ICT Focus

https://www.ictfocus.org

JOURNAL ARTICLE OPEN ACCESS

Development of Underground Perimeter Intrusion Detection System

Odgerel Ayurzana[1], Hiesik Kim[2]

[1]Department of Electronics, Mongolian University of Science and Technology, Ulaanbaatar, Mongolia

[2]Department of Electrical and Computer Engineering, University of Seoul, Seoul, Korea

e-mail: odgerel55@must.edu.mn

Abstract

An underground passive perimeter intrusion detection system employing minimal electric charge detection methodology has been developed and applied in the practical field. Existing technologies for perimeter intrusion detection systems primarily utilize active sensor types. The passive system offers several advantages, notably its immunity to electromagnetic fields since no current flows through the sensor cable, and it is considered an environmentally friendly technology. A fixed-length sensor cable is buried underground within designated security zones. A shielded telecommunication cable can be employed to detect the minimal charges generated by external intrusions. When the underground-buried sensor cable experiences deformation due to external forces and impacts, friction arises between the cable sheath and the inner copper conductor, leading to the generation of triboelectricity. The developed charge-sensitive analog device incorporates specialized hardware techniques for the detection, amplification, and processing of minimal charges. The digital module SCM employs software algorithms to assess and trigger alarms based on the system's sensitivity level. The proposed system demonstrates a dependable intrusion detection rate of approximately 96% to 97% when taking into account all installation and environmental factors.

Keywords: **Sensor cable, Alarm, Charge detection, Tribo-electric effect Detection rate**

https://doi.org/10.58873/sict.v2i1.36

Received: May 10, 2023

Accepted: November 28, 2023

Published: December 30, 2023

Corresponding author: Odgerel Ayurzana

1. INTRODUCTION

The issue of external and internal intrusion detection within factories, companies, and specialized facilities across the country has attained significant importance. The internal security systems of these entities are continuously enhancing and adapting in response to technological advancements. Concurrently, numerous companies are actively engaged in the development and implementation of perimeter intrusion detection systems. Various active sensors and technologies have been employed to ensure

the security of object perimeters [1, 2]. The study [3] provides a compendium of sensor technologies, an explanation of each technology's operating principles and applications, and integration techniques that can be used to enhance perimeter security and intrusion detection planning. The paper [4] illustrates the design of physical protection systems for nuclear materials and facilities. Underground-installed perimeter intrusion detection systems are well-suited for securing objects that cannot be physically fenced off or in cases where potential intruders don't have to be aware of the protective measures in place. In the research study documented in [5], a field-proven buried cable intrusion detection system of the new generation was developed. The study detailed in [6] investigated a buried fiber intrusion detection sensor. An effective volumetric terrain tracking system capable of reliably detecting and precisely locating intruders, whether they are walking, running, or crawling along the perimeter of objects. The benefits of underground intrusion detection systems include the following:

- Invisibility to potential intruders.
- Elimination of the need for above-ground structures.
- Reduced reliance on additional security devices like video systems, microwaves, infrared, and radars.

Various underground intrusion detection systems employing diverse technologies are currently under development and deployment worldwide. The seismic sensors are buried underground and detect and locate intrusions by recognizing vibrations in the ground. The intrusion detection system employing a leaky coaxial cable generates electromagnetic fields. The control device monitors electromagnetic fields to detect and look for changes caused by intrusions. The research presented in [7] focused on investigating the radiation pattern of a buried leaky coaxial cable. The research in [8] explored the use of buried underground fiber optic cables for border protection. The AUMI (active unbalanced Michelson interferometer) system was employed for perturbations induced by a foot stepping on a fiber cable buried underground, vibrating a netted fence, or knocking a window [9]. The central control device detects and locates intrusions by sending out signal pulses and analyzing reflections and disturbances. A perimeter intrusion detection system based on a fiber optic sensor was developed in studies [10, 11]. Intrusion localization using fiber optic sensors for the perimeter detection system was studied [12, 13]. A drawback of the fiber optic system is its demand for high installation and maintenance costs. However, it offers the advantage of precise intrusion location identification. The perimeter detection systems using wireless sensor networks are studied in [14, 15]. All the studies mentioned above used active sensors for sensing intrusion.

