ShahidChamran University of Ahvaz

Iranian Association of Electrical and Electronics Engineers

Journal of Applied Research in Electrical Engineering

E-ISSN: 2783-2864
P-ISSN: 2717-414X
Homepage: https://jaree.scu.ac.ir/

Applied Article

Improved Laser Beams-Based Security Fence to Protect Borders

Rahim Ildarabadi *, and Zohreh Keramat

Faculty of Electrical and Computer Engineering, Hakim Sabzevai University, Sabzevar 9617976487, Iran

** Corresponding Author: r.ildar@hsu.ac.ir*

Abstract: In this paper, the procedure for the protection of borders-based security fences improved using laser beams. Laser beams can be used to protect the border of large departments, large agencies, large universities, and large companies that have a large yard with several-kilometre erecting walls based on laser optic. But it has problems. To implement this system, it uses invention protocol transmission data. The cost of implementing this system is very low. The older methods of this system have been implemented in Hakim Sabzevery University.

Keywords: Infrared beam, security fence, data transmission, optic communication.

Article history
Received 08 August 2020; Revised 22 April 2021; Accepted 02 May 2021; Published online 28 June 2021.

How to cite this article
R. Ildarabadi, and Z. Keramat, "Improved laser beams-based security fence to protect borders," *J. Appl. Res. Electr. Eng.*, vol. 1, no. 1, pp. 50-58, 2022. DOI: 10.22055/jaree.2021.34586.1011

Check for updates

1. Introduction

The protection of very vast lands, such as large universities, military facilities, department agencies, and companies with several borders is a difficult task. These facilities are traditionally protected by inspection by operators, the use of barbed wire interval along its length, and so on. However, these methods have certain assumptions and problems. Inspection by operators can only be performed to a limited extent. When using the barbed wire method, robbers or saboteurs can cut the barbed wire. In addition, this method is costly. Putting closed-circuit television (CCTV) to supervise borders is much more costly and, at the same time, undesirable and irrational. This paper presents an approach for protecting the borders of very vast lands based on infrared beams, which is much less costly and easy to implement.

Laser radiation can pass through various channels, such as fibre optics and atmosphere or open space communications. [1].

Optical communications were used in various forms for messaging or warning thousands of years ago. For example, ancient people used to establish these communications by polishing their shields. Today, optical communications are also done by encoding and decoding optical signals with the help of semaphores and wireless solar telegraphs called heliographs [2].

Many simple and inexpensive consumer remote controls use low-speed communications using infrared (IR) light, which is known as consumer IR technologies.

Atmospheric conditions can cause disturbance in optical connection with open space channels. Like any other communication channel, open space can change both the amplitude and the phase of news signals. Therefore, in a news transmission route, if necessary, relays and amplifiers should be used to minimize the probability of news loss [3]. Although optical relays reduce the speed of data exchange, open space optical communication is still used to exchange data between spacecraft. One of the very simple technologies in outdoor optical communications is Infrared Communication Technology (IrDA) [4]. Due to atmospheric conditions, such as dust particles, fog, and the effects of heat, rain, and snow, the maximum range of optical light communications is usually considered to be less than 3 km above the ground. Due to this fact and even obstacles that sometimes interrupt light transmission completely, this method is not suitable for data transmission at the ground level and on very long distances. However, in 2007, amateur radio operators also reported outdoor light transmission (atmosphere) up to about 278 km with the help of high-power LEDs. According to the conditions of open space channels (atmosphere), one cannot expect too much speed for news transmission, and the cut-off frequency cannot be more than about 4 kHz [5].

Outside the atmosphere, it is practically possible to communicate light in the open air for several thousand kilometres owing to the much lower density of particles in space. In January 2013, NASA used optical telescopes to expand its beams, sending infrared optical communications to transmit space images up to a distance of about 400,000 kilometres using atmospheric interference data correction code algorithms. This algorithm is similar to the algorithm used to correct the data error of compact discs [6].

Secure open-space optical communications can be suggested using the N-infrared interferometer where the infrared signal is in the form of an interference pattern. It can be shown that this method is practically effective and works at the desired emission intervals and can basically be used at long distances in outer space [7].

In Ilderabadi's patent, he used this method to protect the environment from laser beams [8]. The visible laser beam cannot be used during the day. It is also difficult to regulate the transmission and reception of data and maintain it between the transmitter and the receiver through the communication of the laser beam. In this paper, free-space optical communications were used to defend the fence of large agencies based on IR beam communication. The next section describes how the proposed method works.

It should be noted that this work was presented as a research project for the protection of the university environment and was implemented to some extent. But, it was not implemented completely due to the need for about 80 nodes and their installation and adjustment, which was costly and required skilled people who were not available. The project report was also presented at the Twelfth International Conference ICTPE 2016 [9]. In addition, a part of it was published under the title of protection of the walls of cement factories in the scientific, technical, and economic monthly of Cement No. 250 in 2019 [10].

2. Border Security Based on Infrared Beam

This section presents a new approach to protecting the borders of large facilities against unwanted intrusion of people.

