Scientific African 12 (2021) e00819

Contents lists available at ScienceDirect

Scientific African

journal homepage: www.elsevier.com/locate/sciaf

Manhole intrusion detection system with notification stages

Felix Mazunga[a,*], Tawanda Romosi[a,b], Rosemary Guvhu[c]

[a] Applied Physics and Telecommunications Department, Midlands State University, P. Bag 9055, Gweru, Zimbabwe
[b] TelOne, Highlands Exchange, 29 Alexander Road, Harare, Zimbabwe
[c] Educational Foundations Department, Midlands State University, P. Bag 9055, Gweru, Zimbabwe

ARTICLE INFO

Article history:
Received 24 November 2020
Revised 31 May 2021
Accepted 4 June 2021

Editor: DR B. Gyampoh

Keywords:
Intrusion detection
Manhole cover
Copper theft
Critical infrastructure protection
Arduino Uno
GSM

ABSTRACT

Appropriate design of intrusion detection systems is extremely important to safeguard critical and valuable infrastructure. Telecommunications companies (TELCOs) and electric power utilities are experiencing an increased rate of rampant underground copper cable theft and vandalism. This paper addresses the important subject of combating the physical intrusion of critical infrastructure by proposing a low-cost, effective and unique manhole intrusion detection system. Manholes are openings to confined underground spaces that are used to access critical underground infrastructure and utilities such as sewer systems, electricity and telecommunication networks for maintenance and inspection. Critical infrastructure protection is very essential to avoid losses and incapacitations that would have a debilitating effect on economic activities, security, public health and safety, and so on. The increasing rate of rampant copper theft and vandalism could be attributed to the increased demand and high prices for copper on the black market. Critical infrastructure sectors such as TELCOs, electricity supply, water and rail transport are utilizing intrusion detection systems that only trigger an alarm when the critical infrastructure has already been vandalized or stolen. In this paper, we propose a low-cost and unique manhole intrusion detection system with notification stages devoted to safeguard critical infrastructure. Simulations of the system were performed before hardware implementation. The proposed system utilizes an Arduino Uno microcontroller and multiple sensors to trigger the intrusion stages early before the copper cables are vandalized. Due to the inclusion of three different additional sensors, the proposed system has an advantage of timely or early-stage intrusion detection. The response time is improved since the first alert is sent early before the actual cutting of the cable. The GSM messaging system is utilized as the alert mechanism during the intrusion stages. Notifications are also displayed on a local LCD.

Introduction

Appropriate design of intrusion detection systems is extremely important to safeguard critical infrastructure from vandalism and theft [38]. Most developing countries in the world are experiencing an increased rate of rampant underground

* Corresponding author.
E-mail address: mazungaf@staff.msu.ac.zw (F. Mazunga).

https://doi.org/10.1016/j.sciaf.2021.e00819

copper cable theft and vandalism [10,7,42,28,25]. Theft and vandalism of critical and valuable infrastructure would have a debilitating impact on the economy and disrupt essential services in our daily lives [37]. Copper cables are extensively utilized by telecommunication operators, electric power utilities, municipalities and railway control systems to provide essential services [11,7,37]. These cables are usually installed underground in urban areas.

Manholes are openings to confined underground spaces that are used to access critical underground infrastructure and utilities such as water, sewer systems, electricity and telecommunication networks [35] for the purpose of maintenance and inspection. As compared to overhead lines, underground copper cables are less susceptible to adverse environmental conditions such as heavy rainfall, lightning, floods, whirlwind and thunderstorms [43,4]. With the ever increasing downtime and huge loss of potential revenue being experienced by Telecommunications companies (TELCOs) due to stolen and vandalised underground cables, proper design of intrusion detection systems is critical.