In this study, a practical underground passive perimeter intrusion detection system, leveraging the triboelectric effect, was meticulously developed and assessed within a real-world setting. This system stands among the world's pioneering passive underground intrusion detection systems. There is no power supply to the sensor cable. Therefore, no electromagnetic field is generated around the cable. This system represents an environmentally friendly or eco-conscious technology, with a minimal impact on the environment and wildlife. The triboelectric effect is a phenomenon in which a very small electric charge is generated when two dissimilar materials are rubbed against each other. Outdoor telecommunication cables are used as sensor elements. As the cable undergoes deformation, friction arises between the cable sheath and the inner copper conductor, giving rise to the phenomenon of triboelectricity. The charge-sensitive device plays a crucial role in detecting and amplifying extremely minute electrical charges. The sensor cable is buried underground, and when an individual of a specific weight traverses it, deformation occurs, resulting in the generation of a minuscule electric charge. The initial prototype devices, designed for the amplification of charge, noise suppression, and voltage level conversion, were developed as a result of research efforts [16].

https://doi.org/10.58873/sict.v2i1.36

The developed control device employs special hardware techniques and software algorithms to identify intruder activities within underground security zones. Deformation occurs and triggers an alarm in the monitoring application program when a person weighing more than 50 kg steps on the underground buried sensor cable. Based on the experimental results, the system's detection rate exceeds 90% during the warmer seasons. During the winter months, sensitivity was diminished as a consequence of the presence of thick snow and frozen ground. As a result, it becomes necessary to adjust the sensitivity to higher levels than what is required during other seasons.

2. SYSTEM DESIGN AND PROPOSED SOLUTION

2.1. Establishing a Security Zone

Two security zones were established by excavating the ground near the hillside. Figure 1 illustrates the underground installation of the sensor cable. The length of one security zone is approximately 150 meters. We approximated the distance of one adult step to be approximately 1 meter. Hence, the width and depth of the excavated ground for the security zones are 1 meter and 0.15 meters, respectively. As depicted in Figure 1, the sensor cable is fastened on the iron nets by 4 rows in the ground. To maintain consistent sensitivity, the sensor cable is fastened to the nets at uniform distances using metal wire. If the sensor cable is not fastened to the iron nets, heavy rains descending from the mountains during a flood may cause an elevation in water levels, potentially exposing the cable in the gaps between them. The burial depth of the sensor cable varies between 15 to 20 cm in soft, mossy, and grassy areas, and 10 to 15 cm in areas with harder rock-based terrain, depending on the specific ground conditions.

Figure 1. *Underground Sensor Cable Installation*

2.2. System Design and Architecture

The system comprises security zones, a control device, a monitoring center, a GSM modem, and a siren. Figure 2 presents the operational diagram of the core system. The control device consists of four primary components: ASM (Analog Sensing Module), SCM (Sensitivity Control Module), TCP/IP network module, and Power module. The control device can simultaneously monitor two security zones. The ASM serves as the analog component of

the control device. The ASM is responsible for detecting minimal electrical charges, amplifying them, and converting them into voltage values. The SCM functions as the digital component within the control device. The primary role of the SCM is to convert the analog signals received from the ASM into digital format. The SCM module employs specialized software algorithms to discern alarms based on sensitivity levels and subsequently transmits these alarms to the monitoring center through the TCP/IP module. Moreover, the system's sensitivity can be adjusted within the monitoring program according to the environmental conditions and the installation location's hardness. The control device is linked to a high-decibel siren and a GSM modem via output dry contacts, as indicated in [17].