This method is simple. An infrared beam is created at one point of the border and an infrared beam receiver is placed at another point of the border as is shown in Fig. 1. In this design, the laser beam is used to detect night traffic on the wall. Thus, if the laser beam sent by the transmitter is received by the receiver according to Fig. 1, it means that there is no traffic between the receiver and the transmitter (normal state), otherwise if according to Fig. 1b, the transmission is cut off, the lack of laser beam will indicate traffic between the receiver and the transmitter. The distance between the transmitter and receiver can be variable from around 5 to 15 meters. If anyone passes on the border (fence), it will interrupt the infrared beam and the transmitted data will not be received by the receiver, implying that somebody has entered or exited.

In this design, the transmitter and receiver are placed at a distance of about 30 to 80 meters on the sides of the wall according to Fig. 2. As such, traffic on both sides of the wall is practically recognizable. Fig. 3 shows how each node is placed on the fence.

After a node detects an unauthorized bus, the location of the unauthorized password is transferred by that node to the adjacent node in two directions. The sending of the mentioned code continues in the same way and in two directions, until the mentioned code reaches the initial and final nodes and after decoding, the location of the error is determined. Fig. 4 shows how data is exchanged between different nodes. Each node can have four terminals, which are represented by the letter B in which B_{n1} and B_{n2} are the input terminals and B_3 and B_4 are the output terminals.

The possible states for each node are expressed below.
1) Initial display node (first terminal):

Mode A): daytime; if the laser receiver receives continuous light for more than about 10 seconds, it indicates that the air is bright (day) and daytime is shown on the display (Fig. 5).

Mode B): The received code is normal and in this case, the normal state is shown in the display (Fig. 6).

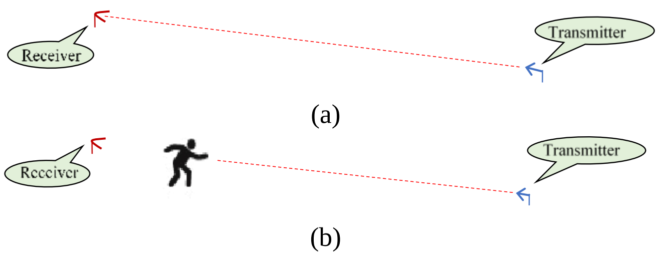


Fig. 1: (a) Data receipt from the wall in normal mode, (b) Data receipt interruption due to traffic through the fence.

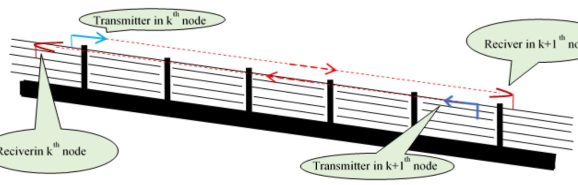


Fig. 2: Schematic of the position of infrared transmitter and receiver.

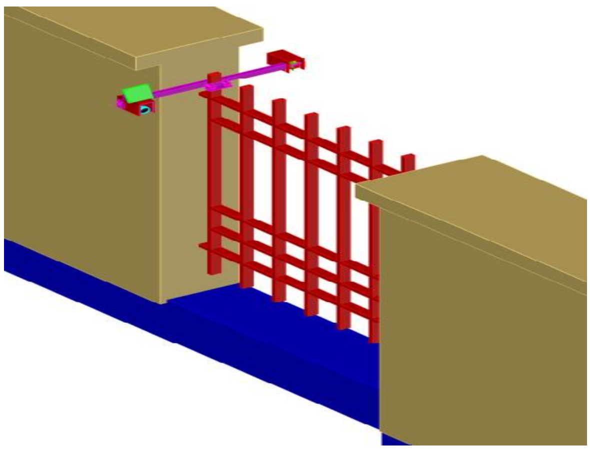


Fig. 3: How to place each node on the fence.

Fig. 4: How to exchange data between nodes.

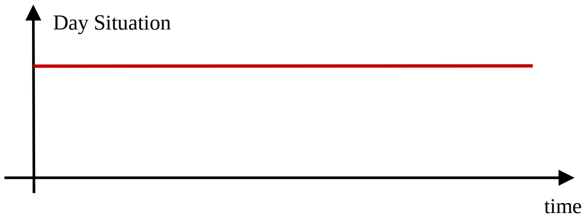


Fig. 5: Format of received data in mode 'a'.

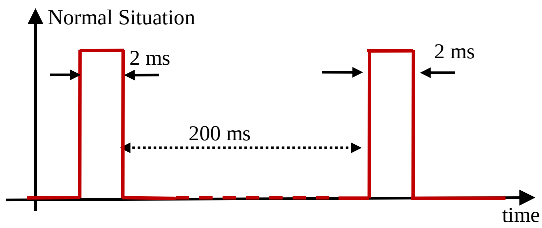


Fig. 6: Format of received data in normal mode.

