POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

A new approach in cyber security of industrial control systems: Li-Fi

Endüstriyel kontrol sistemlerinin siber güvenliğinde yeni bir yaklaşım: Li-Fi

***Yazar(lar) (Author(s))**: Serkan GÖNEN[1], Hasan Hüseyin SAYAN[2], Gökçe KARACAYILMAZ[3], Erhan SİNDİREN[4], Furkan ÜSTÜNSOY[5], Harun ARTUNER[6], Ercan Nurcan YILMAZ[7], Mehmet Fatih IŞIK[8]*

ORCID[1]: 0000-0002-1417-4461

ORCID[2]: 0000-0002-0692-172X

ORCID[3]: 0000-0001-8529-1721

ORCID[4]: 0000-0003-1138-1913

ORCID[5]: 0000-0003-3087-895X

ORCID[6]: 0000-0002-6044-379X

ORCID[7]: 0000-0001-9859-1600

ORCID[8]: 0000-0003-3064-7131

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Gönen S., Sayan H. H., Karacayılmaz G., Sindiren E., Üstünsoy F., Artuner H. Ve Yılmaz E. N., Işık M. F., "A new approach in cyber security of ındustrial control systems: Li-Fi", ***Politeknik Dergisi***, 25(2): 895-902, (2022).

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

DOI: **10.2339/politeknik.976886**

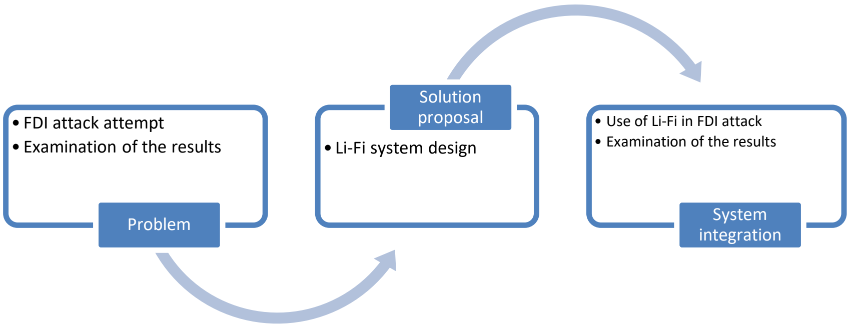
A New Approach in Cyber Security of Industrial Control Systems: Li-Fi

Highlights

- *The usability of the Light Fidelity (Li-Fi) transmission infrastructure*
- *Li-Fi usage areas, advantages, disadvantages and misconceptions*
- *A new solutıon approach to FDI attack: Li-Fi*

Graphical Abstract

In the study, first of all, False Data Injection attack was carried out against the smart city/network infrastructure in order to draw attention to the cyber security vulnerability caused by ICS compliance with technological developments, and it was observed that the memory values of the controller could change as a result of the attack. Subsequently, the usability of Li-Fi (Light Fidelity) transmission technology in industrial control systems has been proposed as a solution against such privacy and integrity attacks (such as data disclosure, FDI and eavesdropping).



• FDI attack attempt
• Examination of the results
Problem
Solution proposal
• Li-Fi system design
• Use of Li-Fi in FDI attack
• Examination of the results
System integration

Figure A. Graphical Abstract

Aim

A new solution proposal against FDI attacks.

Design & Methodology

A virtual test system has been implemented. Then, attacks have been carried out on this test system and the results were examined. Afterwards, its success against FDI attacks was examined by integrating Li-Fi into the system.

Originality

Li-Fi system is currently used in many applications. However, we examined the contribution of this system to cyber security in Industrial Control Systems (ICS).

Findings

Using the Li-Fi transmission environment in ICS will provide considerable convenience in network forensics in the investigation of the event as a result of any attack.

Conclusion

It has been evaluated that this study will enlighten on the use of Li-Fi in ICS and other studies on ICS security and will make important contributions.

Declaration of Ethical Standards

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

A New Approach in Cyber Security of Industrial Control Systems: Li-Fi

Araştırma Makalesi / Research Article

Serkan GÖNEN[1*], Hasan Hüseyin SAYAN[2], Gökçe KARACAYILMAZ[3], Erhan SİNDİREN[4], Furkan ÜSTÜNSOY[2], Harun ARTUNER[3], Ercan Nurcan YILMAZ[5], Mehmet Fatih IŞIK[6]

[1] Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey
[2]Electrical and Electronics Engineering, Faculty of Technology, Gazi University, Ankara, Turkey
[3]Forensic Sciences, Hacettepe University, Ankara, Turkey
[4]Information Security Engineering, Graduate School of Natural and Applied Sciences, Gazi University, Ankara, Turkey
[5] Faculty of Engineering, Mingachevir State University, Mingachevir, Azerbaijan
[6]Electrical and Electronics Engineering, Faculty of Engineering,Hitit University, Çorum, Turkey

(Geliş/Received : 31.07.2021 ; Kabul/Accepted : 20.10.2021 ; Erken Görünüm/Early View : 01.11.2021)

ABSTRACT

Industrial Control Systems used in the control of critical infrastructures, especially in smart grids, have made a rapid transition from an isolated network architecture to wired and wireless external networks due to the factors that facilitate human life such as productivity, economy and speed. With this transition, industrial control systems specific protocols have become insufficient and hybrid protocols have started to be used. As a result, the vulnerabilities specific to the internet and new protocols besides the vulnerabilities specific to industrial control systems have started to threaten control systems. In this study, the usability of the Light Fidelity (Li-Fi) transmission infrastructure in data transmission was investigated as a solution proposal for the smart city / network infrastructure where attack of False Data Injection carried out. This study will make important contributions to the studies carried out for industrial control systems security.

Keywords: Li-Fi, ICS cyber security, ICS forensics, false data injection, wireless network.

