Wireless Industrial Access Control Systems for Autonomous Transportation

Alberto Martínez-Gutiérrez(✉), Javier Díez-González, Rubén Ferrero-Guillén, Paula Verde, José-Manuel Alija-Pérez, and Hilde Perez

Department of Mechanical, Computer and Aerospace Engineering, Universidad de León, 24007 León, Spain
{amartg,jdieg,rferrg,pverg,jmali,hperg}@unileon.es

Abstract. The digitization of industrial assets enables automation, generating added value to manufacturing processes. Digitalization is exemplified by the use of Wireless Sensor Networks (WSN) to monitor mobile robots and personnel in the industrial plant. Based on this infrastructure, the authors propose a novel access control system without the need to interact with any equipment. Hence, the implementation costs are reduced because the same Cyber-Physical Systems (CPS) technologies are reused, preventing the implementation of complementary equipment for both operators and mobile robots. In addition, the security of the wireless protocols has been analyzed by proposing a robust and scalable solution. Therefore, the accessibility to restricted areas is improved by reducing the authentication time compared to other technologies, especially for mobile robots.

Keywords: Autonomous mobile robots (AMR) · Bluetooth low energy (BLE) · Cyber-physical systems (CPS) · Industry 4.0 · Industrial Internet of Things (IIoT)

1 Introduction

The industry is immersed in a digital transformation where information and communication technologies are combined in order to generate higher added value. This new transformation, known as Industry 4.0 [1], is based on the digitization of assets in order to achieve more efficient, autonomous, and sustainable production. To achieve this, data is required, which is obtained by the CPS [2] according to the philosophy of the Industrial Internet of Things (IIoT) [3] which is critical for the connectivity of production processes.

The transport of materials and personnel in the manufacturing plant is an asset where data must be digitized as it is necessary for the optimization of the supply chain [4]. In this context of mobility, there may be restrictions on access to certain facilities due to various factors (e.g., security, regulations). For this reason, access control systems are used in industry and other sectors to manage the entry and exit of both vehicles and personnel into and out of certain areas [5].

However, industrial access control systems are based on technologies which are independent of CPS. This fact implies a greater complexity in the equipment, increasing

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
J. A. Benítez-Andrades et al. (eds.), *Global Challenges for a Sustainable Society*,
Springer Proceedings in Earth and Environmental Sciences, https://doi.org/10.1007/978-3-031-25840-4_34

its cost, as well as the implementation time. Moreover, most of the technologies used require physical interaction with the system, making it harder to integrate them into mobile robots [6]. In addition, all access control equipment requires data for decision-making either by human or expert systems.

In this context, digitalization of the process is sought through the use of CPS already existing in the industry in both humans and mobile robots in order to improve productivity. For instance, an example of digitization is wearable devices (e.g., smartwatches, augmented reality glasses, headphones) where the human is able to interact with the information in a more natural way. Autonomous mobile robots (AMR) which transport materials within the industrial plant according to the supply chain management are another application case [7].

Given this paradigm of digitization in the industrial plant, new access control systems can be developed that are compatible with the wireless technologies used in existing CPSs. In this way, no other complementary equipment will be required for the implementation of access control, thus achieving a collaborative industrial environment. Furthermore, with the implementation of this methodology, no new electronic equipment is required, thus reducing its use and its impact on the environment.

Therefore, the aim of this work is to adapt wireless CPS technologies to allow contactless access. In this way, the access accreditation time is reduced, improving the accessibility for both mobile robots and humans, which is a novelty in the scientific literature.

In addition, the use of wireless technologies allows us to know the room in which the equipment is located by creating a network of wireless sensors. In this sense, there are studies where the placement of beacons is optimized to maximize coverage [8, 9]. Therefore, this methodology also allows the monitoring of the approximate location of personnel, as well as key AMRs for organizational decision making.

The paper is organized as follows: In Sect. 2, the technologies used for access control in industries will be reviewed. Then in Sect. 3, the wireless technology used to achieve the stated objectives will be presented. Then in Sect. 4, the vulnerabilities of the technologies will be shown while in Sect. 5 proposals will be made to avoid the vulnerabilities. Section 6 shows the architecture demonstrator to reach the conclusions in Sect. 7.

2 State of Art

Access control in the industry applies different technologies depending on the needs of the processes or protocols. For this reason, the authors analyze in the scientific literature the different technologies used for access control in order to compare them with the proposed one [10, 11]. Table 1 below compares the technologies used to obtain data on the identification of mobile robots or people.

According to the information shown in Table 1, access control interaction is required for all technologies (i.e., swiping a card or device, looking into a camera, reading a fingerprint). Moreover, biometric systems are only supported by humans, thus requiring additional systems. In addition, RFID and Near Field Communication (NFC) contactless technology does not have sufficient range to identify mobile robots [12]. In addition, none of these technologies is usually incorporated in industrial equipment and these technologies must be implemented in a complementary way.