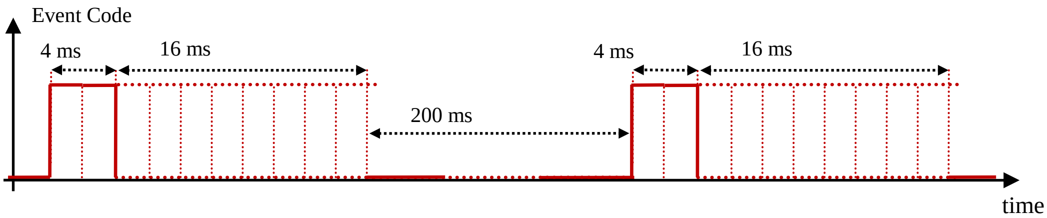


Fig. 7: Format of received data for unauthorized crossing case.

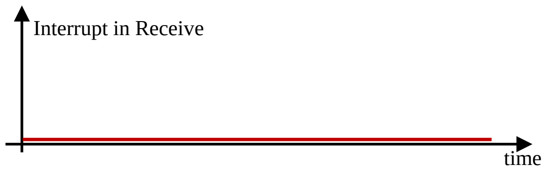


Fig. 8: Format of received data when an interruption occurs.

Mode C) The received code is the error code of one node, so this code should be displayed in the output (Fig. 7).

Mode D) No data is received. It is considered an error between this node and the first node, so the breakdown code in data receiving is shown in the output (Fig. 8).

2) First node:

Mode A) being up to date. If the laser receiver receives continuous light for more than about 10 seconds, do not send light from this node. But always check the status of the receiver (Fig. 9).

Mode B) The received code is normal and in this case, the normal state is sent on both sides (Fig. 10).

C) The received code is the error code sent from other nodes; In this case, this error code will be sent to the primary display node. On the other hand, normal code is still sent to the adjacent node (Fig. 11).

D) Not receiving the signal. It is the occurrence of an error between the first group and its adjacent (second) node. In this case, the corresponding error code is sent to both the display group and the second node (on the other side) (Fig. 12).

3) Middle nodes:

A) If the middle node receives data from both parties, send the received data of each party to the same party. This condition is considered the absence of traffic on both sides of this node. Fig. 13 shows the conditions that can occur in this case.

B) If data is not received from one side, the related error code in this node is sent to the nodes of the parties, and if data is not received from both sides, the error code is sent consecutively (one in between) on both sides. To be. (As shown in Fig. 14).

C) Being up to date. If the receivers of this node receive light continuously for more than about 10 seconds, the data transmission to the parties is interrupted. But, recipients should always check the status (as shown in Fig. 15).

3) End node:

It is like the primary node. The performance algorithm of each node is presented in Fig. 16.

For the end node, B3 is received and checked instead of B4. Also, the normal code is still sent by B1 when receiving the error code via B3, and the received error code is sent by B2 (B4 moves with B3 and B2 with B1).

System implementation in Proteus software is shown in Fig. 19. In this figure, the first node, the middle node, and the end node are implemented by the Atiny13 Atmel microcontroller. The displayer node is implemented by the Atemga 32 microcontroller and shows the result on an LCD. Three state switches are used to create the normal situation, day state, and error accruing state.

(a) (b)

Fig. 9: The format of (a) incoming, and (b) outgoing data during the day

(a) (b)

Fig. 10: The format of (a) incoming, and (b) outgoing data in normal mode

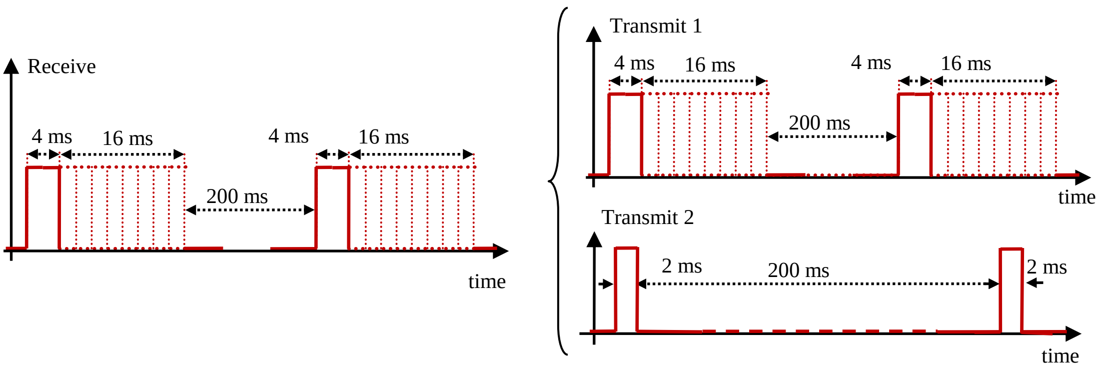
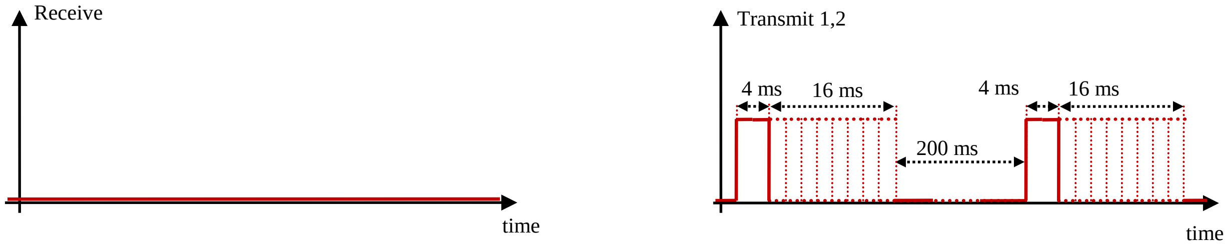


Fig. 11: The format of the received and transmitted data in the error code and the sent normal code to other side



(a) (b)

Fig. 12: Format of (a) received, and (b) sent data in the absence of data.