Besides physical intrusion by humans, some of the critical infrastructure like data communication networks are also vulnerable to cyber-attack or malicious events [9,31]. In literature, intrusion detection systems for monitoring various critical infrastructure include those based on Internet of Things (IoT), edge computing, Arduino, Raspberry Pi, programmable interface controller (PIC) microcontroller and machine learning [15,26,33], (Mulyanto et al., 2021). Machine learning-based intrusion detection systems are frequently utilized to detect cyber-attack or anomalous activities in networked systems [2], (Mulyanto et al., 2021), [9,31]. In spite of all the improvements in machine learning-based intrusion detection techniques, new malicious violations continue to emerge as a result of the ongoing rapid technological advancements (Mulyanto et al., 2021). Considering physical intrusion by humans, a notable number of the existing systems focus on underground cable fault detection while very few are devoted to manhole intrusion detection. Moreover, these monitoring systems mostly rely on a single sensor to detect an anomaly thereby increasing the rate of occurrence of false alarms. An intelligent manhole cover should have self-monitoring capabilities and provide real-time notifications about its status [15]. Intrusion detection systems that enable timely detection and response to manhole intrusions are of paramount importance [5]. Therefore, we propose an effective and affordable Arduino-based manhole intrusion detection system that incorporates three different additional sensors for triggering real-time notifications for various stages of intrusion. The GSM (Global System for Mobile Communications) infrastructure for sending alerts is already deployed in many countries [20]. GSM can co-exist with LTE (Long Term Evolution) and other new technologies like “Narrow Band IoT” (NB-IoT) [23,22].

The significant rise in copper cable theft cases is often attributed to the increased demand and prices of copper on the black market [39,42]. In the year 2020 alone, a loss worth several millions of dollars due to copper theft and vandalism was reported by a major telecommunication service provider in Zimbabwe [25]. Manholes are generally found in urban areas under sidewalks, by the road sides of trunk routes, and even under city buildings. The manholes are protected by covers or lids to prevent accidental or unauthorised access as shown in Figure SM1. Contrary to the objectives of smart cities, displaced, stolen or damaged manhole lids may cause accidents when pedestrians and motorists fall into the uncovered holes [15]. Traditionally, these covers are made of heavy metal which requires a lot of effort to be lifted. In an attempt to increase security of the manholes, the lids are weld-shut. However, the reinforcement of the manhole lids is proving ineffective as the thieves are now utilizing power tools to open up the manholes as shown in Figure SM2. Manholes are placed at every 150 m to 250 m stretch depending on the terrain.

The existing cable alarm systems in Zimbabwe only notify the security team after the cable has already been cut. This implies that the criminals would have vandalized the reinforced manhole lids to gain access to the underground cables. Service restoration may be delayed depending on resource availability. Therefore, effective manhole intrusion detection systems that enable timely detection and response to manhole intrusions should be developed to avoid loss of potential revenue, network service, customer and investor confidence as a result of copper cable theft and vandalism.

In this paper, we propose a cheap and unique manhole intrusion detection system that notifies security teams of four various stages of vandalizing the telecommunication infrastructure in order reduce copper cable theft. The contributions of this paper are summarized as follows.

- A new flowchart representing the new algorithm for implementing an intrusion detection system
- Due to the inclusion of three different additional sensors, the proposed system performs timely or early-stage intrusion detection. The response time is improved since the first alert is sent to the response team early before the actual cutting of the cable.
- The system first immediately notifies the rapid response team upon detecting vibrations caused by the tools during cutting of the manhole lid. A vibration sensor is utilized to detect vibrations caused by the cutting tools.
- The rapid response team is alerted if the manhole lid is opened. An ultrasonic sensor detects the opening up of the manhole lid.
- The security team is then alerted when an access into the manhole has been detected before vandalism of the cable itself. Human movement in the manhole is detected by a passive infrared (PIR) sensor. The proposed system notifies the security team in time before the actual cutting of the telecommunication cables.
- Finally, if the cable is cut, another notification is sent to the security team. Cable loop break is detected by a current sensor.
- The sensors are connected to the Arduino-Uno which sends notifications at every stage of vandalism via the GSM SIM 800 L module. An LCD for local display of the notifications is also utilized in our system. The incorporation of multiple sensors limits false alarms.

The rest of this paper is organized as follows. Section 2 highlights some of the related work. Section 3 presents details of the proposed system. Results are provided in Section 4. Finally, Section 5 concludes the paper.