Table 1 Comparison of the different methods used for access control in industrial environments

Method	Type	Technology	Max range	Energy used	Reliability	Cost
Electronic card	Contactless	RFID	5 cm (13.56 MHz)	Built-in battery	High	Low
Facial recognition	Biometrics	Camera/algorithms	40 cm approx.	Power supply required	Dependence on conditions	High
Fingerprint recognition	Biometrics	Capacitance readers/algorithms	Contact required	Built-in battery	Dependence on conditions	Middle
Short-range wireless	Contactless	NFC	20 cm	Built-in battery	High	Middle

For this reason, an access system capable of identifying people and AMRs at a greater distance without the need to incorporate complementary systems is required. In this way, the number of devices is reduced, reducing the cost of implementation and improving accessibility. To this end, the authors propose the following technologies based on wireless communications.

3 BLE and Wi-Fi Technologies

Bluetooth Low Energy (BLE) and Wi-Fi technologies are widespread communication interfaces in industrial CPS and most wearables [13]. The Bluetooth standard works in the industrial, scientific, and medical (ISM) 2.4 GHz band using 40 channels of 2 MHz in order to avoid interference. On the other hand, the Wi-Fi standard, despite operating on the same frequency, has a longer range (i.e., tens of meters) due to its transmitting power, resulting in higher power consumption. In this context, BLE technology, having a shorter range than Wi-Fi (i.e., 2–3 m) as well as lower power consumption, is the most suitable for wireless access control systems.

Based on BLE standard specifications of the Generic Access Profile (GAP), devices have four roles: broadcaster, observer, central and peripheral [14]. Sender devices use the 3 advertisement channels to publish information in the broadcast format (i.e., multi-point) while observers within range are able to read it. However, this information is not encrypted so any device can listen to it making device authentication difficult. However, this methodology does not require a previous connection to be established, decreasing the response time of the system.

Another method is the establishment of a point-to-point encrypted connection to determine identity by sending a password or token. This requires a central device and a peripheral device which requires a pairing or prior connection. Once authenticated, the link is encrypted and long-term keys (LTK) are stored for a faster connection. For pairing the devices must negotiate a methodology for the generation of the temporary secret key (STK) with 3 main methods [15]:

- **Just work (JW)**: The STK is generated on both sides according to the packets exchanged. Nevertheless, this procedure is vulnerable to man-in-the-middle attack (MitM), which is a security vulnerability. However, since version 4.2 BLE has incorporated the Elliptic Curve Diffie-Hellman (ECDH) algorithm which is based on discrete logarithms [16]. As a result, it is simple for the partners to compute a symmetric password while for MiTM the computation of LTK is unfeasible computationally. LTK is stored in both in order to facilitate future connections.
- **Out Of Band (OOB)**: The devices use other protocols (e.g., Wi-Fi, NFC) in order to exchange the pairing and authentication password. Unfortunately, not all industrial devices have multiple communication interfaces.
- **Pass-keys**: One device generates a code which has to be manually entered into the other device by a user. Although this procedure is only performed on the first connection, not all industrial devices have to write and display interfaces.

Given the diversity of communication modalities, Fig. 1 shows an outline of the type of connections, as well as their vulnerabilities.

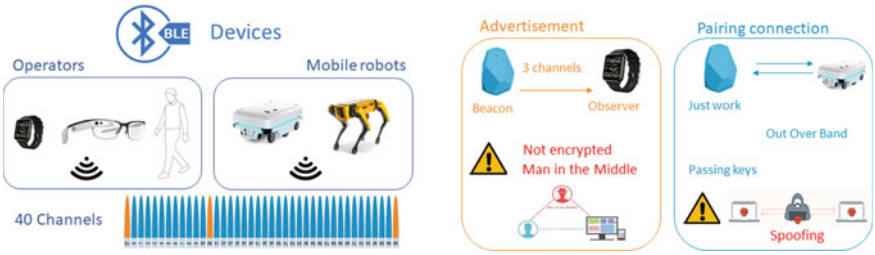

Fig. 1 Diagram of BLE functionalities and vulnerabilities in industrial environments

4 Vulnerability Analysis

Based on the methodologies presented in Fig. 1, to achieve a secure communication channel without the need for the user or mobile robot interaction, the JW or OBB method is required. However, the connection does not involve user authentication but the creation of a secure channel that avoids MiTM. Moreover, the BLE stack provides the message authentication service but does not provide the device authentication service.

Furthermore, a recent study [17] alerts to security vulnerabilities in the authentication of equipment reconnection via LTK. For this purpose, the researchers developed the BLE spoofing attacks (BLESA) tool where they spoof other devices by violating the authenticity of the messages. In this context, a design vulnerability for reactive authentication and implementation issues for proactive authentication of messages were discovered. Therefore, this security gap is unacceptable in an access control system. Hence, the authors propose the following proposals.