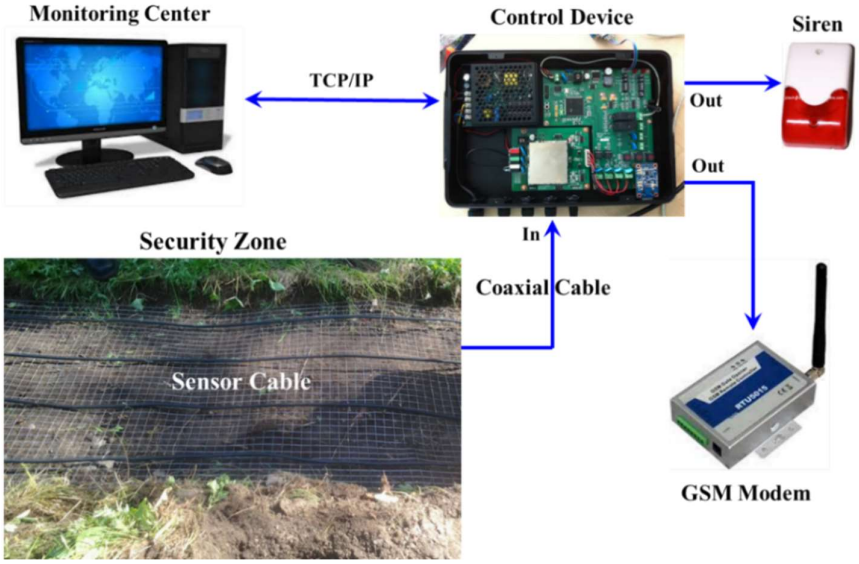

Figure 2. *Main System Diagram*

Instead of sensor elements, the system employs shielded 15-pair outdoor telecommunication cables (0.5mm x 15) to detect forces and impacts on the security zones. The sensor cable length for one zone is restricted to a range of 500-600 meters. As the sensor cable operates without a supplied power source, it can be categorized as a passive intrusion detection system.

An RG58 type of coaxial cable is utilized for transmitting small electric charges between the sensor cable and the control device. Because this type of coaxial cable has a very high input impedance, a low-noise cable must connect to the charge preamplifier input. The RG58 coaxial cable is specially treated to minimize triboelectric noise generated inside the cable due to the physical movement of the cable. The coaxial cable is required to effect electrostatic shielding around the high impedance input leads and prevent external noise pickup.

2.3. Charge Sensitive Preamplifier

The ASM comprises a charge-sensitive device, filters, voltage amplifiers, a signal-shaping scheme, and a comparator. The charge-sensitive device represents the core component of the ASM, encompassing both filters and a charge-sensitive preamplifier. Figure 3 presents a schematic diagram of a charge-sensitive preamplifier. The charge-sensitive preamplifier transforms the number of charges present on the buried sensor cable into a corresponding voltage value.

https://doi.org/10.58873/sict.v2i1.36

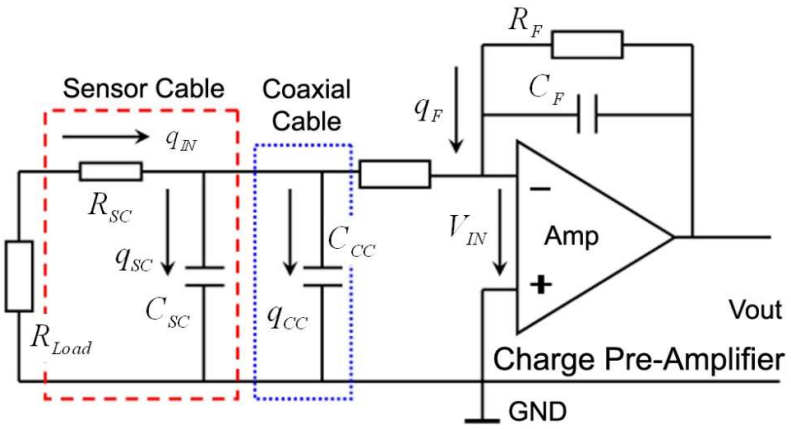

Figure 3. *Schematic of the Charge-Sensitive Preamplifier*

The input charge is expressed as the summation of the following three charges.

$$q_{IN} = q_{SC} + q_{CC} + q_F \tag{1}$$

$$q = V * C \;\rightarrow\; q_{IN} = V_{IN}(C_{SC} + C_{CC}) + V_{OUT} * C_F \tag{2}$$

where:

q_{IN} - Input charge;
q_{SC} - Sensor cable charge;
q_{CC} - Coaxial cable charge;
q_F - Operational amplifier feedback charge;
C_{SC} - Capacitance of sensor cable;
C_{CC} - Capacitance of coaxial cable;
C_F - Capacitance of operational amplifier feedback;
R_{SC} - Resistance of sensor cable;
R_{LOAD} - Constant load resistance;
R_F - Resistance of operational amplifier feedback;