Literature review

[29] proposed a cable fault monitoring system. Although it is a highly creative concept, the implementation of a frequency detector provides an avenue for signal noise causing false readings under certain conditions as well as having multiple points of potential error. [27] developed a cable theft monitoring system (CTMS) using a GSM modem, a programmable interface controller (PIC) microcontroller system, a voltage divider, a temperature sensor and several other peripherals. The system was aimed at alleviating the issues of cable theft experienced by Telekom Malaysia despite their adoption of several other ultimately futile measures. These included prevention campaigns at national level, security patrols, greasing telecommunication poles, replacing existing cable with fiber and proprietary systems, all at great cost. In addition to being costly, another challenge of the authors' proposed system is that it is relatively bulky in comparison to the proposed system of our current work.

The system proposed by [27] was later modified by another group of engineers [7] with Nazri being involved again. The authors improved the system's sensitivity and accuracy in detecting temperature changes specifically associated with faults or breaks caused by theft. The authors only introduced minor changes in the code, detection algorithms and choice of temperature sensors used. A 99% efficiency and detection success rate of the improved system was reported. However, there is too little evidence to corroborate this claim. [8] presented a system for detecting theft of both conductive and non-conductive cables. The system is comprised of a GPRS module, ZigBee module, Power Line Carrier (PLC) and four cameras. However, such a system is expensive and cameras may also be vandalized. Moreover, notifications are only sent when the cable has already been cut. (Sulaiman et al., 2016) proposed a GSM based system for preventing theft of copper cables. The system relies on a single vibration sensor and was specifically designed for overhead copper cables. Chances of false alarms due to birds are high in this system.

Norizan was again instrumental in another system proposed by [18] that utilized the detection of voltage drops in copper cables to ascertain and locate cable thefts, failures and breaks. The system utilized an SK40C microcontroller with a microchip PIC16F877. However, the presence of the SK40C at multiple detection points creates a point of weakness in that the system can be re-programmed if the intruders have sufficient knowledge of the PIC being used. The intruders may manipulate the code to ignore any voltage drops or inconsistencies. Moreover, the system would cost more due to the cost of the SK40C plus the PIC and GSM modules at multiple points.

A system for monitoring manhole covers by utilizing "edge computing" was demonstrated by [15]. Edge computing is a recent technology that employs both IoT and cloud computing [40]. This technology has an advantage of improved response time which is a key factor for critical applications requiring real-time monitoring. The proposed system was aimed at reducing accidents due to damaged, displaced or stolen manhole covers in central business district (CBD) areas. All the covers had the capability to transmit sensed data to a common server. The system was tested several times on 20 manhole covers and one of the challenges observed by the authors was the offline state of some of the covers due to hardware issues and intermittent internet connectivity of the adopted "Narrow-Band IoT (NB-IoT)" (3 [45]) communication module.

A GSM-based system for detecting vandalism of an oil pipeline was presented by [1]. The authors utilized a single piezoelectric disk sensor for detecting vibrations on the pipe. In this system, chances of false alarms are high since animals and other environmental conditions can cause vibrations. In addition, implementation of the system becomes costly since it requires installation on the pipe after every two meters. [19] proposed a field programmable gate array (FPGA) based system for monitoring the tampering of critical infrastructure cables. The system detects a change in the capacitance of a cable when there is a short circuit or open circuit. Besides being bulky, the system only sends an alert message when a cable has already been cut or vandalized.

IoT-based systems that utilize Ohm's Law for detecting the exact locations of underground cable faults were recently proposed by [41,26,16]. An IoT-based system that relies on the "Murray loop" method to locate underground cable faults was presented by [13]. However, these recently proposed IoT-based systems would raise an alert after an open circuit or the actual cable cutting has occurred. [38] presented an improved machine learning-based intrusion detection system for protecting IoT network infrastructure from intruders. According to the authors, the issues of network latency and overhead associated with the popular "centralized (cloud-based)" intrusion detection systems were minimized by employing distributed and semi-distributed approaches. An improved intrusion detection accuracy was reported by the authors. A system for detecting physical intrusion of critical infrastructure by both drones and humans was presented by (Zhang et al., 2020). The cameras utilized by the authors are expensive and therefore attract attack by criminals.