Endüstriyel Kontrol Sistemlerinin Siber Güvenliğinde Yeni Bir Yaklaşım: Li-Fi

ÖZ

Özellikle akıllı şebekelerde kritik altyapıların kontrolünde kullanılan Endüstriyel Kontrol Sistemleri, üretkenlik, ekonomi ve hız gibi insan hayatını kolaylaştıran faktörler nedeniyle izole bir ağ mimarisinden kablolu ve kablosuz dış ağlara hızlı bir geçiş yapmıştır. Bu geçişle birlikte endüstriyel kontrol sistemlerine özgü protokoller yetersiz kalmış ve hibrit protokoller kullanılmaya başlanmıştır. Sonuç olarak, endüstriyel kontrol sistemlerine özgü zafiyetlerin yanı sıra internete ve yeni protokoller özgü zafiyetler, kontrol sistemlerini tehdit etmeye başlamıştır. Bu çalışmada, sahte veri enjeksiyonu saldırısının gerçekleştirildiği akıllı şehirler ve ağ altyapıları için çözüm önerisi olarak ışık bağlantısı (Li-Fi) iletim altyapısının veri iletiminde kullanılabilirliği araştırılmıştır. Bu çalışmanın, endüstriyel kontrol sistemleri güvenliği kapsamında diğer çalışmalara önemli katkılar sağlayacağı düşünülmektedir.

Anahtar Kelimeler: Li-Fi, EKS siber güvenliği, EKS adli analizi, sahve veri enjeksiyonu, kablusoz ağ.

1. INTRODUCTION

When the existing Industrial Control Systems (ICS) communication infrastructure used in the management of smart city / networks is evaluated, it has transformed from an isolated independent network structure to an external network open with the requirements of the digitalization era [1]. With this transition, ICS-specific protocols have become insufficient and hybrid protocols (TCP / IP-Modbus, etc.) have started to be used. As a result, the vulnerabilities specific to the internet and new protocols besides the vulnerabilities specific to ICS have started to threaten control systems. Among these attacks, there are ICS-derived attacks such as Start / Stop [2] and False Data Injection (FDI) [3, 4] as well as the attacks frequently encountered in commercial networks such as DoS / DDoS and MitM [5].

In the study, firstly, in order to draw attention to the cybersecurity vulnerability resulting from ICS compliance with technological developments, it was observed that the memory values of the controller could be changed as a result of the FDI attack against the smart city / network infrastructure. Subsequently, Li-Fi (Light Fidelity) transmission technology has been proposed as a solution against privacy and integrity attacks (such as data disclosure, FDI and eavesdropping). Hence, data from field equipment to MTU (Master Terminal Unit) and from there to HMI (Human Machine Interface) is transferred via Li-Fi. As this stage is the most critical stage in which information received by MTU is processed and transmitted to HMI, it contains the most valuable information assets of ICS. In this process, the

**Sorumlu Yazar (Corresponding Author)*
e-posta : sgonen@gelisim.edu.tr

confidentiality, integrity and accessibility components of the data were protected by Li-F.

2. LI-FI TECHNOLOGY

The rise of the IoT and the widespread usage of mobile devices have increased the need for wireless communication exponentially. Within the scope of this need, Li-Fi technology, which is the use of light as a new mobile communication infrastructure, stands out with its innovations and usage areas. Li-Fi uses a visible spectrum light from 400 THz to 800 THz. It is a more economical and more durable and efficient technology than Wireless Fidelity (Wi-Fi). It is a technology that can send data about 100 times faster than Wi-Fi, at the terabit rate per second, using visible light instead of radio waves [6]. Li-Fi uses IEEE 802.15.7 with Optical Wireless Communication Protocols (OWC). The Li-Fi system refers modulation schemes such as OOK, VPPM, CSK [7]. Li-Fi system is used in many areas such as street lights and public internet access, autopilot vehicles communicating with running lights. Furthermore, Li-Fi is an alternative that may ensure faster data access rates in fields such as medical applications, underwater applications, aircraft, and disaster management where Wi-Fi is mostly inadequate or inconvenient to use. Li-Fi is a technology designed especially for interiors rather than outdoors. Thus, it can be applied in ICSs located in places such as a high critical nuclear facility or in military and mobile systems that require high security. It also reduces the possibility of the system being attacked [8].