In the event of deformation on the sensor cable, a non-zero voltage difference exists between the negative and positive inputs (V_{IN}!=0). The operational amplifier gain in Figure 3 is determined by Equation 3.

$$\frac{V_{OUT}}{V_{IN}} = -\frac{R_F}{R_{MAIN}} \;\rightarrow\; V_{OUT} = -V_{IN} * \frac{R_F}{R_{MAIN}} \tag{3}$$

$$R_{MAIN} = R_{LOAD} + R_{SC} \tag{4}$$

As demonstrated in equations (2), (3), and (4), the relationship between the input charge and output voltage is described by equation (5).

$$V_{OUT} = \frac{q_{IN} * R_F}{R_F * C_F - (R_{LOAD} + R_{SC}) * (C_{SC} + C_{CC})} \tag{5}$$

The other components of the ASM process (filter, voltage amplify, signal shape) output voltage and transmit it onto the SCM module.

2.4. Operating Principle of the System

The sensor cables of the security zones are connected to the control device through a coaxial cable. When intruders exert external force and impact within the underground buried

security zones, small electric charges are produced between the cable isolator and the conductors. The coaxial cable transfers the generated minimal electric charges on the sensor cable to the control device. The analog module within the control device employs specialized hardware techniques to detect, amplify, and process the minimal charges. The digital module in the control device utilizes software algorithms to assess sensitivity levels and determine alarms, subsequently transmitting these findings to the monitoring center through Ethernet. The monitoring center is responsible for verifying and documenting the alarms generated by the control device, as well as the system's operational modes, in the event of intrusions or issues within the security zones. For example, in cases where the coaxial or sensor cable is severed or experiences a short circuit, alarms are triggered in the monitoring center.

The system can provide real-time monitoring of the security zones. The inclusion of a siren and modem is aimed at enhancing the reliability and detection performance of underground intrusion detection systems. A high-decibel siren is positioned outside the secured premises, serving as a means to alert the security team in the event of alarms. A GSM modem is responsible for transmitting messages to the security team when alarms are triggered within the security zones.

It was approximated that the average weight of an individual walking within the security zones is approximately 50 kg. This system can adapt and fine-tune its sensitivity based on the ground conditions, whether it's in wetlands, swamps, or rocky terrain. The system offers manual sensitivity adjustment with a range of up to 20 steps, which can be modified on the ASM of the control device. Furthermore, sensitivity adjustments can be made through the application program located in the monitoring center. The operational algorithm of the system is depicted in Figure 4.

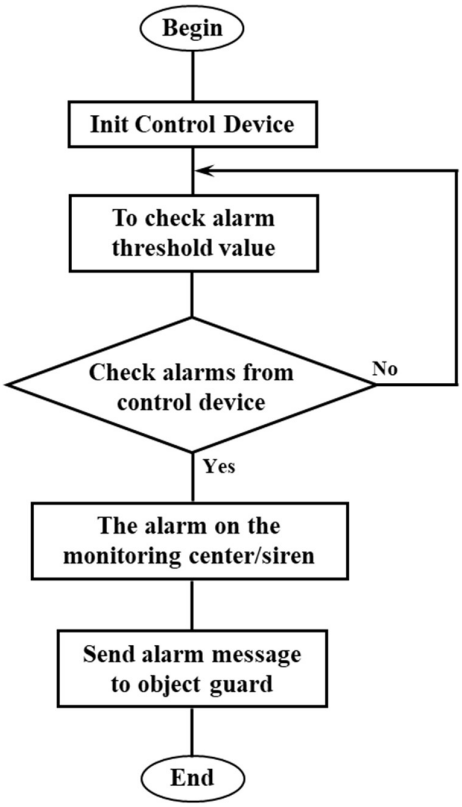

Figure 4. *System Working Algorithm*

https://doi.org/10.58873/sict.v2i1.36

3. EXPERIMENT AND FINDINGS

Figure 5 presents the input and output signal configurations when sensitivities of the control device are adjusted to higher (18th) and lower (10th) levels.