An Arduino-based system for detecting vandalism of oil and gas pipelines was demonstrated by [30]. Their system relies on geophones to detect seismic waves due to digging and drilling activities. However, the detection units are installed 200 m apart thereby reducing the detection accuracy. The system does not detect and report the presence of humans who are running or walking. The algorithms utilized by the authors consider running and walking as "non-threatening" activities. An intrusion detection system targeting "advanced metering infrastructure" in smart grids was proposed by [44]. The system leverages on the aggregation of "convolutional neural networks" and "long short-term memory" networks. The authors reported an improved accuracy in detecting abnormal information in the network. A network-based intrusion detection system for detecting cyber-attack by considering the sequential nature of traffic data was proposed by [31]. According to the authors

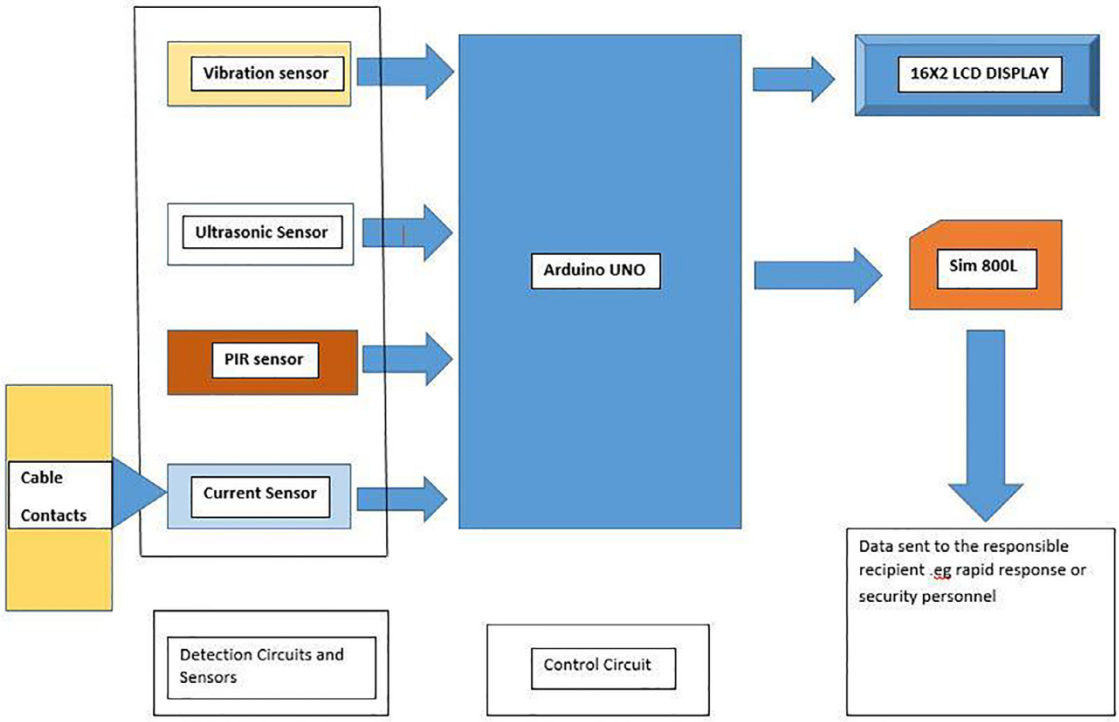

Fig. 1. Block Diagram of Proposed System.

in (Mulyanto et al., 2021), machine learning and deep neural networks often experience high "false-positive" alarm rates and reduced chances of threat detection. Besides, computational overheads are also introduced by the complex algorithms in an attempt to improve detection accuracy.

Most of these recently proposed systems focus on detecting cyber-attack and cable faults in different networks. Also, the existing intrusion detection systems for cable theft prevention and underground cable fault location rely mainly on a single sensor thereby increasing the chances of false alarms. The additional huge storage and processing capabilities possessed by some systems reviewed above are not needed for our intended application (manhole intrusion detection) and therefore add unnecessary costs [17,6,34]. Also, considering cost-effectiveness, the Arduino Uno board utilized in this proposed work is currently available at an affordable price of £20 each [3]. The prices of Arduino boards vary according to the version [3]. In this paper, we propose an inexpensive and unique manhole intrusion detection system that detects physical intrusion by humans.

