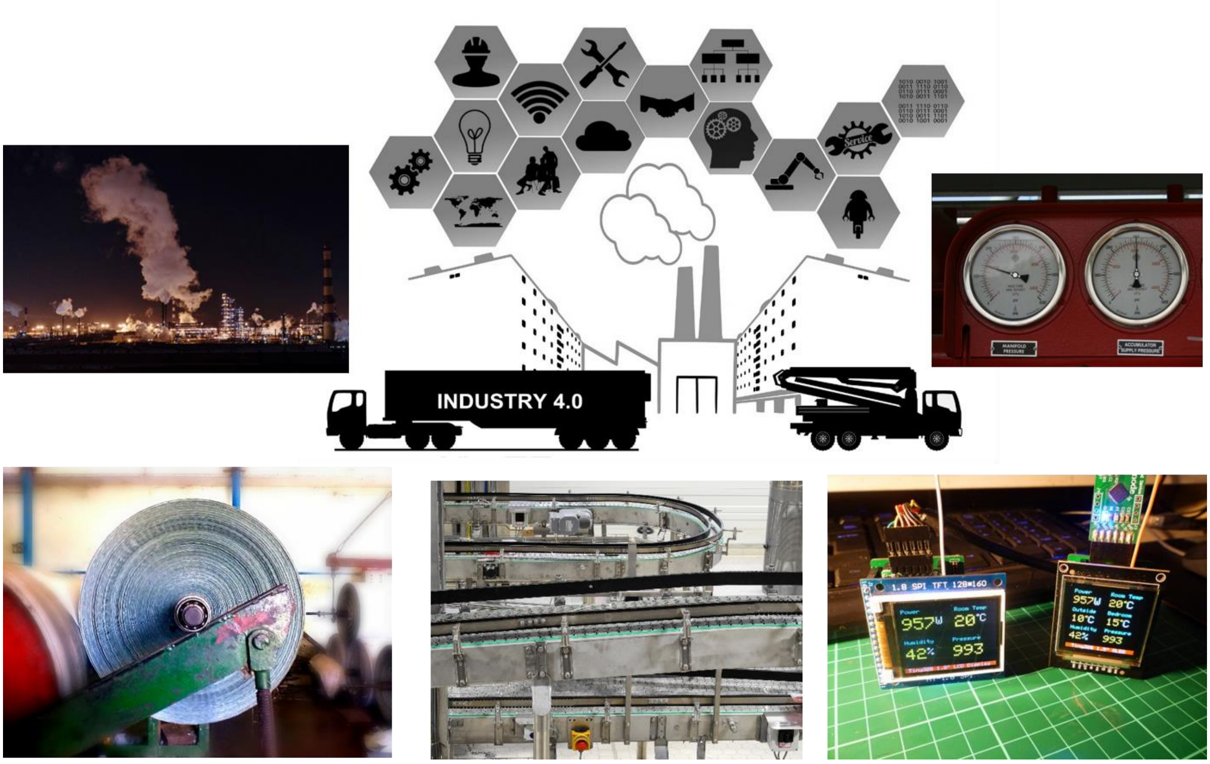


Figure 1. An example of IIoT enabled Paper Mill.

failure' stance. According to Caterpillar's projection, the outcome of this focused work on IIoT will be more efficient and automated operations, along with an increased availability of the fleets for the customers.

- As a second example to the ``factory of future", which actually follows the German government plan, is the Siemens AG's plant: The main goal is achieving a fully automated, Internet and IoT-based (remotely accessible) ``smart factory".

By using smart sensing and automation, IIoT will help increasing the energy efficiency of indoor heating/cooling systems and therefore be helpful to the nature by decreasing the greenhouse gas emissions related to energy consumption. Eventually, IIoT will hopefully have positive effect on earth by helping it to be more livable place.

IIoT is on the rise and expected to replace lots of wired/wireless components (sensors, actuators, etc.) of industrial sites in the near future. Smart factory is a very good application example on integration of IIoT to the real world industry [3]. There can be many sensors (temperature, pressure etc.), actuators or other control devices implemented and integrated to IIoT, in order to monitor and command the whole factory from single point of control (SPOC).