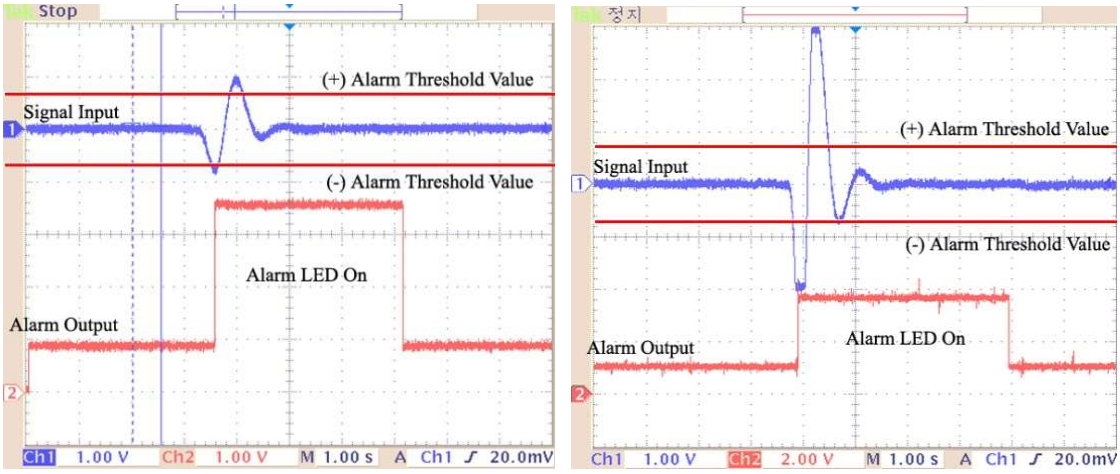

Figure 5. *Input and output signal configurations at lower and higher sensitivity*

The alarm signal, indicated by the LED turning on, is triggered when a person of average weight (approximately 50 to 60 kg) walks on the underground-buried sensor cable. The input signal (depicted in blue) is the output signal of the sensor cable as it passes through all stages of the control device, including filters and voltage amplifiers. Alarms are generated when the signal input value (depicted in blue) surpasses the predefined threshold values (represented by the red line).

Table 1 displays a selection of recorded alarms at the monitoring center during the period from July 1, 2019, to December 25, 2019.

TABLE I

Recorded Alarms on the Monitoring Program

Alarm time	Alarm zone	Alarm reason	Operator
2/7/2019 15:12	2	A herd of boar	P.Davaadorj
7/7/2019 10:36	1	Test: Normal	S.Chuluun
10/7/2019 15:05	1	A herd of deer	G.Olzii
13/7/2019 12:04	2	A stone rolled down from the mountain	S.Chuluun
15/7/2019 02:12	1	Test: Normal	P.Davaadorj
21/7/2019 16:41	2	A wild boars	B.Shinebayar
28/7/2019 12:19	1	Test: Normal	B.Shinebayar
12/8/2019 11:00	2	Test: Normal	G.Olzii
19/8/2019 12:00	1	A lost person	B.Shinebayar
30/8/2019 14:06	2	Test: Normal	B.Shinebayar
12/9/2019 13:24	1	A herd of deer	G.Olzii
21/9/2019 17:17	2	Test: Normal	P.Davaadorj
28/9/2019 10:18	2	A herd of boar	B.Shinebayar
11/10/2019 10:18	1	The squirrel cut the cable	G.Olzii
5/11/2019 12:33	1	Test: Normal	S.Chuluun
10/11/2019 02:11	2	Alarm with an unknown cause	P.Davaadorj
16/11/2019 11:05	2	Test	G.Olzii
24/12/2019 11:05	1	Test: No alarm, the ground froze, increased sensitivity	B.Shinebayar

As evident from the recorded alarms, when the sensitivity is set to the 18th level (maximum being the 20th), alarms are triggered even by the presence of small animals such as wolves

and foxes entering the underground security zones. An alarm can be activated when an intruder enters the underground security zone with a weight of less than 50 kg. Hence, sensitivity is typically set to the 13th or 14th level during the summer, fall, and spring seasons. The sensitivity of the underground security zones is lowered when the ground is frozen, as indicated by the environmental conditions. Therefore, during the winter season, the sensitivity is adjusted to higher levels, typically the 18th or 19th level.