Our proposed system is superior since it utilizes four sensors to detect four different manhole intrusion stages and thereby facilitate timely intervention by the response team before the actual cutting of the cable. The system enables timely detection and response to manhole intrusions. GSM messaging system is used for alerting the security team.

Material and methods

System description

Our proposed unique manhole intrusion detection system in Fig. 1 utilizes an Arduino Uno microcontroller and multiple sensors to trigger the intrusion stages before the copper cables in a manhole are tempered with. Due to the inclusion of three additional sensors, the proposed manhole intrusion detection system has an advantage of enabling timely or early-stage intrusion detection. The Arduino Uno board is based on the ATmega328 microcontroller. It incorporates "14 digital input/output pins, 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, a reset button, 32 kB flash memory, 2 kB SRAM and 1 kB EEPROM" [24]. The Arduino was utilized for our purpose due to reasons that include the following. The intended application of the proposed system does not demand added processing and storage capabilities that are found in other higher-priced platforms [6,34]. Computation-intensive algorithms are not utilized in our proposed system. Arduino is also capable of detecting the environment by accepting input from a variety of sensors and can trigger different actuators. It is an open-source hardware/software platform that does not need an external hardware programmer to upload

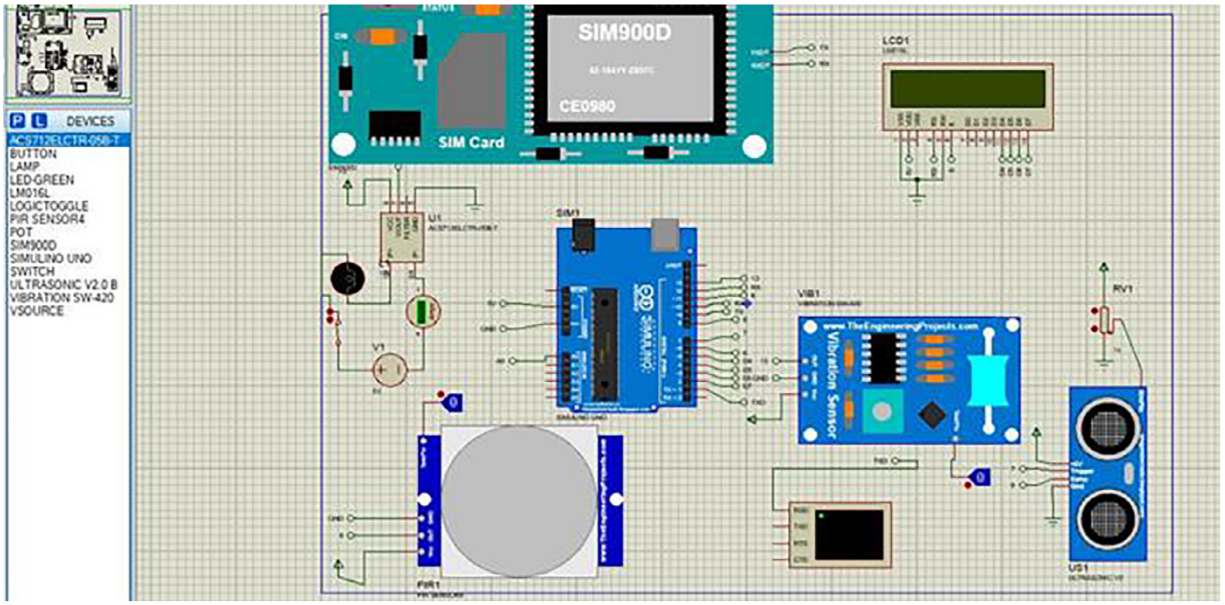

Fig. 2. Schematic presentation of the proposed system in Proteus.

new code [21]. In spite of having an affordable price [14,3], an Arduino is easily programmable and is suitable for rapid prototyping [17,21].