In a typical modern factory (for instance one that produces paper polishing material from marble dust), one can observe that several automated machinery equipment are being armed with IIoT sensor and actuators (see Figure-1 for an illustration of a paper mill).

The equipment is mainly composed of grinders, mixers, heaters, conveyor bands, etc. The installed IIoT sensors and actuators facilitate mainly three categories of functions:

1. Digitized on-the-go remote monitoring and control of equipment.
2. Optimization of machines within a production line (monthly or annual) due to collected short/long term process related data.
3. Instant alarming and shutting-down of the equipment in the case of emergency situations.

In this kind of facilities, especially heat and pressure sensors are highly critical and can be the target of the adversaries. Especially *category#1* and *category#3* can be point of interest for attackers. Any kind of outsider intervention might cause malfunctions which eventually would end-up not only with batch and/or property damage, but also casualties due to the unpreventable explosions. Hence these systems (sensors and actuators) are mostly IIoT enabled, they are hack-able and reachable by adversaries unless special cyber-security precautions are taken.

As in all industrial automation systems (such as SCADA systems), IIoT will also be required to behave highly reliable and secure. This will enable well acceptance of IIoT by the vast majority of the industrial automation and application sectors. In terms of security, CIA (confidentiality, integrity and availability) are the three upmost features desired to be assured by the systems. Therefore, IIoT will need to provide these security features to its users. One of the biggest threats against CIA is the intrusions towards the systems. A security solution needs to have an Intrusion Detection System (IDS) in order to detect and mitigate the risks pertaining to the intrusion [4]. Hence, its clear that IDS will be one of the key components in securing IIoT.

Because of introducing agile response nearby the edge components, fast implementation and business growth of fog computing is expecting for future IoT applications. Thereby, the integration of fog computing will not only remain in just IoT domain, but also expand to IIoT and further other areas. This will impose its own challenges to IIoT, as well as bringing benefits [5]. Especially, cross relations among fog computing devices and underlying IIoT network and communication protocols are the research area of interest.

The organization of this paper is as follows: Section-2 provides possible threats posed by security related vulnerabilities and stresses the importance of cyber-security measures to protect the property and life in those mentioned industrial facilities. Section-3 discusses the underlying network technologies of the IIoT, whereas Section-4 provides the security discussions associated with the previously presented protocols. Finally, Section-5 concludes the paper and Section-6 draws the future work.

2. REAL WORLD INDUSTRIAL CYBER ATTACKS

Here in this section, author presents and summarizes possible threats against industrial networks, especially to IIoT.

2.1 Stuxnet Worm

Stuxnet is a malware initially distributed over Microsoft Windows platforms. It became recognized after it targeted Iranian Nuclear centrifuges that were operating SCADA controllers on June 2010. It attacks Siemens programmable logic controllers (PLCs) step7 software through Microsoft Windows machines. Stuxnet attacked Iranian PLCs by gathering industrial systems information and initiating the fast-spinning centrifuges to tear themselves apart [6].

In the past closed-loop industrial networks (mostly Intranet or SCADA based) was considered as secure and no cyber security precaution was taken. Stuxnet proved that, even closed-loop industrial networks are susceptible to cyber attacks and rang the bell for the security experts to make them consider security all times by taking precautions for any type of network, regardless of its type of connectivity.

2.2 Mirai and Torii Botnets

Botnet attacks are increasingly targeting IoT and IIoT networks, as the end-nodes (such as IP cameras, home routers, etc.) are mostly operated with default password setting. Besides, these networks work maybe for long time periods (months or even years) in an unattended and insecure way.

Mirai and Torii Botnet attacks mainly target these weakly protected IoT end-devices by capturing them and then utilizing them to participate in higher class of attacks, such as Distributed Denial-of-Service (DDoS) attacks, against well protected systems.

2.3 RPL attacks

As a strong routing protocol candidate for IoT and IIoT environments; Routing Protocol for Low-power and lossy networks (RPL) is presented. RPL is a proactive distance vector routing protocol in which the nodes are organized in a hierarchical way to be comprised of a root, children, and descendants. RPL allows nodes to increase/decrease their ranks according to the overall state of their neighborhood.