Alarms are registered at the monitoring center when larger animals like wild boars and deer access the security zone during nighttime. A cable break alarm was triggered due to a squirrel cutting the coaxial cable. In instances of heavy rain and water descending from the mountain, the buried cable was exposed and struck by a stone rolling down the mountainside, resulting in an alarm activation. Moreover, individuals who have lost their way within the forest have unintentionally entered the security zone. In these scenarios, the system has functioned as expected.

The sensitivity is reduced due to the thickness of snow within the security zones. In December and January, when the ground was frozen, there were instances where the alarm did not activate even when the sensitivity of the control device was set to 14th. Hence, during winter, it becomes necessary to increase the sensitivity to levels higher than what is required during other seasons. Out of the 100 alarms recorded during 6 months, it was found that 3 to 4 of them were classified as potential false alarms, as the exact cause of the alarm could not be conclusively determined. As a result, the intrusion detection rate for the system was estimated to be approximately 96% to 97%. Figure 6 displays a screenshot of the monitoring program for the intrusion detection system.

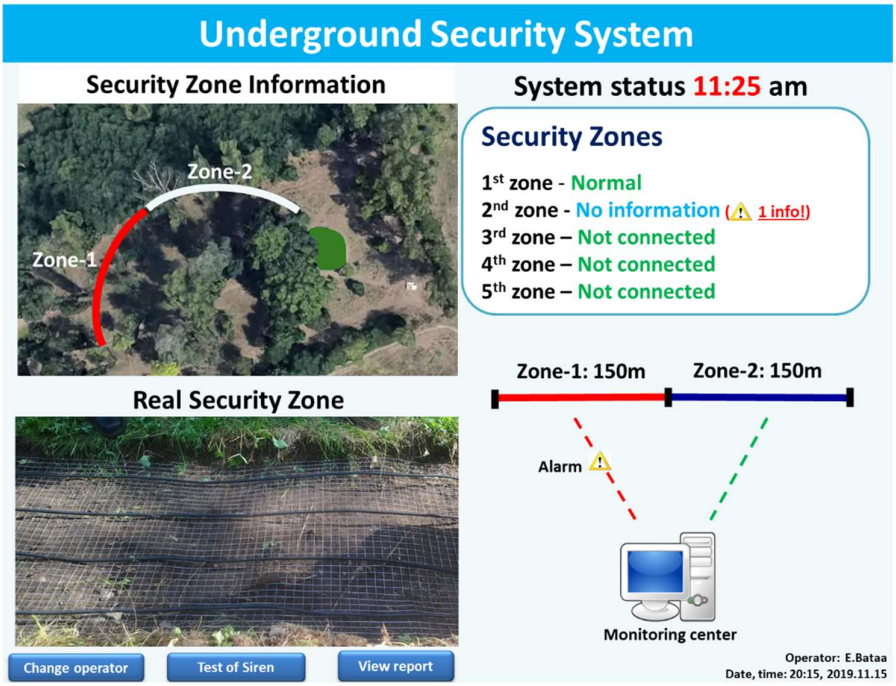

Figure 6. *Screenshot of the Monitoring Program*

Log data, including alarms and control device modes, are stored within the monitoring center. The monitoring program acquires real-time zone information from the control device. The monitoring center displays all the available information. This information includes alarms related to intruders, cut or short-circuited sensors and coaxial cables, as well as instances where the control device cover is opened. Data reports are accessible in various formats and can be both viewed on-screen and printed. Furthermore, it is possible to activate or deactivate the alarms for each specific zone within the system. In this study, the operator manually

inspects and records the reasons for the alarms. Hence, it is necessary to incorporate cameras into the system to verify the cause of the alarms. A perimeter intrusion detection system is designed to identify the presence of an unauthorized object within a safeguarded outdoor area over a specified timeframe, incorporating the use of a camera [18]. Paper [19] introduces the use of Fourier Descriptor (FD) and Histogram of Oriented Gradients (HOG) techniques to achieve effective detection of human bodies in various postures captured by stationary cameras. The perimeter intrusion detection algorithm utilizes image-based features to differentiate between genuine objects and moving vegetation or other potential distractions [20]. Our plan involves integrating cameras with the intrusion system to visually monitor the intrusion zones for alarm verification.