Table 1. Li-Fi usage areas, advantages, disadvantages and misconceptions

Usage Areas	*Generic usage areas*	Li-Fi has the advantage of being useful in electromagnetic sensitive areas such as aircraft cabinets, hospitals and nuclear power plants without causing electromagnetic interference. Both Wi-Fi and Li-Fi transmit data over the electromagnetic spectrum, but when Wi-Fi uses radio waves, Li-Fi uses visible, ultraviolet and infrared light [9]. Most data consumption occurs indoors and increasingly in areas such as aircraft and other vehicles. This high demand for video and cloud-based data is expected to increase and is a strong driving force for the adoption of the new spectrum, including the use of optical wireless media.
	Education system	Li-Fi can replace Wi-Fi in educational institutions and provide faster internet speeds.
	Medical applications	Wi-Fi is not allowed in operating theaters because they can interfere with medical equipment. Moreover, their radiation poses a risk to patients. Li-Fi uses light and therefore it can be used instead of Wi-Fi.
	Internet access on airplanes	Using Wi-Fi is prohibited on airplanes, as they can interfere with cruising on airplanes. That's why Li-Fi is a safe alternative to Wi-Fi on airplanes because it uses light and can provide faster internet access.
	Underwater applications	Underwater ROVs (Remote Operated Vehicles) work through large cables that provide their power and get signals from their pilots in the water. However, the cable used in ROVs is not long enough to allow them to explore larger areas. If the cables were replaced by light, then the discoveries would be more free, thanks to a high-power lamp immersed in water. They can also use their headlights to communicate with each other, process data independently and periodically send their findings back to the surface. Li-Fi can work underwater where Wi-Fi is completely unsuccessful, thus providing clear and plain opportunities for military operations.
	Radio broadcasting	Broadcasting by radio masts requires a lot of power, which makes them inefficient. On the other hand, very low power is required for the LEDs to work. Therefore, it can be preferred in radio broadcasting [10].
Advantages	*Security*	It is the high physical access security that Li-Fi systems provide advantage over RF systems. Basically, this advantage stems from the inability of light to penetrate through the walls [11]. Because visible light does not enter through the walls. This contributes significantly to preventing unauthorized access of the free signal by unauthorized person. Li-Fi is working in point to point base while Wi-Fi multi-point is working. Additionally, since it supports the Li-Fi IEEE 802.1X standard, it assists authentication methods thanks to authorized user control [12]. Although it is a closed environment, it is possible for the signal to pass to the outside environment by reflecting from spaces such as windows or glass surfaces [13, 14]. Another weakness to be considered is the capture and interpretation of transmitted data by unauthorized persons within the institution, which is described as an insider.
	Data transfer speed	The data rate of Li-Fi is 100 times faster than Wi-Fi, and internet browsing, such as uploading and downloading, takes place within a few seconds [15]. It provides the theoretical speed of a gigabyte in a second.
	Efficiency	Li-Fi devices consume low power for operation and therefore can be used effectively in IoT applications. It saves a lot of energy in the lighting industry using Li-Fi-based devices. In addition, components such as LED lamps and photodetectors are easier to find than the Wi-Fi router [16, 17].
	Capacity	While the U.S. Federal Communications Commission warned against a potential spectrum crisis because Wi-Fi is close to full capacity, Li-Fi has virtually no limitation on capacity. Because the Visible light spectrum is 10,000 times larger than the entire radio frequency spectrum. It also takes advantage of the free band that doesn't need any licensing [18].

	Health	Unlike RF spectrum, it works on non-harmful optical bands. Therefore, there is no health concern in the Li-Fi based system. Light is actually a source of life and practically has no side effects. Thus, Li-Fi proves to be the most advanced technology without any pollution or damage. The operating theaters do not allow Wi-Fi due to radiation concerns, and there is also a lack of a dedicated spectrum. Due to Wi-Fi interference from mobile phones and computers, it causes blocking of signals from monitoring equipment. Li-Fi solves both problems. Wi-Fi and many other types of radiation are not preferred for sensitive areas such as power plants. Li-Fi can offer a safe (since there is no radiation) connection for these sensitive places. This will not only save economically from existing power plant designs, but the reduction in a power plant's own reserve can be reduced [19].

Table 1. Li-Fi usage areas, advantages, disadvantages and misconceptions **(**cont.**)**

Disadvantages	*Security*	If used outdoors, it can be captured by undesired people.
	Availability	The internet can only be used where the source device has light. Internet access may be interrupted if the light source fails. This can limit access to the internet wherever someone needs it. Although there are new studies, its range is limited. When the device is installed outdoors, changing weather conditions must be taken into account. The coverage is very limited, just 10 meters, while Wi-Fi coverage is approximately 32 meters. Due to the interference of external sources such as sunlight, its reliability may decrease [20].
	Cost	Although the installation is simple, the Li-Fi system needs a completely new infrastructure. This will add cost to companies / people who want to get the Li-Fi internet service.

	Claim	*Answer*	*Truth*
Misconceptions	The lights cannot be dimmed	No	Like as eU-OFDM, there are advanced modulation techniques that enable the Li-Fi to operate close to the LED's on voltage (ToV), which signifies the lights can be operated at very low light output levels while preserving high data.
	Lights flicker	No	The lowest frequency at which the lights are modulated is in the 1 MHz region. The refresh rate of the computer screen is about 100 Hz. This signifies that the vibration speed of a Li-Fi led is higher than the vibration speed of a computer screen. Therefore, there is no noticed vibration.
	This is for downlink only	No	An important advantage is that Li-Fi can be combined with LED lighting. However, this does not signify that both functions should always be used together. Both functions can be easily detached [21].

3. LI-FI ASSESSMENT IN TEST ENVIRONMENT NETWORK

The projected system architecture and recommended Li-Fi system infrastructure to prevent the attack are depicted in Figure 1. The intelligent measuring layer is the layer where energy consumption and network data of each electrical consumer is measured and sent to the distribution transformer that transfers energy to the building with the industrial RF-Module. The layer where the data of each subscriber fed by the distribution transformer is collected and energy management is Remote Terminal Unit (RTU) layer. In fact, every distribution transformer is like an intermediate station designed as RTU. The MTU layer is the layer where the data received from the RTU layers with the GPS module is processed and all energy management is performed. This layer covers many functions such as data storage and remote control and invoice tracking over the web. The part where the measurement data is taken and processed from energy transmission lines and power plants is named as the network measurement layer.

The data measured for the consumer in the test environment designed in the laboratory were transferred to the central unit using the Modbus communication protocol and wireless connection. An FDI cyber-attack was carried out on the central controller by an insider on the premises as depicted in Figure 2. As a result of the attack, the attacker changed the memory values of the controller.