The system monitors manholes by employing multiple sensors namely vibration sensor, ultrasonic sensor, PIR sensor and the current sensor. Any form of triggering of the sensors indicates a breach in real time which will be reported via the GSM module SIM 800 L to a designated rapid response contact. The response time is improved since the first alert is sent early before the actual cutting of the cable. The new system flowchart shown in Figure SM3 was used for developing a new algorithm for the code used in our proposed system.

The system notifies the designated recipient in stages. The vibration sensor detects the forceful opening of the manhole lid. Once the sensor input is detected as "High", a notification message is wirelessly communicated to a designated rapid response recipient via the GSM module. The local LCD displays updates on the status of ongoing activities during all intrusion stages. The next stage is triggered by the ultrasonic sensor which is positioned facing the lid. When the distance between the ultrasonic sensor and the lid in front of it increases, it means the manhole lid has been opened. A notification is sent via the GSM module sim 800 L to the designated recipient. The next stage of notification is triggered by the PIR sensor that detects movement within the manhole when entry has been gained. An alert message is also sent via the GSM module to the designated recipient and the LCD display is updated. The last notification stage is triggered by the current sensor when the current in the copper cable loop falls to zero. This indicates that the cable has been damaged or vandalized and an alert message is also sent. The notification stages are essential because they provide an update of the activities occurring in real-time so as to significantly reduce the massive copper cable thefts.

System block diagram

Fig. 2

Positioning of sensors

The vibration sensor is responsible for detecting shocks on the manhole lid as the forceful entry is in progress. The sensor is mounted near the lid to detect the impact as indicated in Figure SM4. The ultrasonic sensor is positioned on the same bracket mount that holds the vibration sensor whilst facing the lid so that the distance between the ultrasonic sensor and the lid is monitored. The current sensor is positioned within the unit in order to detect the current flowing through the cable. The PIR sensor is strategically positioned at the front of the unit so as to detect human movements once entry into the manhole has been gained.

System simulation

The project simulation was performed using "Proteus 8 Professional" software. It is a simulation and design software tool that possesses 2D CAD drawing features among other tools. The software was developed by Lab Center Electronics for electrical and electronic "from concept to completion" circuit design. It facilitates the drawing of schematics and simulation

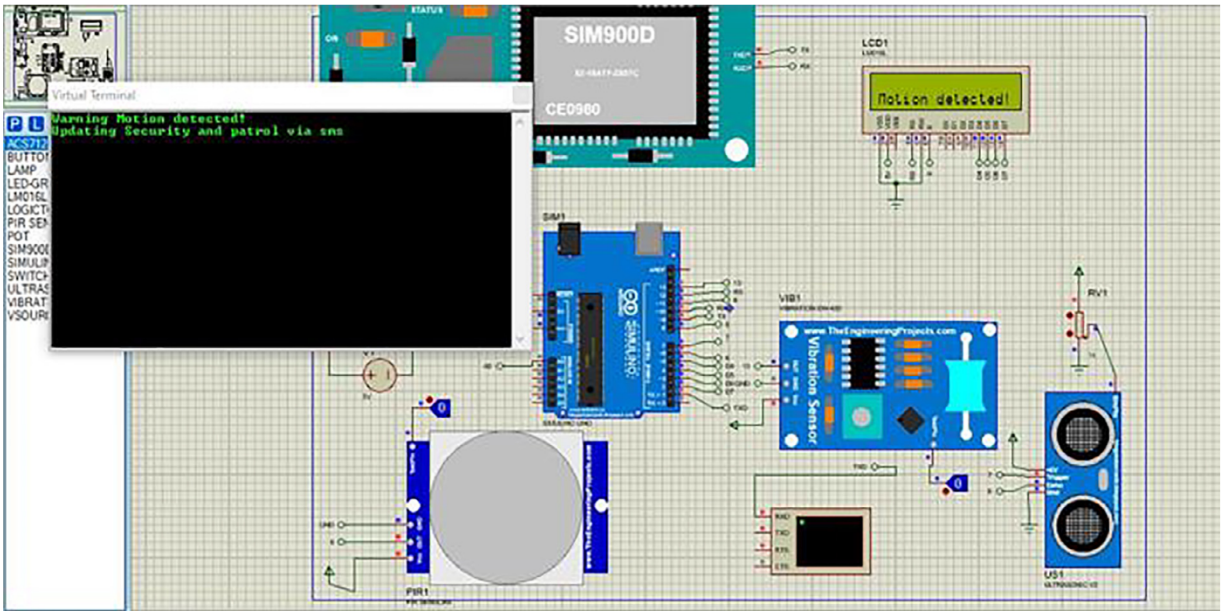

Fig. 3. Simulation of motion sensor.

of data logger system in real time. Proteus constitutes libraries with a wide range of components and analysis tools like Arduino boards [32], GSM modules, and virtual terminals.