4. CONCLUSIONS

The underground passive perimeter intrusion detection system, utilizing minimal charge detection technology, has been created and tested for the first time under specific weather conditions. The developed charge-sensitive device leverages specialized algorithms for the detection, amplification, and processing of the minimal charges generated. The digital module within the control device makes use of software algorithms to identify alarms contingent on the sensitivity level. This system is particularly well-suited for securing objects in environments where constructing a physical fence is unfeasible due to challenging environmental conditions. The experiment results reveal that the sensor cable is buried at a depth of 15 to 20 cm in softer areas with moss and grass, and at a depth of 10 to 15 cm in areas with harder, rocky ground, depending on the specific soil conditions. The system is capable of triggering an alarm when an intruder with a weight of less than 50 kg enters the underground security zone. A high-decibel siren is positioned outside the secured premises to sound alarms and alert the security team. A GSM modem is used to relay alarm messages to the system operator, informing them of the intrusion. The recorded findings indicate that the intrusion detection rate is around 96% to 97% during the summer, fall, and spring seasons. Certain alarms are triggered when a group of wild boars and deer enter the security zones during the nighttime. Additionally, alarms occurred when individuals who had lost their way in the forest unintentionally entered the security zone. During the winter season, sensitivity levels decreased due to the thickness of the snow in the security zones. In December and January, during frozen ground conditions, there were instances where alarms did not activate unless the sensitivity was adjusted to its highest level. As a result, it becomes necessary to raise the sensitivity to higher levels during winter than in other seasons. In the future, our plan includes integrating cameras into the system to visually monitor the intrusion zones for alarm verification. Furthermore, we need to research to enhance sensitivity during the winter season.

REFERENCES

[1] NISE East Electronic Security Systems Engineering Division "Perimeter Security Sensor Technology Handbook" North Charleston, South Carolina, 1997.

[2] Garcia, L. Mary "The Design and Evaluation of Physical Protection Systems" Woburn, MA: Butterworth-Heinemann, 2001, https://doi.org/10.1016/C2009-0-25612-1

[3] Defense Advanced Research Projects Agency (DARPA) and The National Institute of Justice (NIJ) "Perimeter Security Sensor TechnoLogies Handbook" National Criminal Justice Reference Service (NCJRS), 1998

[4] IAEA Nuclear Security Series "Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities" International Atomic Agency Vienna, 2021.

[5] Southwest Microwave "Buried cable intrusion detection system", System Introduction, Jul 2019.

[6] Jeff Bush, Carol A. Davis, Pepe G. Davis, Allen Cekorich, and Fred P. McNair "Buried Fiber Intrusion Detection Sensor with Minimal False Alarm Rates", Proc. SPIE 3860, Fiber Optic Sensor Technology and Applications, Dec 1999, https://doi.org/10.1117/12.372970

[7] N. Blaunstein, Z. Dank, and M. Zilbershtein "Prediction of Radiation Pattern of a Buried Leaky Coaxial Cable" Springer, Subsurface Sensing Technologies and Applications, Vol. 1, No. 1, 2000. DOI: 1566-0184/00/0100-0079

[8] Suleyman Alpay Aslangula "Detecting Tunnels for Border Security based on Fiber Optical Distributed Acoustic Sensor Data using DBSCAN" 9th International Conference on Sensor Networks March 2020, DOI: 10.5220/0008869600780084

[9] Hsin Hsieh, Kai-Shuo Hsu, Tai-Lang Jong, and Likarn Wang "Multi-Zone Fiber-Optic Intrusion Detection System with Active Unbalanced Michelson Interferometer Used for Security of Each Defended Zone" IEEE Sensors Journal, Vol. 20, No. 3, Feb 2020. DOI: 10.1109/JSEN.2019.2946904

[10] Qiwen Zeng, Jianfeng Tao, Sajun Guo, Huiliang Ge "Target detection method based on optical fiber fence" Journal of Physics 2019. DOI: 10.1088/1742-6596/1237/2/022149