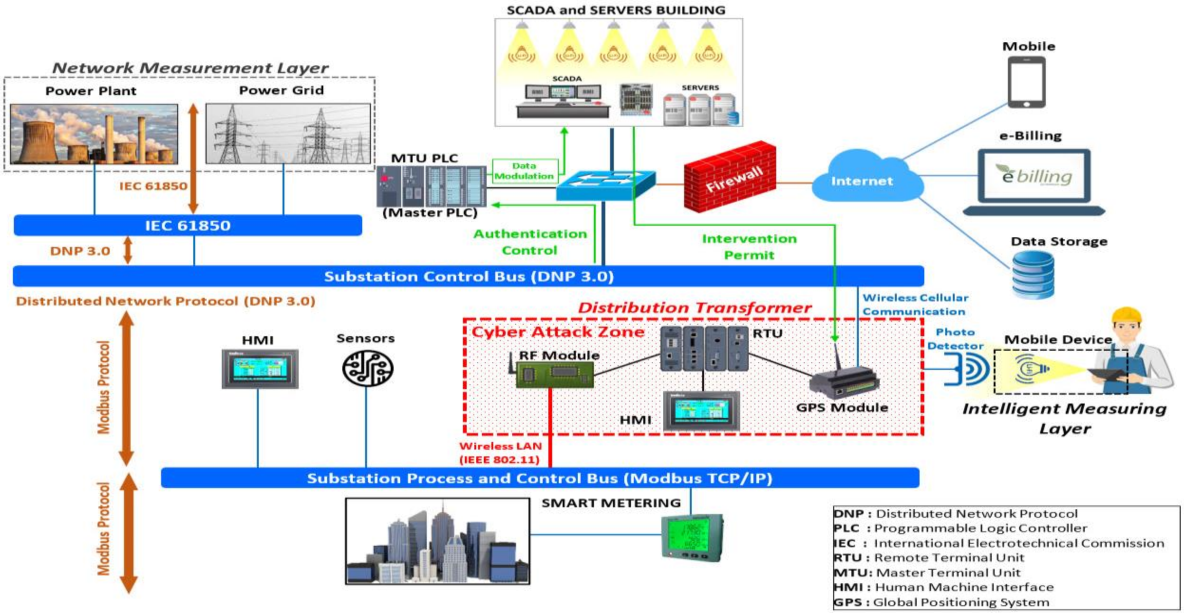

SCADA and SERVERS BUILDING
SCADA
SERVERS
Mobile
e-Billing
e billing
Data Storage
Internet
Firewall
Network Measurement Layer
Power Plant
Power Grid
IEC 61850
IEC 61850
DNP 3.0
MTU PLC
(Master PLC)
Data Modulation
Authentication Control
Intervention Permit
Substation Control Bus (DNP 3.0)
Distributed Network Protocol (DNP 3.0)
Wireless Cellular Communication
Distribution Transformer
Cyber Attack Zone
RF Module
RTU
HMI
GPS Module
HMI
Sensors
Photo Detector
Mobile Device
Intelligent Measuring Layer
Modbus Protocol
Wireless LAN (IEEE 802.11)
Substation Process and Control Bus (Modbus TCP/IP)
SMART METERING
Modbus Protocol
DNP : Distributed Network Protocol
PLC : Programmable Logic Controller
IEC : International Electrotechnical Commission
RTU : Remote Terminal Unit
MTU : Master Terminal Unit
HMI : Human Machine Interface
GPS : Global Positioning System

Figure 1. Projected system architecture and Li-Fi communication line

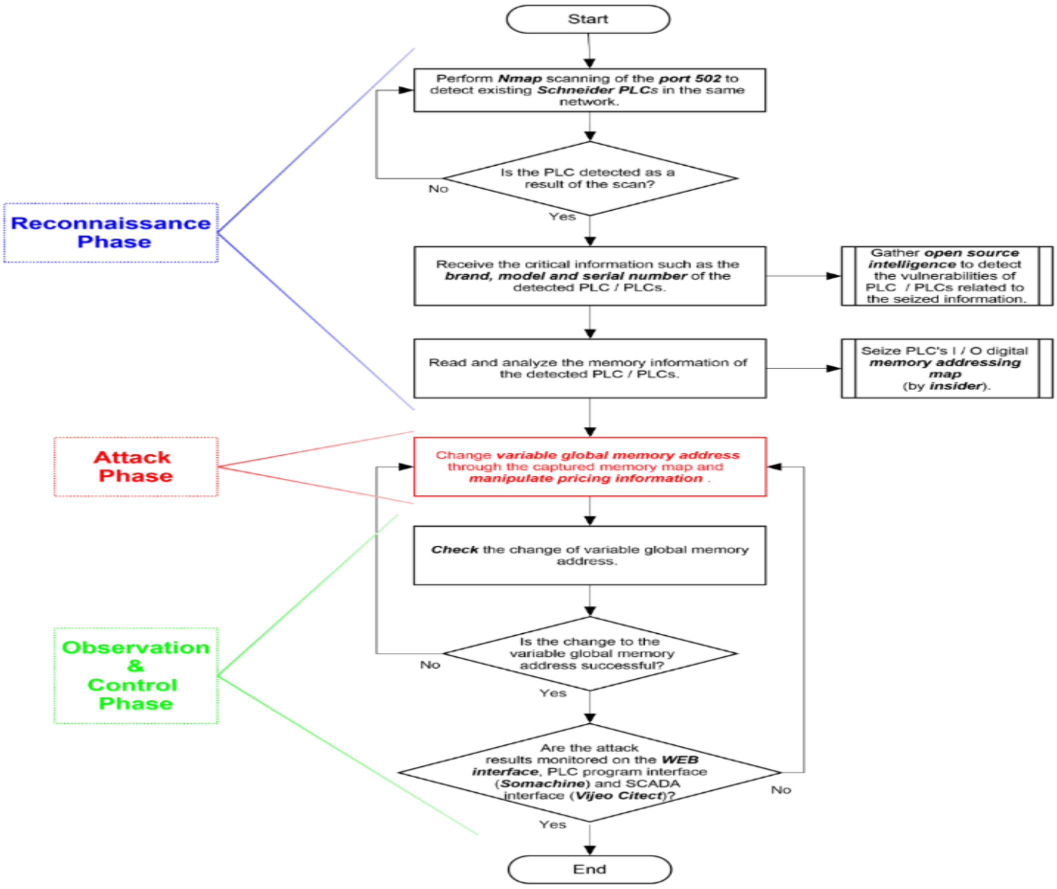
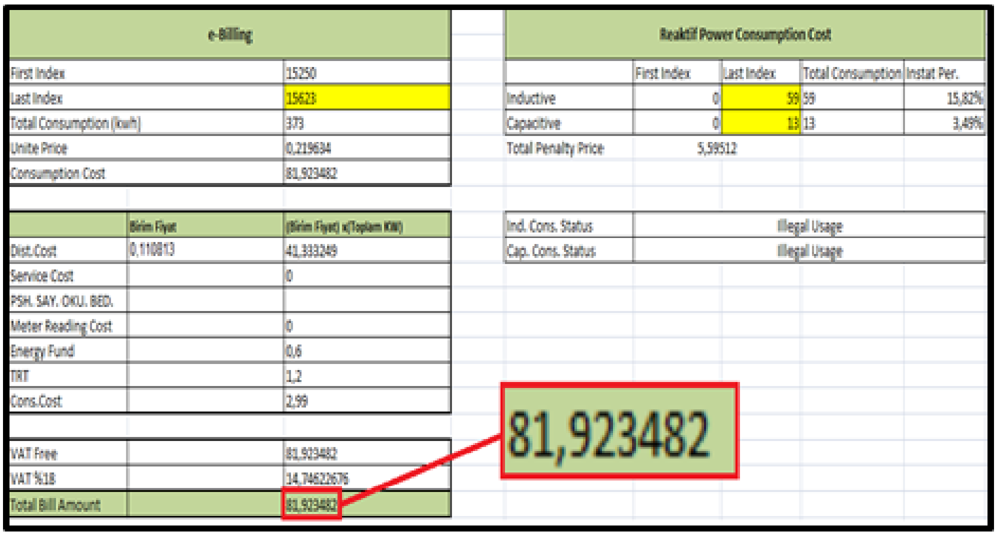