Schematic representation of simulated system

A schematic presentation of our proposed system was done using Proteus 8 simulation tool as shown in Fig. 2.

System coding

During the coding phase of the Arduino board, *C++* language [36] was used in this proposed project. The code of the whole system was built by integrating the separate programs written during the stage of testing the individual components with the microcontroller and a few modifications were done. A snapshot of the code is shown in Figure SM5. As for the code's functionality, the SMS messaging system was implemented because of its simplicity and it takes less time to program. Besides, GSM messaging system is often utilized as an alert mechanism in intrusion detection systems due to its affordability, reduced latency, wide spread coverage capabilities and so on, enabling the system to be online for almost all the time [12].

Results and discussions

Simulation results

The system was simulated with Proteus 8 Professional as shown in Fig. 3. The simulation of the vibration sensor behaved as expected. When an impact was detected by pushing the toggle switch, the system initiated the notification sequence. The ultrasonic sensor was simulated using a 5 V source and a variable resistor as the trigger input as shown in Figure SM6. When the HG-POT was tuned upwards, it represented an increase in distance from the sensor to the lid. This triggered an SMS notification sequence. The motion sensor was simulated using a toggle switch. When an input was applied to the toggle switch, an SMS notification was sent.

Hardware implementation of the system

Hardware testing of the system was done on a bread board with jumper leads. The findings were as follows:

- The LCD responded normally by displaying the activities performed by the microcontroller as indicated in Fig. 4 and Fig. 5.
- The current sensor measured the current within the cable loop.

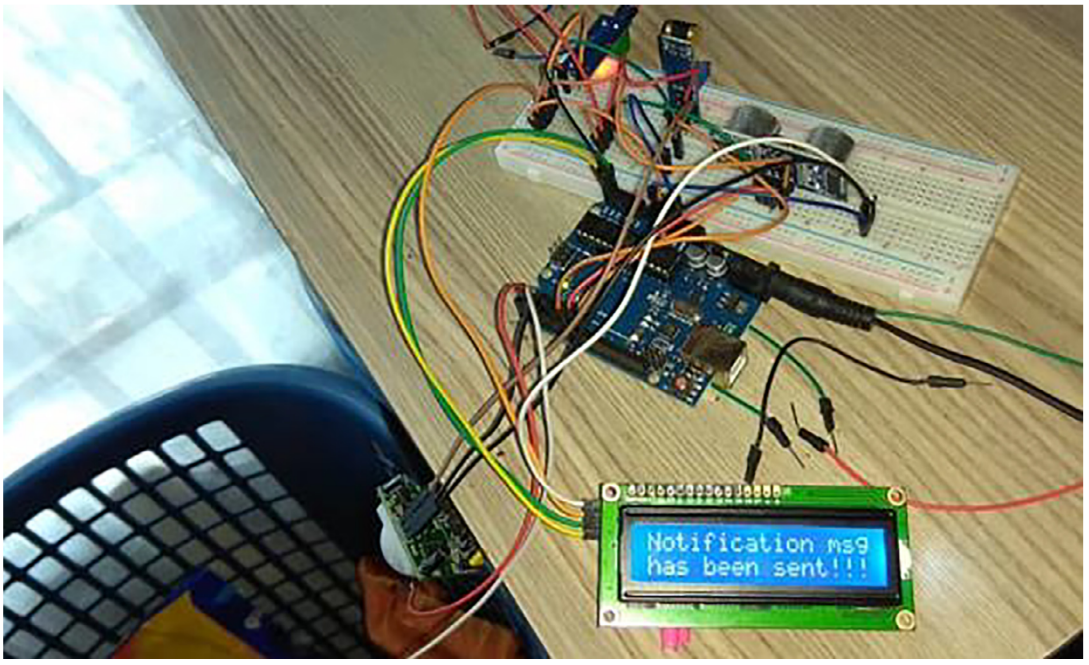

Fig. 4. Photo for testing of the bread board model of proposed system.