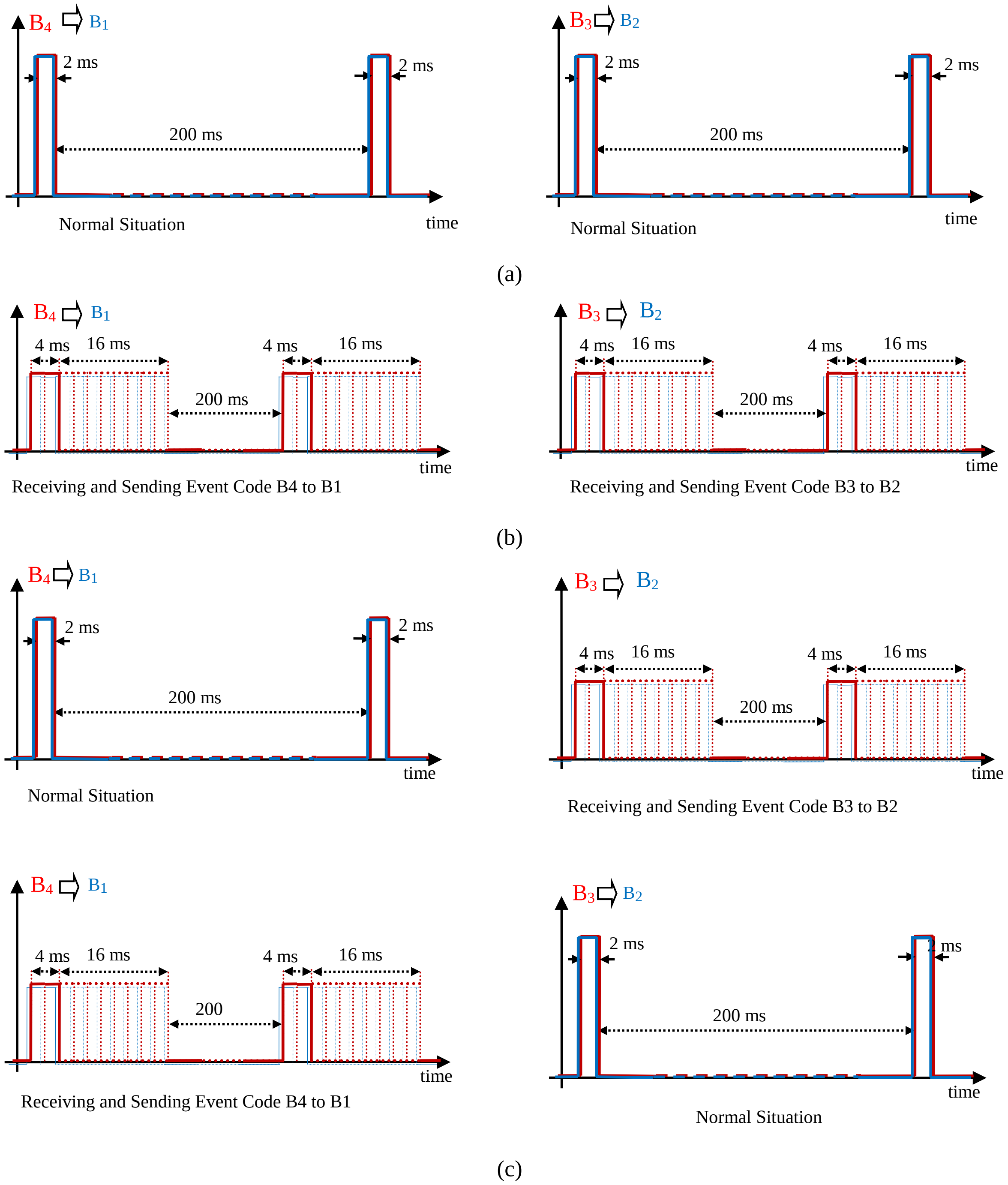


Fig. 13: (a) The format of incoming and outgoing data in the case of the middle's nodes receiving data from both sides. B_1 and B_2 are input terminals and B_3 and B_4 are output terminals (Normal Situation), (b) Receiving and sending event code between two middle nodes, and (c) From one side Receiving and sending error code, and from another side Receiving and sending Normal code.