Start
Perform Nmap scanning of the port 502 to detect existing Schneider PLCs in the same network.
Is the PLC detected as a result of the scan?
No
Yes
Reconnaissance Phase
Receive the critical information such as the brand, model and serial number of the detected PLC / PLCs.
Gather open source intelligence to detect the vulnerabilities of PLC / PLCs related to the seized information.
Read and analyze the memory information of the detected PLC / PLCs.
Seize PLC's I / O digital memory addressing map (by insider).
Attack Phase
Change variable global memory address through the captured memory map and manipulate pricing information .
Check the change of variable global memory address.
Observation & Control Phase
Is the change to the variable global memory address successful?
No
Yes
Are the attack results monitored on the WEB interface, PLC program interface (Somachine) and SCADA interface (Vijeo Citect)?
No
Yes
End

Figure 2. FDI attack steps carried out on central controller

Situations when access privileges on systems are not controlled can result in critical information leaks [22]. It has been seen that if the insider captures the addressing map, critical memory values can be changed. The change in consumption value resulting from the attack is given in Figure 3, and invoice details created in real time with the Total Billing button on the SCADA screen are given in Figure 4.



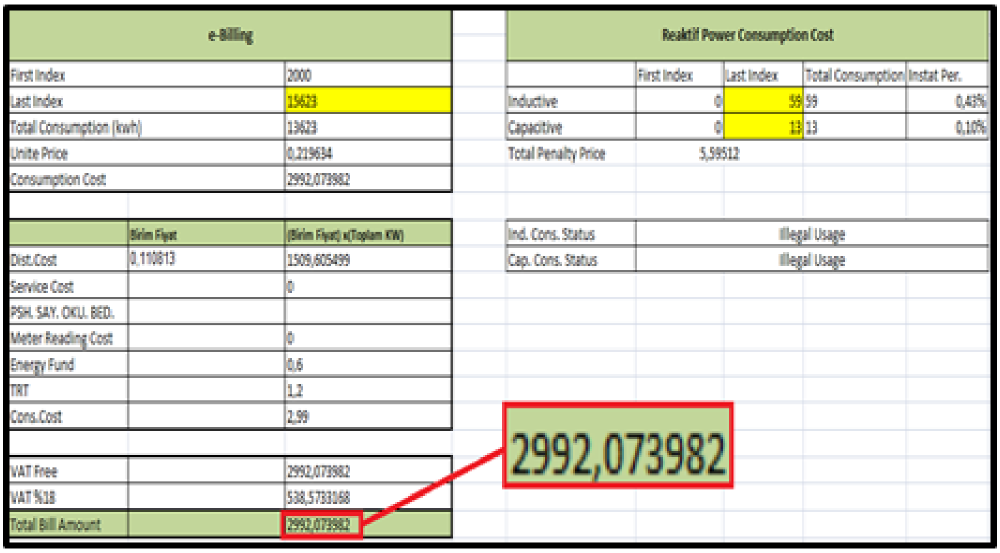
e-Billing		
First Index		15250
Last Index		15623
Total Consumption (kwh)		373
Unite Price		0,219634
Consumption Cost		81,923482
	Birim Fiyat	(Birim Fiyat) x(Toplam KW)
Dist.Cost	0,110813	41,333249
Service Cost		0
PSH. SAY. OKU. BED.		
Meter Reading Cost		0
Energy Fund		0,6
TRT		1,2
Cons.Cost		2,99
VAT Free		81,923482
VAT %18		14,74622676
Total Bill Amount		81,923482

Reaktif Power Consumption Cost				
	First Index	Last Index	Total Consumption	Instat Per.
Inductive	0	59	59	15,82%
Capacitive	0	13	13	3,49%
Total Penalty Price	5,59512			

Ind. Cons. Status	Illegal Usage
Cap. Cons. Status	Illegal Usage

81,923482

Figure 3. An example SCADA invoice detail actual value



e-Billing		
First Index		2000
Last Index		15623
Total Consumption (kwh)		13623
Unite Price		0,219634
Consumption Cost		2992,073982
	Birim Fiyat	(Birim Fiyat) x(Toplam KW)
Dist.Cost	0,110813	1509,605499
Service Cost		0
PSH. SAY. OKU. BED.		
Meter Reading Cost		0
Energy Fund		0,6
TRT		1,2
Cons.Cost		2,99
VAT Free		2992,073982
VAT %18		538,5733168
Total Bill Amount		2992,073982