RPL rank increase/decrease attacks can be really dangerous if the attacker manage to decrease its rank (low rank means parenting), it can lure its neighbours that it is their parents, or more drastically it can lure the whole network to act as a root node (please refer to Figure-2 to observe RPL architecture and a sample attack scenario).

RPL rank attacks might cause the network to spend more energy by causing packet drops and increases the average end-to-end delay for the packet deliveries. Therefore they need to be positively identified in a timely manner: In order to achieve this, parent-child relationship can be observed (if they are broken or not) as mentioned in Yang et al.'s work [7]. Also, Mayzaud et al.'s proposal detects this attack as follows: Each node monitors its' neighbors and keeps a counter to record the rank increases from each neighbor [8]. When a specific threshold is triggered, it is an indication of a possible ongoing rank increase attack.

2.4 Other types of attacks

There might be some other attacks towards specific protocols of the IoT, such as MQTT, 6LoWPAN, CoAP, etc. Due to the multitude of heterogeneous devices of the IoT, storing and managing the certificates along with key exchanges for every session is a real burden. Moreover, SSL and TLS suffer from attacks such as BEAST, CRIME, RC4, Heartbleed, etc. Therefore, a scalable, lightweight and robust security mechanism is required for IoT protocols (MQTT, 6LoWPAN, CoAP, etc.) [9].

2.5 Summary

It can be stated that the network security of an IIoT system should be custom tailored, according to the vulnerabilities (these can be determined according to the analysis of the IIoT System Attacks) of that specific IIoT system along with the trust metrics of the network (depending on the IIoT Cloud and device Trust) and also depending on the security requirements of the IIoT system managers and the users (privacy levels, authorization levels, access control lists, etc.). As in the case of industrial automation and control domains, the

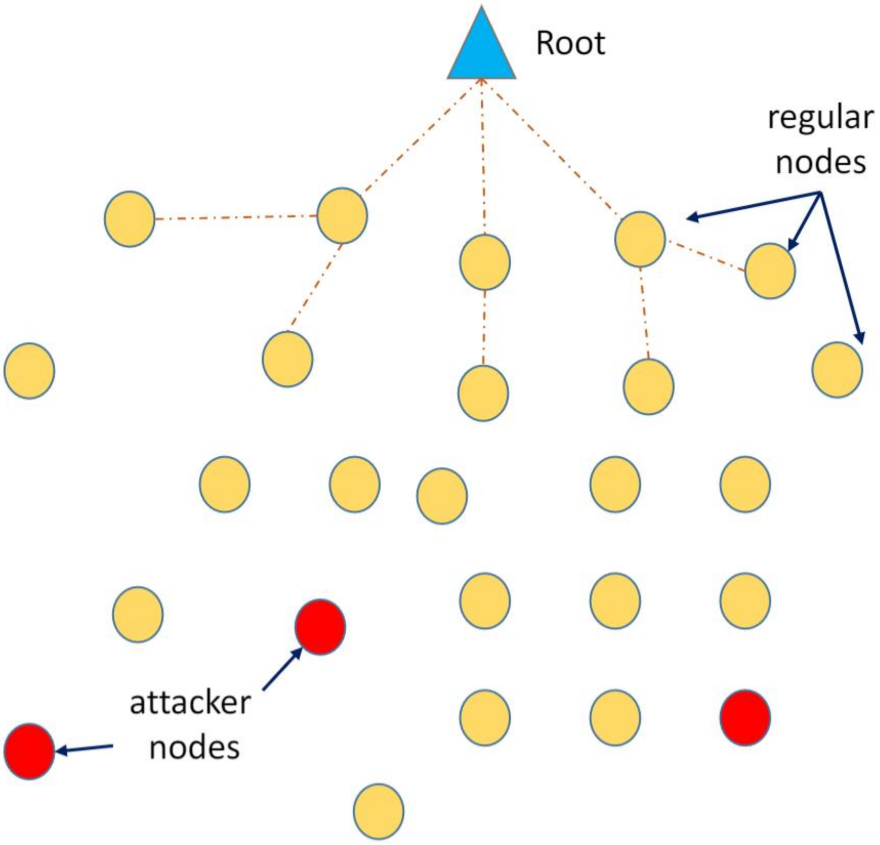


Figure 2. An overview of RPL-attack scenario against IIoT networks.

resulting security design of an IIoT system should be dynamic; security level of the design could be improved at will via updates with patch distribution or with version updates [10].