[11] Xiaolei Li, Qizhen Sun, Jianghai Wo, Manliang Zhang and Deming Liu "Hybrid TDM/WDM-based Fiber-Optic Sensor Network for Perimeter Intrusion Detection" Journal of Lightwave Technology, Vol. 30, No. 8, pp.1113-1120, April 2012. DOI: 10.1109/jlt.2011.2170401

[12] Mieczyslaw Szustakowski and Marek Życzkowski "Fiber optic sensors for perimeter security with intruder localization" Congress on Optics and Optoelectronics, Sep 2005, Poland". DOI: https://doi.org/10.1117/12.622776

[13] Marek Zyczkowski "Intruder localization and identification in fiber optic systems" Conference on Optics and Photonics for Counterterrorism and Crime Fighting IV, Oct 2008. DOI: 10.1117/12.800076

[14] Cai Xia Liu, Fang Yi Xie "A Perimeter Intrusion Detection System (PIDS) Based on Sensor Network" Applied Mechanics and Materials Vol. 568, No. 570, pp. 468-472, June 2014. https://doi.org/10.4028/www.scientific.net/AMM.568-570.468

[15] Yuheng Liu, Chao Li, Yang He, Jing Wu, and Zhang Xiong "A Perimeter Intrusion Detection System using Dual-Mode Wireless Sensor Networks" Second International Conference on Communications and Networking, China, pp.861-865, 2007, DOI: 10.1109/chinacom.2007.4469520

[16] Odgerel Ayurzana and Hiesik Kim "Minimal Electric Charge Detection Device for Perimeter Security System" Journal of Electrical Engineering, David Publishing, USA, Volume 5, Number 6, Nov-Dec 2017. DOI: 10.17265/2328-2223/2017.06.005

[17] Hiesik Kim and Odgerel Ayurzana "Reducing False Alarms Caused by Wind Effect in Automatic Security Perimeter System" ESCS-2016, Las Vegas, USA, Jul 25 – 28, 2016. ISBN: 1-60132-433-2, CSREA Press ©

[18] Devashish Lohani, Carlos Crispim-Junior, Quentin Barthélemy, Sarah Bertrand, Lionel Robinault and Laure Tougne Rodet "Perimeter Intrusion Detection by Video Surveillance: A Survey" MDPI, Sensors May 2022. DOI: https://doi.org/10.3390/s22093601

[19] Zhang Y.L, Zhang Z.Q, Xiao G, Wang R.D, He X "Perimeter intrusion detection based on intelligent video analysis" IEEE Conference ICCAS-2015, Busan, Korea, 13–16 Oct 2015. DOI: 10.1109/ICCAS.2015.7364811

[20] Vijverberg J.A, Janssen R.T, Zwart R, With P.H "Perimeter-intrusion event classification for on-line detection using multiple instance learning solving temporal ambiguities" IEEE Conference ICIP-2014, Paris, France, 27–30 Oct 2014. DOI: 10.1109/ICIP.2014.7025487

BIOGRAPHIES

Odgerel Ayurzana received B.S. and M.S. degrees in Computer Hardware Engineering from the Mongolian University of Science Technology (MUST) in 2000 and 2002, respectively. Also, he received his Ph.D. in Electrical and Computer Engineering Department University of Seoul, Republic of Korea. Currently, he is working as head of the Electronics Department in the MUST. His areas of research include sensor networking, sensor application, and embedded systems.

https://doi.org/10.58873/sict.v2i1.36

Hiesik Kim received a bachelor's degree in Mechanical Engineering at Seoul National University in 1977. And a master's degree in Production Engineering at KAIST (Korea Advanced Institute of Science and Technology) and a Ph.D. degree in Production Engineering at Stuttgart University, Germany, in 1987. He worked as a technical official at the Ministry of Science and Technology of the Korean Government (1979-1982) and then as a Senior Researcher, at the CAD/CAM Research Lab at KIST (Korea Advanced Institute of Science Technology) (1987-1989) and he is now a Professor at the Department of Electrical and Computer Engineering of University of Seoul since 1989. His research areas are the optical measurement of geometries, applications of sensors for automation, and image processing.