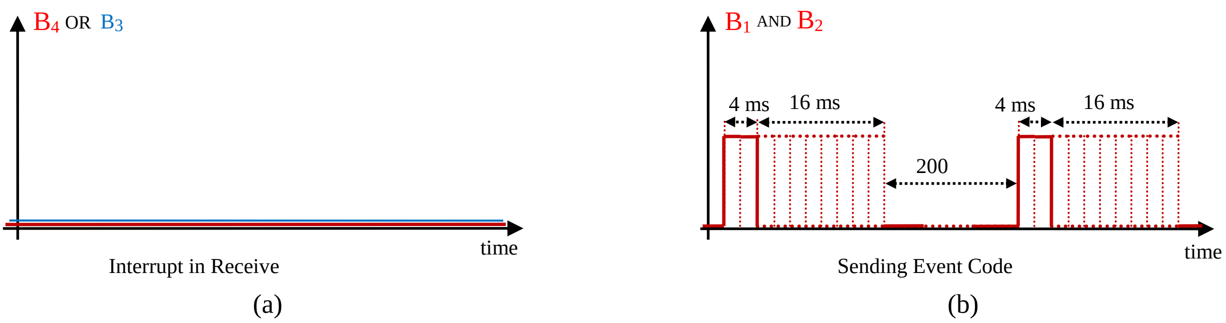


Fig. 14: The format of (a) incoming and outgoing data in the case of the middle group does not receive data on one side.

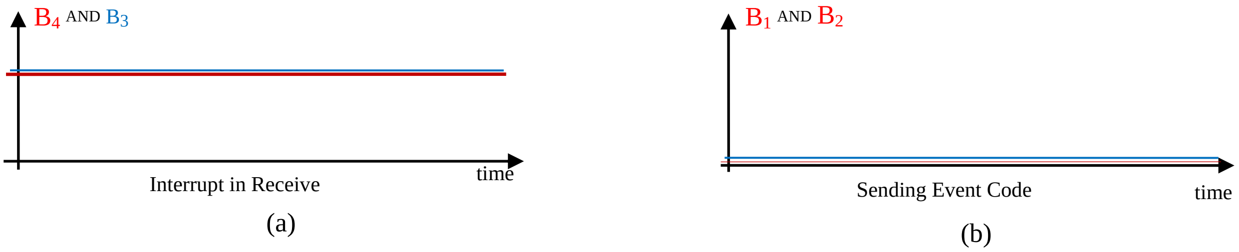


Fig. 15: The format of (a) incoming and (b) outgoing data in the current state.