3. UNDERLYING COMMUNICATION AND NETWORK PROTOCOLS OF THE IIOT

Here in this section, IIoT are categorized according to the major underlying communication and network protocols:

3.1 BACnet

Building automation and control networks (BACnet), is an open (non-proprietary) communication protocol aimed at building automation, as the name implies [11]. It was published as ANSI standard in 1995. It allows interoperability between multiple systems from various vendors. To implement OSI, it has 4 layers of communication architecture: physical, data-link, network, and application. BACnet possess up-to-date security features, however it is not mandatory or dictated by the protocol. The implementation of the security functions is left to application developers to harmonically utilize the security features provided.

3.2 HART, WirelessHART

Highway Addressable Remote Transducer (HART) communications protocol was first proposed by Bell Labs in mid 1980s, yet one of the most deployed communication protocol for industrial environments that involve large number of end-points [11]. To implement OSI, it has 4 layers of communication architecture: physical, data-link, transport, and application. It does not have any embedded (built-in) security functions or features that can be leveraged by security experts.

WirelessHART is designed as an extension to the traditional HART protocol. It has a security level that is comparable with secure-wired solutions. Hence, it implements AES-128 algorithm along with four different settings: public, network, join, session. To implement OSI, it has five layers of communication architecture: physical, data-link, network, transport, and application.

3.3 LPWAN

As the name implies, Low Power Wide Area Network (LPWAN) can support and resume operation in a long range sense yet at the same time does not cause its components to consume energy as much as the ones in traditional WANs.

3.3.1 LoRaWAN:

LoRa is a a widely adopted technology for LPWAN which is designed to allow connectivity for connected objects (e.g. remote sensors). LoRa and its specification LoRaWAN [12] continue to grow over a number of IoT application fields such as smart cities and oil/gas operations.The v1.1 version of the LoRaWAN was a significant advance of the protocol features and addressed many previously reported security problems [13]. Especially, the latest version of LoRaWAN (v1.1) was shown to be secure against most of the known threats [14]. Security functions are provided by the protocol and mandated to the users.

LoRa is composed of three OSI layers: LoRa specifies the physical layer of the OSI protocol and LoRA-Allience specifies the data-link layer, whereas the application layer can utilize one of these protocols: UDP, OIC, NDEF, or AllJoyn.

3.3.2 NB-IoT

Narrow-band IoT (NB-IoT), also known as *Cellular-IoT*, is developed by the 3rd Generation Partnership Project (3GPP). It is an LPWAN standard which enables a wide range of cellular devices and services to be connected with each other. NB-IoT focuses especially on indoor coverage along with low cost, long battery life, and high connection density. NB-IoT uses a subset of the LTE standard, however limits the bandwidth to a single narrow-band of 200kHz. NB-IoT uses UDP protocol for its back-haul communication. To implement OSI, it has four layers of communication architecture: physical, data-link, transport, and application. NB-IoT security (authentication and encryption) is still in its maturation phase, it is optional and to be implemented by the cell phone operators [15].

3.4 Modbus

Modbus is a serial communications protocol originally published by Modicon Inc. (now it is Schneider Electric) in 1978 for use with its programmable logic controllers (PLCs). Modbus has become a preferred standard communication protocol which is openly published and royalty-free. It is now a commonly available means of connecting industrial electronic devices [17]. To implement OSI, it has 5 layers of communication architecture: physical, data-link, network, transport, and application. Modbus protocol itself also does not provide any security against unauthorized commands or interception of the data [18].

3.5 PROFIBUS and PROFINET

PROFIBUS is an open, digital communication protocol with wide range of applications from distributed automation to manufacturing industry [11]. To implement OSI, it has 3 layers of communication architecture: physical, data-link, and application. Neither a dedicated function nor a feature set exists for the security of PROFIBUS.