5 Proposals

To solve the authentication of the devices it is necessary to create asymmetric keys (i.e., public and private) in order to certify the authentication of both devices (i.e., central and peripheral) preventing spoofing. In addition, this way, vulnerabilities to BLESA are resolved. However, this methodology needs to be developed in the application as the BLE protocol layers are not secure, which makes it difficult to integrate into CPSs.

Alternatively, every access point could incorporate a Beacon which would issue temporary codes on advertisement channels which are public and exposed to MiTM attacks. In this case, the temporary codes would be hashed based on timestamps in combination with an identifier token and a random number. Moreover, both beacons and mobile robots must have another secure communication interface (i.e., authentication, message integrity, accessibility) in order to communicate with an access manager. Thus, beacons constantly emit different hashes which are meaningless in the case of MiTM. Moreover, in case of spoofing, since there is no connection to the server and the connection is authenticated, access would be denied in case of attack. Furthermore, this ephemeral key method hinders attacks due to the temporary limitation of access without the need for pairing. Figure 2 illustrates the architecture of the access control system.

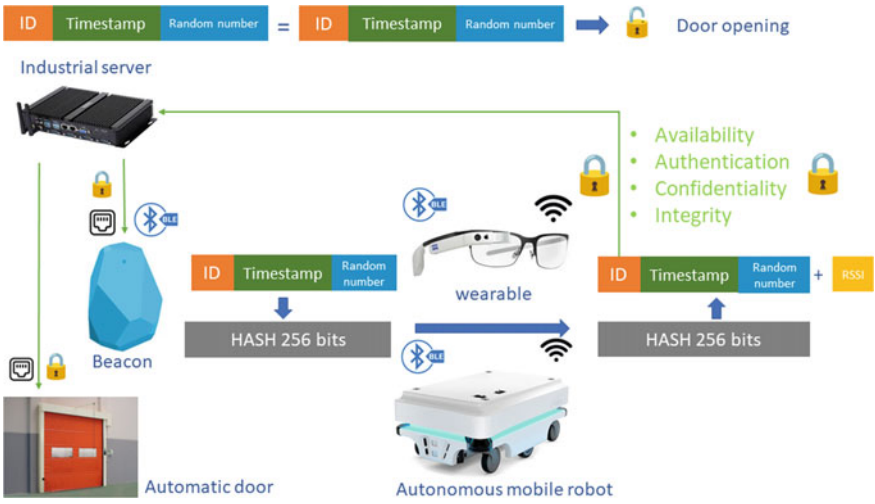

Fig. 2 Proposed architecture for wireless access control system in industrial environment

According to Fig. 2, the system would enable access control from an external point, as well as the location of mobile robots and industrial plant personnel. Furthermore, the transmitting power can be regulated from the beacons to modify the radius of action, as well as the power consumption. In addition, the receivers can delay the strength with which they receive the signal (e.g., RSSI) as an indication of proximity to the access points. This parameter, as well as access policies, can be controlled in real-time from industrial data acquisition and control systems (SCADAs) or industrial computers.

However, this same philosophy can be used in reverse, with the beacon being the mobile agent acting as the observer beacon. The following is a detailed description of how a demonstrator of this technology has been implemented for both human and mobile robots.

6 Architecture Demonstrator

Considering the diversity of equipment, two generic ESP-32 development boards have been used to test this methodology, both of which have Wi-Fi and BLE communication interfaces. To this end, one board acts as a beacon while the other simulates a CPS. The CPS and the beacon send the information to the access control server using Message Queuing Telemetry Transport (MQTT) with Transport Layer Protocol (TLS).

The access control server has been programmed with the node-red tool which allows connecting hardware as well as APIs. When the message emitted by a CPS matches the one sent by a beacon, the server gives the order to open the door using the same protocol. In addition, the location of the CPS can be monitored from the access control interface. In addition, the access control policy can be defined from this interface.

Meanwhile the CPS and beacons have been programmed in C ++ using visual studio by Platformio editor. In this case the door opening control and the beacon are integrated on the same board simulating with a LED diode the opening signal. This demonstrates that the architecture is operational and functional for integration in industrial CPS. Furthermore, the demonstrator is suitable for industrial mobile equipment such as operator wearables.

7 Conclusions

The wireless access control systems increase the productivity and comfort of the personnel. In order to achieve this, wireless technologies compatible with the CPS have been used, which have a wider range of action, such as BLE, as opposed to the current ones. Nevertheless, the security in the authentication of the devices is a problem in the BLE protocol. However, this problem has been solved through the use of industrial ethernet platforms characteristic of Industry 4.0. In this way, it has been possible to connect a digitized ecosystem allowing greater information on the location of industrial assets. Therefore, it has been possible to automate access control to mobile robots and personnel in a secure way, which is a novelty in the scientific literature. Furthermore, this methodology can be applied to other sectors (e.g., hospitals, and hotels) where access control is a problem.