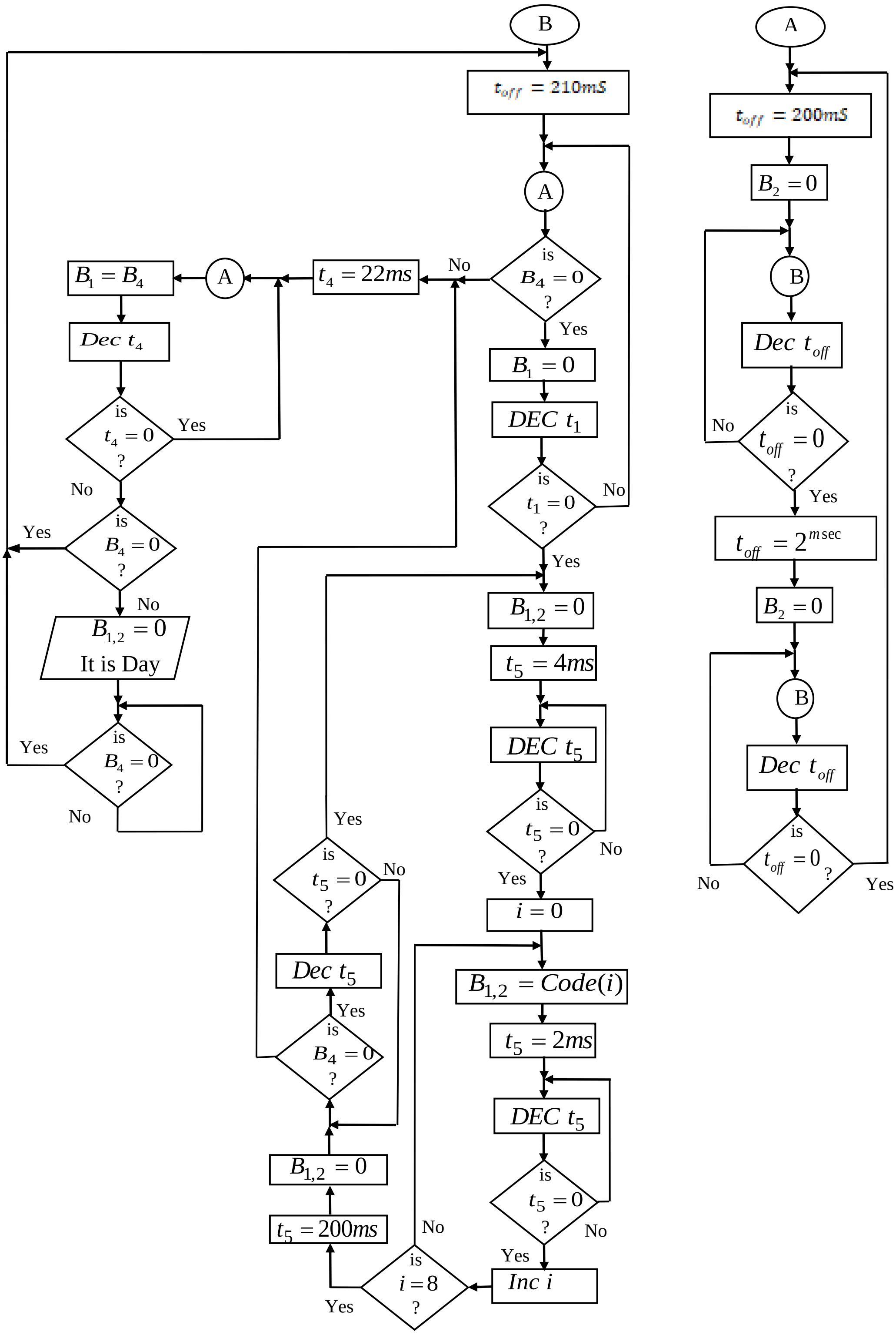


Fig. 16: System performance algorithm for the first node.

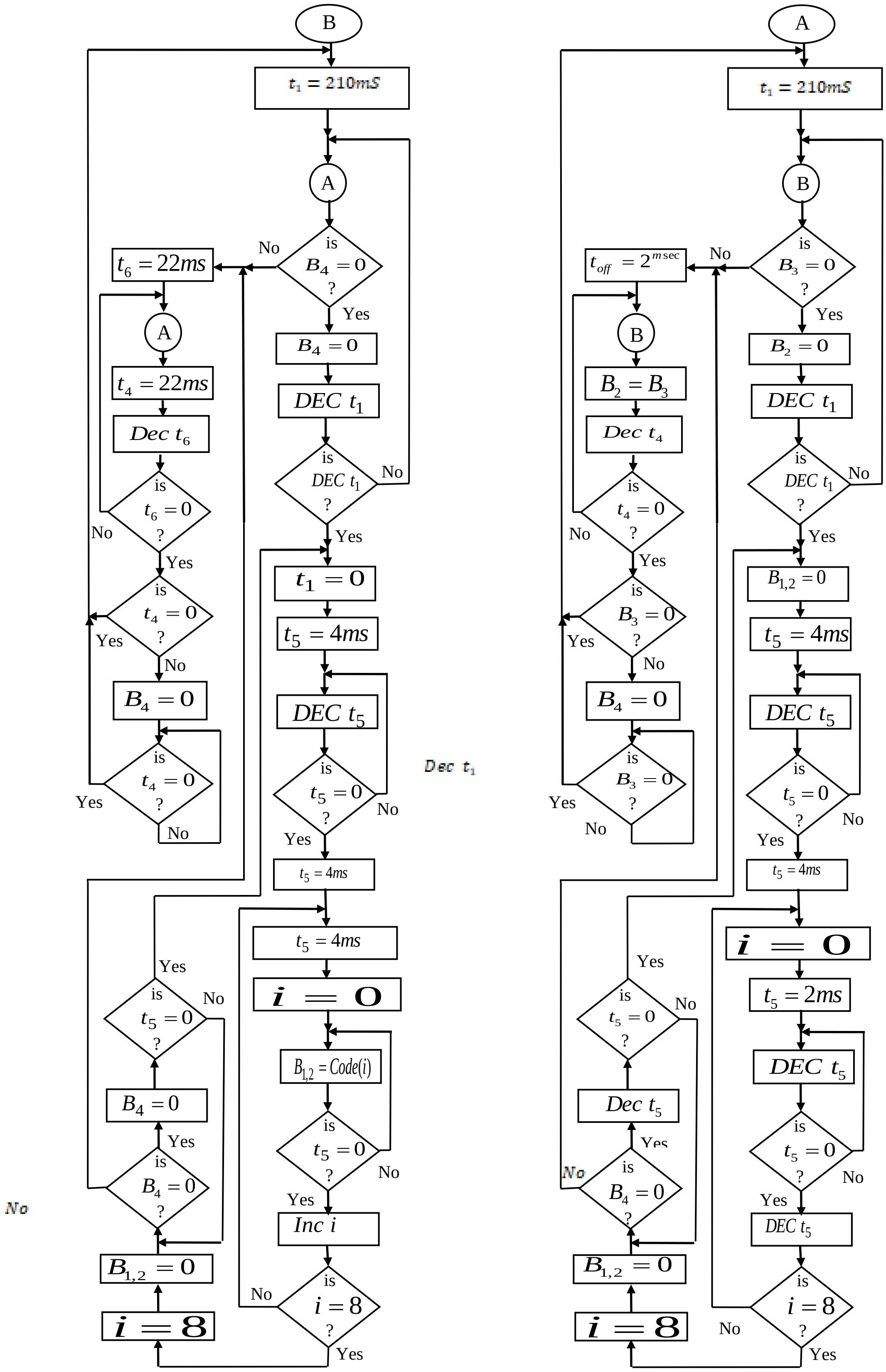


Fig. 17: System performance algorithm for the first intermediate nodes.