PROFINET is the open standard for industrial Ethernet and covers PROFIBUS. PROFINET is a version of PROFIBUS that is fully compatible with the Ethernet according to IEEE standards [11]. Security is optional in PROFINET and provided to secluded automation cells by PROFINET *security module*. This module allows only uniquely identified and authorized messages to be transmitted to the secluded automation cell.

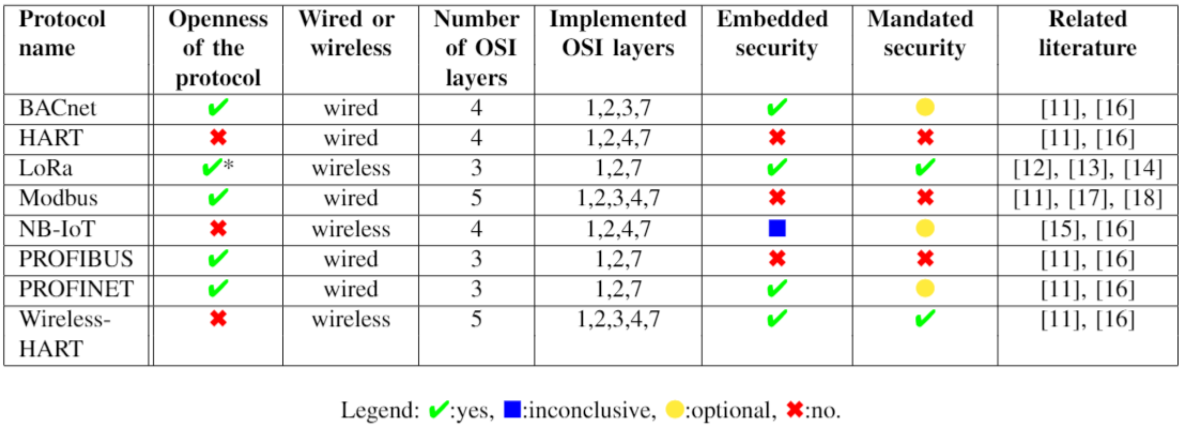
4. SECURITY DISCUSSIONS

4.1 Security Analysis of Existing IIoT Technologies

Table-1 provides the comparison of the IIoT communication and network protocols from the security point of view:

- In Table-1, the column with ``Openness", mentions whether the protocol is proprietary or not. It can be deduced that open protocols can be more secure, as more researchers can work in that manner with a combined effort.
- The column with ``Wired/wireless" stresses whether the associated technology communicates via wired or wireless. Wired solutions are susceptible to wire taping attacks, whereas wireless ones suffer from interference, jamming and also eavesdropping.
- The column with ``Number of OSI layers" declares how many of the OSI layers, whereas ``Implemented OSI layers" column states which are implemented by the corresponding technology.
- The ``Embedded Security" column states whether security functions and/or features are provided, whereas the ``Mandated Security" column shows whether those embedded security functions are mandatory for the relevant technology. Here, it is important to mention that some of the wired communication technologies, i.e. PROFIBUS, HART, and Modbus rely on closed network architecture and do not consider security as an enhanced threat for the operational safety by design. Therefore, by

Table 1. Comparison of the IIoT Communication and Network Protocols from the Security Point of View.



Protocol name	Openness of the protocol	Wired or wireless	Number of OSI layers	Implemented OSI layers	Embedded security	Mandated security	Related literature
BACnet	✔	wired	4	1,2,3,7	✔	●	[11], [16]
HART	✖	wired	4	1,2,4,7	✖	✖	[11], [16]
LoRa	✔*	wireless	3	1,2,7	✔	✔	[12], [13], [14]
Modbus	✔	wired	5	1,2,3,4,7	✖	✖	[11], [17], [18]
NB-IoT	✖	wireless	4	1,2,4,7	■	●	[15], [16]
PROFIBUS	✔	wired	3	1,2,7	✖	✖	[11], [16]
PROFINET	✔	wired	3	1,2,7	✔	●	[11], [16]
Wireless-HART	✖	wireless	5	1,2,3,4,7	✔	✔	[11], [16]

Legend: ✔:yes, ■:inconclusive, ●:optional, ✖:no.