Reaktif Power Consumption Cost				
	First Index	Last Index	Total Consumption	Instat Per.
Inductive	0	59	59	0,43%
Capacitive	0	13	13	0,10%
Total Penalty Price	5,59512			

Ind. Cons. Status	Illegal Usage
Cap. Cons. Status	Illegal Usage

2992,073982

Figure 4. Attack result an example SCADA invoice detail

4. A NEW SOLUTION APPROACH TO FDI ATTACK: LI-FI

The advantages of the existing infrastructure of Li-Fi systems over Wi-Fi are generally seen physically. Transmission nodes of Li-Fi systems can be as vulnerable as RF counterparts when deployed in common areas and/ or when large windows are found in the coverage areas. For this reason, the Li-Fi infrastructure used in this study, as depicted in Figure 5, was designed taking into account information security requirements in ICS data communication. Thanks to Li-Fi's support of the IEEE 802.1X authentication standard, a dongle with a unique Id / tag was used for each user / hardware authorized in the Li-Fi transmission environment for authentication in architecture. Dongle belonging to all users in the system through the authentication application is authorized according to the authorization class and location (geo) information. In this way, each terminal will have access rights only according to its authority domain and class.

There are also various mechanisms for authentication such as biometric systems, software-based password authentication. However, there are important vulnerabilities in other authentication methods that cause this model not to be selected. One the most important authentication mechanism is using biometrics. However, there are vulnerabilities when recording a person's biometrics, such as fingerprints, iris, and facial features. Some of these vulnerabilities are situations involving physical damage (e.g. laser retinal scanning), loss of privacy (irreversible loss of personal data), low efficiency of biometric devices (low accuracy), and production of fake biometric data. These vulnerabilities are the main threats encountered in biometric authentication.

Additionally, three are types of attacks that try to exploit these threats are generally divided into four groups. These are Processing and Transmission Level Attacks, Input Level Attacks, Back-End Attack (especially for DoS) and Enrollment Attack [23]. The information is transmitted via wireless channels between the reader and the electronic tag, and the electronic tag has a small storage space and poor protection capacity, so it is vulnerable to side channel attack and system fraud, which can severely affect the security of the systems. Therefore, RFID based authentication mechanisms are also vulnerable to attacks [24]. Another common authentication mechanism is single factor authentication systems using only username and passwords. Only single-factor software passwords provide insufficient protection due to threats such as the capture of usernames and passwords with social engineering, the use of weak passwords to successfully exploit the vulnerabilities (brute force, dictionary attack, rainbow attack). Therefore, two-factor authentication (2FA) systems have become almost mandatory for security [25].

The reason for choosing this mechanism for authentication is that it is more secure than other authentication mechanisms. In addition, in the comparisons made on identity verification, it is seen that the hardware (token, dongle, cards) authentication mechanism has superior security features compared to other methods [26]. In the security architecture suggested in the article, unique hardware is designed in order to access the network where Li-Fi infrastructure is used. Even if another dongle of the same brand is owned, it cannot enter the ICS network because each authorized dongle is registered in the system and the access of the unauthorized dongle to the network is restricted. After the user accesses the network with the Dongle with an authorized ID, user authentication is performed over the active directory via 802.1X for user authentication to access the server and secure data. In summary, two factor authentication mechanism is used in the model.

The model proposed in the study has been designed considering these security vulnerabilities. Since the dongle proposed in the model has a personal and unique ID, it may pose a threat only if it is physically stolen or copied by malicious people (insiders). However, if the same ID is used more than once, the system will warn (a device with the same ID has been found in the network - duplicate ID), and in case of theft, access to the system will be blocked by adding to the banned ID list. When the authentication methods are evaluated in general, using dongles with unique ID addresses in management communication of critical infrastructures such as ICS is more secure than other authentication method For the confidentiality of data transmission, the use of symmetric encryption (AES 256 and above) or asymmetric encryption (RSA, Elliptic curve) infrastructure has been proposed. In the choice of encryption infrastructure, the value of the information asset to be transmitted in terms of the enterprise and the investment cost accordingly should be taken into consideration. After this selection, any of the preferred encryption / decryption methods for privacy can be used by enabling between dongle and Li-Fi transceiver hardware. In this way, even in the interference attacks that will be realized as a result of any reflection of the light out of the outside [27] or the entry of physically unauthorized people based on user error, a dongle with unique id / tag and symmetric / asymmetric key will be required for authentication. The proposed architecture is an important solution for FDI and / or interference attacks (MitM, eavesdropping, etc.) based on the insider factor, which are important attacks for ICS. Until this stage, privacy and integrity components of information security have been provided. In addition, considering the technical features provided by the Li-Fi technology mentioned in the second section, it will also make an important contribution to accessibility, as the architecture enables the authorized users to access the data sources they need at high speeds. Li-Fi is a light-based wireless communication technology. Li-Fi uses light instead of radio waves to transmit data. Therefore, Li-Fi is faster than other wireless technologies like Wi-Fi, Bluetooth, etc. [28]. For example, using the 2.4 GHz frequency band and radio wave data transmission