Funding. This research has been developed and funded by the project of the Spanish Ministry of Science and Innovation grant number PID2019-108277GB-C21.

References

1. Lasi, H., Kemper, H.-G., Feld, T., Hoffmann, M.: Industry 4.0. Negocios e información (2014). https://doi.org/10.1007/s12599-014-0334-4
2. Liu, X., Cao, J., Yang, Y., Jiang, S.: CPS-based smart warehouse for industry 4.0: a survey of the underlying technologies. Computers **7**(1), 13 (2018). https://doi.org/10.3390/COMPUTERS7010013
3. Mumtaz, S., Alsohaily, A., Pang, Z., Rayes, A., Tsang, K.F., Rodriguez, J.: Massive internet of things for industrial applications: addressing wireless IIoT connectivity challenges and ecosystem fragmentation. IEEE Ind. Electron. Mag. **11**(1), 28–33 (2017). https://doi.org/10.1109/MIE.2016.2618724
4. Pamoshika Jayarathna, C., Agdas, D., Dawes, L., Yigitcanlar, T., Masmoudi, M.: Multi-objective optimization for sustainable supply chain and logistics: a review. mdpi.com (2021). https://doi.org/10.3390/su132413617
5. Figueroa-Lorenzo, S., Añorga, J., Arrizabalaga, S.: Methodological performance analysis applied to a novel IIoT access control system based on permissioned blockchain. Inf. Process Manag. **58**(4), 102558 (2021). https://doi.org/10.1016/J.IPM.2021.102558
6. Martínez, A., et al.: Digital twin for the integration of the automatic transport and manufacturing processes. IOP Conf. Ser. Mater. Sci. Eng. **1193**(1), 012107 (2021). https://doi.org/10.1088/1757-899X/1193/1/012107
7. Martínez-gutiérrez, A., Díez-gonzález, J., Ferrero-guillén, R., Verde, P., Álvarez, R., Perez, H.: Digital twin for automatic transportation in industry 4.0. Sensors **21**(10), 3344 (2021). https://doi.org/10.3390/S21103344
8. Díez-González, J., Verde, P., Ferrero-Guillén, R., Álvarez, R., Pérez, H.: Hybrid memetic algorithm for the node location problem in local positioning systems. Sensors **20**(19), 5475 (2020). https://doi.org/10.3390/S20195475
9. Ferrero-Guillén, R., Díez-González, J., Álvarez, R., Pérez, H.: Analysis of the genetic algorithm operators for the node location problem in local positioning systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 12344 LNAI, pp. 273–283 (2020). https://doi.org/10.1007/978-3-030-61705-9_23/FIGURES/7
10. Ibrahim, R., Zin, Z.M.: Study of automated face recognition system for office door access control application. In: 2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011, pp. 132–136 (2011). https://doi.org/10.1109/ICCSN.2011.6014865
11. Farooq, U., ul Hasan, M., Amar, M., Hanif, A., Usman Asad, M.: RFID based security and access control system. Int. J. Eng. Technol. 309–314 (2014). https://doi.org/10.7763/IJET.2014.V6.718
12. Couraud, B., Deleruyelle, T., Deleruyelle, T., Vauche, R., Flynn, D., Daskalakis, S.N.: A low complexity design framework for NFC-RFID inductive coupled antennas. IEEE Access **8**, 111074–111088 (2020). https://doi.org/10.1109/ACCESS.2020.3001610
13. Díez, V., Arriola, A., Val, I., Velez, M.: Reliability evaluation of Bluetooth low energy for industry 4.0. In: IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, vol. 2019, pp. 1148–1154 (2019). https://doi.org/10.1109/ETFA.2019.8869211
14. Cäsar, M., Pawelke, T., Steffan, J., Terhorst, G.: A survey on Bluetooth low energy security and privacy. Comput. Netw. **205**, 108712 (2022). https://doi.org/10.1016/J.COMNET.2021.108712
15. Ghori, M.R., Wan, T.C., Sodhy, G.C.: Bluetooth low energy mesh networks: survey of communication and security protocols. Sensors **20**(12), 3590 (2020). https://doi.org/10.3390/S20123590

16. Subramanian, E.K., Tamilselvan, L.: Elliptic curve Diffie-Hellman cryptosystem in big data cloud security. Cluster Comput. **23**(4), 3057–3067 (2020). https://doi.org/10.1007/S10586-020-03069-3/FIGURES/6
17. Wu, J., et al.: {BLESA}: Spoofing attacks against reconnections in Bluetooth low energy. usenix.org, Available: https://www.usenix.org/conference/woot20/presentation/wu