OSI layers mentioned in the table are as follows:
Layer-1 stands for physical, 2 for MAC, 3 for network, 4 for transport,
5 for session, 6 for presentation, and finally, 7 for application layer.
** The physical layer of the LoRa protocol is proprietary (designed by Semtech Inc. [19]),*
however, upper layers are available to public by the LoRa-Alliance [20].

default, they do not provide any embedded or mandated security functions/features.

- Finally, the ``Related literature'' column forwards the readers to the associated references from the literature.

4.2 Cyber-Security Defense Considerations on the Industrial IoT

In order to secure IIoT networks, 2-types of defense strategy can be followed:

- Pro-active defense: It includes taking cyber-security measures before they happen which can be also considered as `Intrusion Prevention'. Some examples might be, hardware-based cyber-security solutions, such as Hardware Security Module (HSM), Physically Unclonable Function (PUF), System on a Chip (SoC), and Tamper Resistant Memory (TRM) [21]. Installment of these hardware-based intrusion prevention mechanism might help improvement of the overall security of the IIoT networks and increase the public trust on them which would enhance their acceptance by the industrial community.
- Re-active defense: It includes taking cyber-security measures after they happen which can be also considered as `Intrusion Detection'. Some examples might be, Intrusion Detection Systems (IDS) that are based on *Evolutionary Computing*, on the *Data-streaming*, or *Adaptive and Continuous Monitoring* [22, 23, 24].

5. CONCLUSIONS

IIoT systems security is and will be a prime concern of the network implementer and operators, as the issues and problems are not yet completely addressed and solved. Among those presented IIoT enabling technologies, by possessing embedded and mandated security functions/features, LoRa and WirelessHART seems to be promising solutions in terms of security.

According to the prediction of the author, wireless IIoT solutions will mostly inherit RPL as their routing protocol in the near future. In order to protect RPL-based IIoT networks, an IDS can be implemented and run on the root node to thwart attacks. Especially, attacks towards routing table formations (e.g. RPL attacks such as RPL Rank Attacks) can be seamlessly detected and mitigated at the root node.

As mentioned thoroughly in this text, in order to increase security of IoT and IIoT protocols; pro-active defense mechanisms such as hardware-based security or light-weight cryptography solutions; or re-active defense mechanisms such as evolutionary-based, data-streaming-based intrusion detection systems should be employed in a coordinated and planned manner.

6. FUTURE WORK

In the near future, fog computing might be a preferred approach for diverse IoT applications such as smart grid, smart home, intelligent transportation systems, IIoT and industrial automation, smart health-care systems, etc. Fog computing as a Service (FaaS) might be provided to IIoT users as a sub component of cloud-based services in the near future, other than the three major services currently offered, namely Infrastructure as a Service

(IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [5]. Hence, integration of Faas with IIoT network and communication protocols will expose several security issues. Addressing these will be a challenging task and open research area.

It is also projected that IDSs [4] to be one of the key security components of the IIoT; hence they provide early warning related to real incidences happening and can buy time for the security teams to react against intrusions on-time.

As a future work, author plans to expand the comparative analysis provided in Table-1 by including not only more comparison metrics, but also more relevant network and communication technologies proposed for IIoT/industrial-networks. Author will also explore the security issues that will be exposed by the fog computing - IIoT integration.

DECLARATION OF ETHICAL STANDARDS

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

AUTHORS' CONTRIBUTIONS

İsmail BÜTÜN: Performed the experiments, analyzed the results and written the manuscript.

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] Laros, S., "5 Examples of How the Industrial Internet of Things is Changing Manufacturing," available online: ***https://www.engineering.com/AdvancedManufacturing/ArticleID/13321***, (2016).

[2] Roberts, F., "9 examples of manufacturers making IIoTwork for them," available online: ***https://internetofbusiness.com/9-examples-manufacturers-iiot/***, (2016).