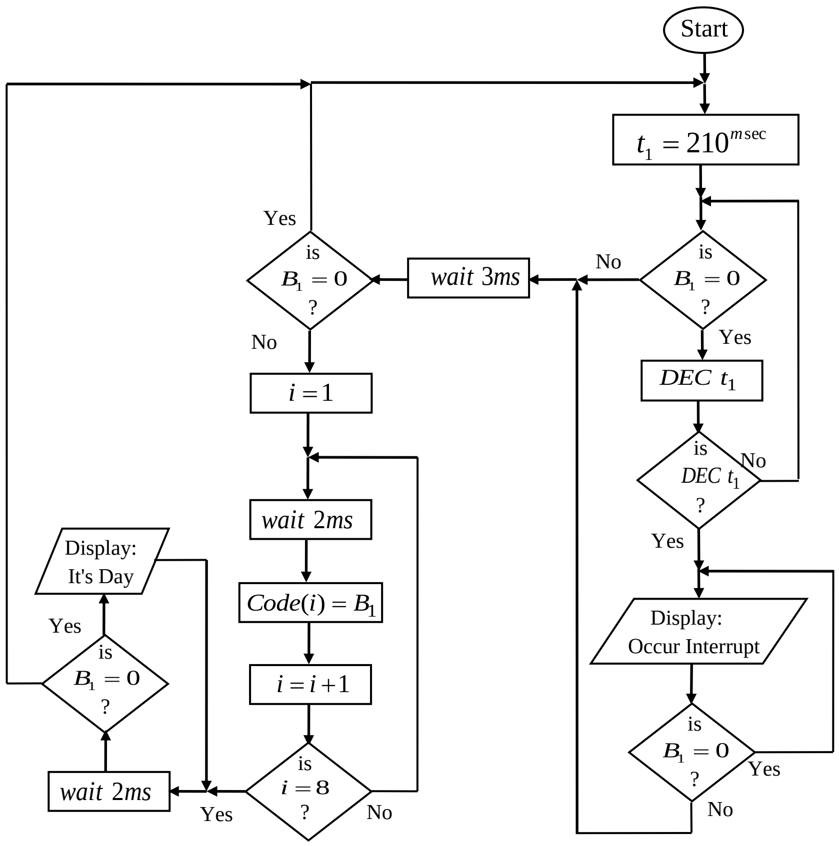


Fig. 18: System performance algorithm for display node.