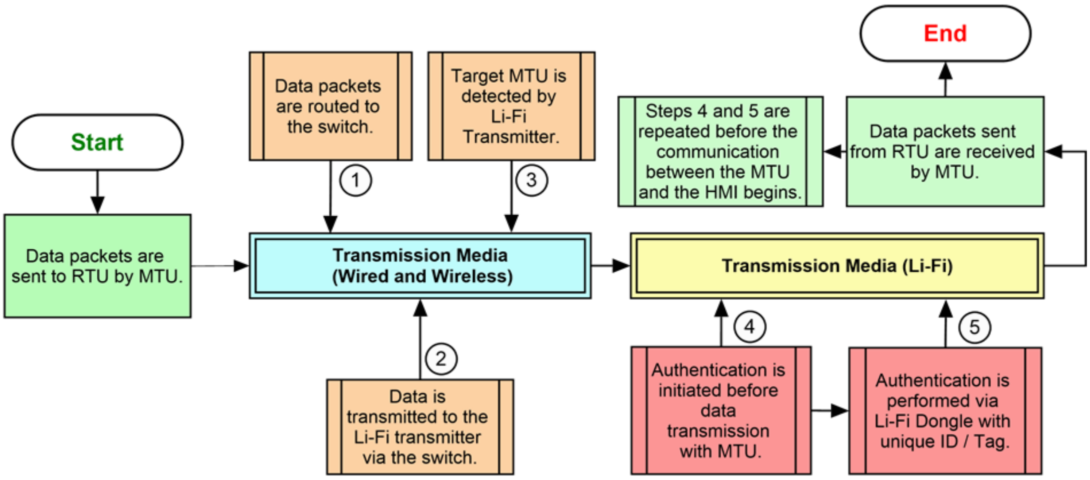

Start
Data packets are sent to RTU by MTU.
Data packets are routed to the switch.
1
Target MTU is detected by Li-Fi Transmitter.
3
Transmission Media (Wired and Wireless)
2
Data is transmitted to the Li-Fi transmitter via the switch.
Transmission Media (Li-Fi)
4
Authentication is initiated before data transmission with MTU.
5
Authentication is performed via Li-Fi Dongle with unique ID / Tag.
Data packets sent from RTU are received by MTU.
Steps 4 and 5 are repeated before the communication between the MTU and the HMI begins.
End

Figure 5. Li-Fi in ICS data flow diagram

method, Wi-Fi transmits data at speeds of 150-600 Mbps. On the other hand, Li-Fi, which uses the frequency band at THz levels and uses visible light in data transmission, can transmit data at speeds higher than 10Gbps. Although these speeds vary in theory and practice, all studies indicate that Li-Fi technology has very high data transmission rates compared to other wireless transmission technologies, especially Wi-Fi [20, 29-30].

Lack of forensics tools for ICS, cost of mirroring or backing up for not preventing continuity are important challenges for ICS forensics. Because, one of the most important problems in the attacks carried out over the existing network is the difficulty of accessing the existing log records in the event analysis after the attack and detecting the attacker from the too much data after access. In the Li-Fi communication model using the dongle with a single ID proposed in this study, it will be possible to determine which dongle is used for the attacks and other unauthorized operations on the network, and access to the network will only be made through authorized dongles. In this way, the data on which forensic analysis will be carried out will be narrowed and the results can be reached much faster, more accurately and effectively. There are threats such as copying authorized dongles and stealing the dongle. However, it will be possible to revoke the authorization and prevent the attack in a short time if it can be quickly determined on which authorized dongle the attack was carried out. Therefore, using the Li-Fi transmission environment in ICS will provide considerable convenience in network forensics in the investigation of the event as a result of any attack. Additionally, it will make significant contributions to the final conclusion by performing the forensic analysis much faster. As the Li-Fi transmission includes;

- Dongle use in transmission medium security,
- Network segmentation of critical devices,
- Permit physical access to a limited number of authorized personnel, continuous monitoring with cameras,
- Retention of GEO data in data transfer.

5. CONCLUSION

In this study, an architectural solution proposal using Li-Fi transmission infrastructure is presented for information stealing and changing attacks such as FDI, MitM, eavesdropping to smart city / network infrastructure. In architecture, the access of only authorized users is provided both hardware and software checks, including on mobile devices, with the use of Li-Fi medium in the transmission of data in environments where the most critical components of ICS such as MTU and HMI are present. The architecture proposed in the study includes a unique tag / id for each hardware and authorization users in ICS, and the Li-Fi transmission infrastructure in which authentication based on IEEE 802.1X and data is encrypted. With this infrastructure, the Privacy and Integrity dimensions are provided as the critical data of ICS is only transmitted in an unclear form among authorized users. In addition, with the broad spectrum (RGB) and capacity provided by Li-Fi technology, faster and more efficient data transmission can be achieved. This aspect also supports availability. In this way, the data security triad of ICS is protected by transmitting the data in a tampered (secure) environment. It has been evaluated that this study will enlighten on the use of Li-Fi in ICS and other studies on ICS security and will make important contributions.

ACKNOWLEDGEMENT

This study has been funded by Istanbul Gelişim University Scientific Research Projects Application and Research Center. Project number: KAP-141220-SG.

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

Serkan GÖNEN: Wrote the manuscript.

Hasan Hüseyin SAYAN: Performed the experiments and analysed the results.

Gökçe KARACAYILMAZ: Performed the experiments and analyse the results.

Erhan SİNDİREN: Performed the experiments and analysed the results.

Furkan ÜSTÜNSOY: Performed the experiments and analysed the results.

Harun ARTUNER: Performed the experiments and analysed the results.

Ercan Nurcan YILMAZ: Wrote the manuscript.

Mehmet Fatih IŞIK: Performed the experiments and analysed the results.

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] Üstünsoy F., Sayan H. H., “Sample laboratory work for energy management with SCADA supported by PLC”, ***Journal of Polytechnic***, 21(4): 1007-1014, (2018).

[2] Yılmaz E. N., Gönen S., “Attack detection/prevention system against cyber attack in industrial control systems”, ***Computers & Security***, 77: 94-105, (2018).

[3] Li Y., Wang Y., "False data injection attacks with incomplete network topology information in smart grid", ***IEEE Access***, 7: 3656-3664, (2018).

[4] Myers D., Suriadi S., Radke K., Foo E., "Anomaly detection for industrial control systems using process mining", ***Computers & Security***, 78: 103-125, (2018).