[3] Forsstrom S., Butun I., Eldefrawy M., Jennehag U. and Gidlund M., "Challenges of securing the industrial internet ofthings value chain," in ***IEEE Workshop on Metrology for Industry4.0 and IoT***, pp. 218–223, (2018).

[4] Butun I., Morgera S. D. and Sankar R., "A survey of in-trusion detection systems in wireless sensor networks," ***IEEE Communications Surveys & Tutorials***, vol. 16, no. 1, pp. 266–282, (2014).

[5] Butun I., Sari A. and Osterberg P., "Security implicationsof fog computing on the internet of things," ***in IEEE International Conference on Consumer Electronics (ICCE)***, pp. 1–6, (2019).

[6] Karnouskos S., "Stuxnet worm impact on industrial cyber-physical system security***," in IECON 37th Annual Conference on IEEE Industrial Electronics Society***, pp. 4490–4494, (2011).

[7] Yang W., Wang Q., Wan Y. and He J., "Security vulnerabili-ties and countermeasures for time synchronization in ieee802.15.4 e networks," in ***IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)***, pp. 102–107, (2016).

[8] Mayzaud A., Sehgal A., Badonnel R., Chrisment I. and Schonwalder J., "A study of rpl dodag version attacks," in ***Springer IFIP international conference on autonomous infrastructure, management and security***, pp. 92–104, (2014).

[9] Singh M., Rajan M., Shivraj V. and Balamuralidhar P. , "Secure mqtt for internet of things (iot)," in ***IEEE Fifth International Conference on Communication Systems and Network Technologies***, pp. 746–751, (2015).

[10] Al F., Dalloro L., Ludwig H., Claus J., Frohlich R. and Butun I., "Networking elements as a patch distribution platform fordistributed automation and control domains," ***U.S. patent App.***, PCT/US2012/043,084., Dec. 27, (2012).

[11] Zurawski R., "Industrial communication technology handbook", ***CRC Press***, 2nd Edition, (2015).

[12] Lora Alliance, "LoRaWAN 1.1 Specification.", available online: ***http://lora-alliance.org/lorawan-for-developers***, (2020).

[13] Butun I., Pereira N. and Gidlund M., "Analysis of lorawan v1.1 security," in ***Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects***, p. 5, (2018).

[14] Butun I., Pereira N. and Gidlund M., "Security risk analysis of lorawan and future directions," ***MDPI Future Internet***, vol. 11, no. 1, p. 3, (2019).

[15] O. Patau. "Security of nb-iot devices," available online: ***https://accent-systems.com/blog/security-of-nb-iot-devices/***, (2018).

[16] A. Sari, A. Lekidis, and I. Butun, "Industrial Networks and IIoT: Now and Future Trends," in ***Industrial IoT by Springer***, pp. 3–55, (2020).

[17] B. Drury, "Control techniques drives and controls handbook," by ***IET***, 2nd Edition, no. 35, (2009).

[18] Lewis T. G., "Critical infrastructure protection in homeland security: defending a networked nation," by ***John Wiley & Sons***, (2014).

[19] "What is LoRa?," available online: ***https://www.semtech.com/lora***, (2020).

[20] "LoRaAlliance," available online: ***http://lora-alliance.org***, (2020).

[21] Butun I., Sari A. and Osterberg P., "Hardware Security of Fog End-Devices for the Internet of Things," ***MDPI Sensors***, vol. 20, no. 20, p. 5729, (2020).

[22] Aydogan E., Yilmaz S., Sen S., Butun I., Forsstrom S. and Gidlund M., "A Central Intrusion Detection System for RPL-Based Industrial Internet of Things," in ***15th IEEE International Workshop on Factory Communication Systems (WFCS)***, pp. 1–5, (2019).

[23] Butun I., Almgren M., Gulisano V. and Papatriantafilou M., "Intrusion Detection in Industrial Networks via Data Streaming," in ***Industrial IoT by Springer***, pp. 213–238, (2020).

[24] Butun I., dos Santos D., Lekidis A. and Papatriantafilou M., "Adaptive and Continuous Intrusion and Anomaly Detection for Smart Grid Systems," (2020).