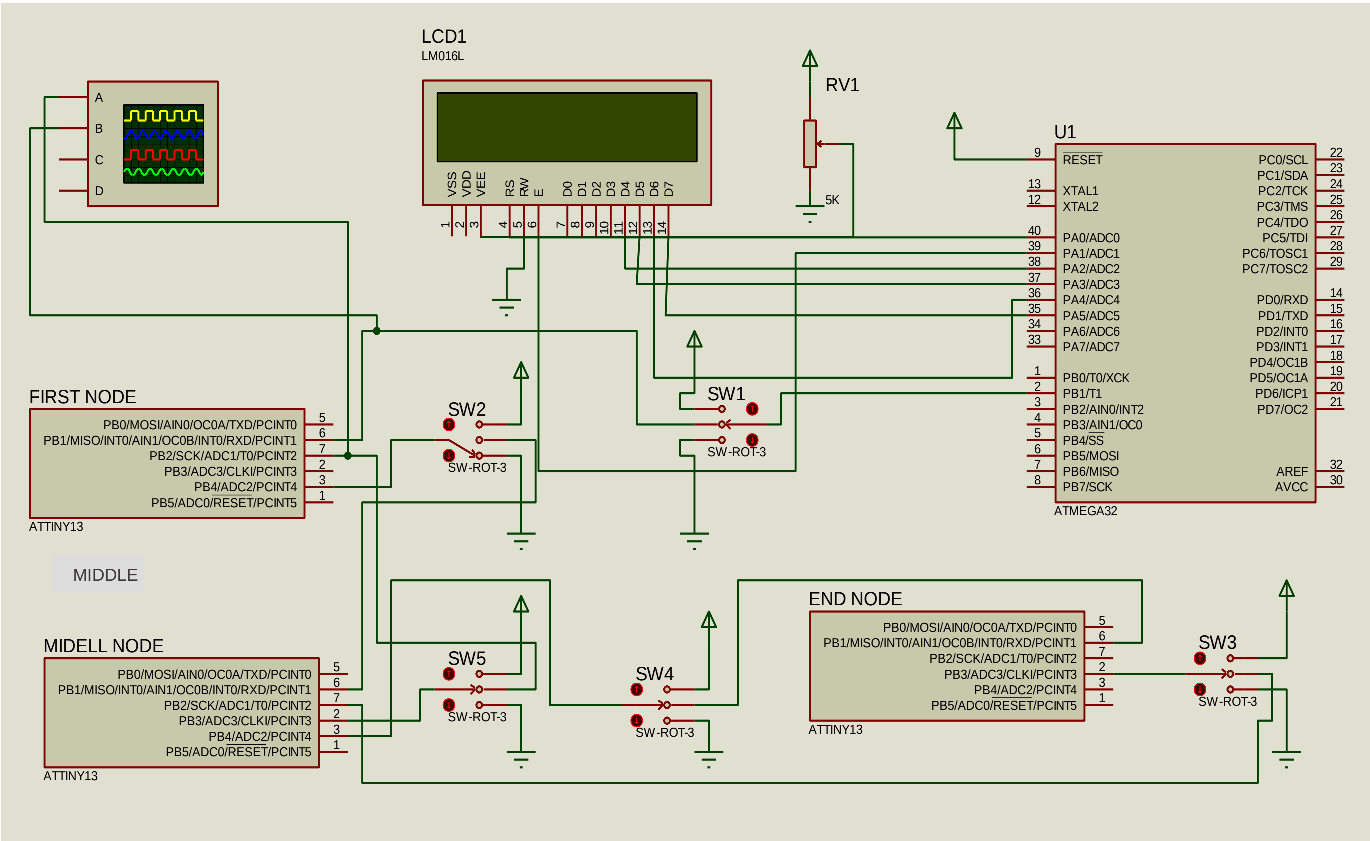


Fig. 19: System implementation in Proteus software.

3. Conclusion

This paper presented a new approach to protecting vast locations, such as large universities, military organizations, and corporations. Operator inspection, the use of barbed wire on walls and borders, and the like are used as traditional methods to protect these types of places. But they have their own problems. In this paper, a method based on optical communication based on laser light beam was presented. This system can reduce the cost of protection in the establishment and operation. This version is a new version of the enhanced protection system previously provided by the first patent author.

CRediT Authorship Contribution Statement

Rahim Ildarabadi: Conceptualization, Data curation, Formal analysis, Software, Supervision, Visualization. **Zohreh Keramat:** Formal analysis, Roles/Writing - original draft.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The ethical issues; including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, redundancy has been completely observed by the authors.

References

[1] C. Lim, A. Nirmalaths, and D. Novak, "Techniques for multichannel data transmission using a multisection infrared in millimetre-wave fibre-radio systems", *IEEE Transactions on Microwave Theory and Techniques*, vol. 47, no. 7, pp. 1351-1357, 1997

[2] H.D. Wacker, J. Borcsok, and H. Hillmer, "Redundant optical data transmission using semiconductor infrareds", in *IEEE/ACS International Conference on Computer Systems and Applications*, pp. 1040-1045, 2008.

[3] M. A. Khalighi, and M. Ugsal, "Survey on Free Space Optical Communication: A Communication Theory Perspective", *IEEE Communications Surveys & Tutorials*, vol. 16, no. 8, pp. 2281-2258, Nov. 2014.

[4] Xiaoming Zhu, and J. M. Kahn, "Free-space optical communication through atmospheric turbulence channels", *IEEE Transactions on Communications*, vol. 50, no. 8, pp. 1293 – 1300, 2002.

[5] Clint Turner. (June 28, 2011). *A 173-mile 2-way all-electronic optical contact*. Available: http://www.modulatedlight.org/optical_comms/optical_qso_173mile.html

[6] I. E. Lee, M. L. Sim, and F. W. L. Kung, "Performance enhancement of outdoor visible-light communication system using selective combining receiver", *IET Optoelectron*, vol. 3, no. 1, pp. 30-39, 2009.

[7] F. J. Lopez-Martinez, G. Gomez; and J. MaríaGarrido-Balsells, "Physical-Layer Security in Free-Space Optical Communications", *IEEE Photonics Journal*, vol. 7, no. 2, pp. 1-14, 2015.

[8] R. Ildarabadi, "Environmental protection system based on optical data communication for universities, military barracks and boundaries", I.R. Iran Patent 1396/7/3-93679, International Classification: "G06F/00; G08B 13/00; G06f 19/00"

[9] R. Ildarabadi, and Z. Keramat, "Laser based security fence to protect military and administrative organs", in *12th International Conference on Technical and Physical Problems of Electrical Engineering*, 2016, p.p. 1-6.

[10] R. Ildarabadi, and Z. Keramat, "Infrared Beam based Security Fence to Protect the Border of Cement Factory", *in 5th conference and exhibition of cement industry*, 2019.

Biography

Rahim Ildarabadi was born in Sabzevar, Iran in 1975. He received his Ph.D. degree from the Ferdowsi University of Mashhad in 2010. His main areas of interest are automation systems, electrical machine drives, renewable energy, instruments, and measurement. He is currently an Assistant Professor of electrical engineering at Hakim Sabzevari University.

Zohreh Keramat was born in Sabzevar, Iran in 1983. She received her M.Sc. degree in mechatronics at Hakim Sabzevari University, Sabzevar, Iran in 2015. Her research areas include automation systems, electrical machines, variable frequency drive, and modeling and control of systems.