[5] Yılmaz E. N., Sayan H. H., Üstünsoy F., Gönen S., Karacayılmaz G., "Cyber security analysis of DoS and MitM attacks against PLCs used in smart grids", ***7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)***, Istanbul, Turkey, 36-40, (2019).

[6] Ayyash M., Elgala H., Khreishah A., Jungnickel V., Little T., Shao S., Rahaim M., Schulz D., Hilt J., Freund R., "Coexistence of WiFi and Li-Fi toward 5G: concepts, opportunities, and challenges", ***IEEE Communications Magazine***, 54(2): 64-71, (2016).

[7] Kaur R., Walia H., "Review on light fidelity (Li-Fi)-an advancement of wireless network", ***I.J. Wireless and Microwave Technologies***, 7(3): 25-35, (2017).

[8] Jennifer L. J., Jayanthy S., Sujitha J., "Li-Fi Technology based Fleet Vanguard and Security", ***Indian Journal of Science and Technology***, 9(11): 1-5, (2016).

[9] Pawar S., Kinny T., Puthuva F., Komban A., Belekar D., "Data Communication using visible light", ***International Journal of Students Research in Technology & Management***, 3(5): 358-362, (2015).

[10] Gupta A., Garg P., Sharma N., "Hybrid LiFi- WiFi indoor broadcasting system", ***28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC '17)***, Montreal, QC, Canada, 1-6, (2017).

[11] Perwej Y., "The next generation of wireless communication using Li-Fi (light fidelity) technology", ***Journal of Computer Networks***, 4(1): 20-29, (2017).

[12] Jha P. K., Mishra N., Kumar D. S., "Challenges and potentials for visible light communications: State of the art", ***International Conference on Positron Annihilation (1849)***, Kerala, India, 1-7, (2017).

[13] Classen J., Chen J., Steinmetzer D., Hollick M., Knightly E., "The spy next door: Eavesdropping on high throughput visible light communications", **In Proceedings of the 2nd *International Workshop on Visible Light Communications Systems***, 9-14, (2015).

[14] Yucebas D., Yuksel H., "Power analysis based side-channel attack on visible light communication", ***Physical Communication***, 31: 196-202, (2018).

[15] Kulkarni S., Darekar A., Joshi P., "A survey on Li-Fi technology", ***International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET '16)***, Chennai, India, 1624-1625, (2016).

[16] Ebrahim K. J., Al-Omary A., "Sandstorm effect on visible light communication", ***9th IEEE-GCC Conference and Exhibition (GCCCE)***, Manama, Bahrain, 1-7, (2017).

[17] Wang Q., Liverman S., Chu Y., Borah A., Wang S., Nguyen T., Natarajan A., Wang A. X., "WiFO: A Hybrid WiFi Free-Space Optical Communication Networks of Femtocells", ***20th ACM International Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '17)***, Miami, FL, USA, 35–42, (2017).

[18] Irshad M., Liu W., Wang L., Shah S. B. H., Sohail M. N., Uba M. M., "Li-local: green communication modulations for indoor localization", ***2nd International Conference on Future Networks and Distributed Systems (ICFNDS '18)***, Amman, Jordan, 1-6, (2018).

[19] Wang Y., Haas H., "A Comparison of Load Balancing Techniques for Hybrid LiFi/RF Networks", ***4th ACM Workshop on Visible Light Communication Systems (VLCS '17)***, Snowbird, UT, USA, 43–47, (2017).

[20] Kuppusamy P., Muthuraj S., Gopinath S., "Survey and challenges of Li-Fi with comparison of Wi-Fi", ***International Conference on Wireless Communications, Signal Processing and Networking (WISPNET)***, Chennai, India, 896-899, (2016).

[21] Haas H., "Li-Fi: Conceptions, misconceptions and opportunities", ***IEEE Photonics Conference (IPC)***, Waikoloa, HI, USA, 680-681, (2016).

[22] Sindiren E., Ciylan B., "Application model for privileged account access control system in enterprise networks", ***Computers & Security***, 83: 52-67, (2019).

[23] Alaswad A. O., Montaser A. H., Mohamad F. E., "Vulnerabilities of Biometric Authentication Threats and Countermeasures", ***International Journal of Information & Computation Technology***, 4(10): 947-58, (2014).

[24] Wang Y., Shen J., Guo X., Dong W., "Research on RFID attack methods", ***In 2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE),*** IEEE, Shenyang, China, 433-437, (2020).

[25] Zhang J., Tan X., Wang X., Yan A., Qin Z., "T2FA: Transparent two-factor authentication", ***IEEE Access***, 6: 32677-32686, (2018).

[26] Komarova A., Menshchikov A., Negols A., Korobeynikov A., Gatchin Y., Tishukova N., "Comparison of Authentication Methods on Web Resources", ***International Conference on Intelligent Information Technologies for Industry, Springer, Cham***, Varna, Bulgaria, 104-113, (2017).

[27] Marin-Garcia I., Guerra V., Perez-Jimenez R., "Study and validation of eavesdropping scenarios over a visible light communication channel", ***Sensors***, 17(11): 1-18, (2017).

[28] Afzal M. A., He D., Zhu Z., Yang Y., "Performance Evaluation of Wi-Fi Bluetooth Low Energy & Li-Fi Technology in Indoor Positioning", ***2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)***, IEEE, Shanghai, China, 1-5, (2018).

[29] Sharma P. K., Ryu J. H., Park K. Y., Park J. H., Park J. H., "Li-Fi based on security cloud framework for future IT environment", ***Human-centric Computing and Information Sciences***, 8(1): 1-13, (2018).

[30] Ramadhani E., G. Mahardika P., "The technology of LiFi: A brief introduction", In IOP Conference Series: Materials Science and Engineering, (Vol. 325, No. 1, p. 012013*), **IOP Publishing***, Yogyakarta, Indonesia, 1-10, (2018).