Fig. 5. Photo for cable theft sensing.

Notifications received

The designed system successfully delivered SMS texts to an emergency number at every sensor input stage during the testing stage, achieving consistent and effective communication each time. The sensors were programmed with flags to limit the number of notifications. Fig. 6 shows the inbox of a mobile phone after each detection. The SMS texts are triggered in sequence. The SMS notification “Alert! Lid tempering detected!” shows that the vibration sensor has been triggered. The SMS text “Alert! Lid has been opened!” means that the ultrasonic sensor has been triggered. The notifications “Alert! Motion detected in manhole!!” and “Alert! Cable has been cut!” indicate that the PIR and current sensors have been triggered respectively. The SMS notification sequence minimizes the number of false alarms.

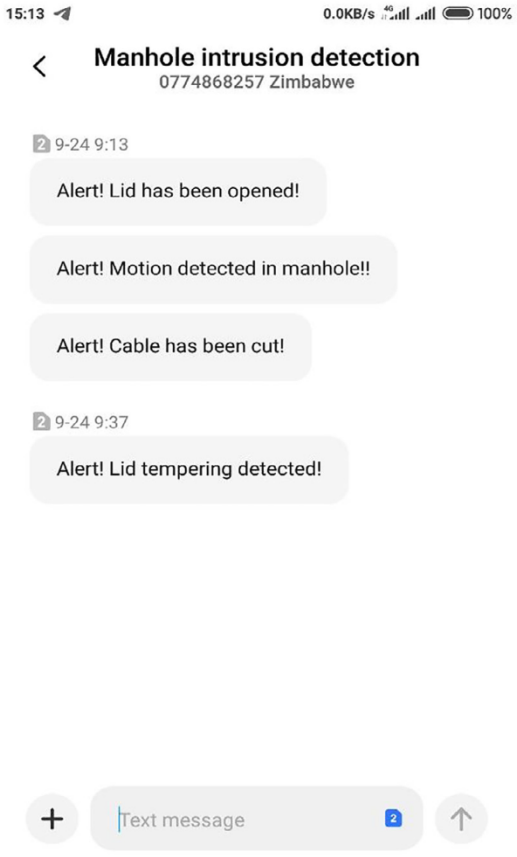

Fig. 6. Snapshot of mobile phone notification messages sent by the proposed system.

Conclusion

The development of a unique manhole intrusion detection system with notification stages was successfully completed. The system managed to sequentially send notifications when triggered by inputs from vibration, ultrasonic, PIR and current sensors. Due to the inclusion of three additional sensors, the proposed system has an advantage of timely or early-stage intrusion detection. The response time is improved since the first alert is sent early before the actual cutting of the cable. GSM Sim 800 L technology was utilized for sending notifications. Notifications were also displayed on a local LCD. The low-cost system significantly reduces the impacts of cable theft. The incorporation of multiple sensors limits false alarms. The system can be integrated into Network Operations Center (NOC) with a graphical user interface that can define the actual position of the breach on google maps. In future, there is also need for interconnection of multiple controllers to form clusters of nodes for ease of connectivity and identification. It should, however, be brought to attention that scaling up the proposed solution to include more networked sensors during operationalization may strain system performance parameters like response time, network throughput and so on. This work can be expanded in many dimensions for computer science, informatics and engineering disciplines especially for learning purposes.

Financial disclosure statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

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.

References

[1] L.A. Ajao, E.A. Adedokun, C.P. Nwishieyi, M.A. Adegboye, J. Agajo, J.G. kolo, An anti-theft oil pipeline vandalism detection: embedded system development, Int. J. Eng. Sci. Appl. 2 (2) (2018), doi:10.13140/RG.2.2.35175.55203.

[2] Q.A. Al-Haija, S. Zein-Sabatto, An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks, Electronics 2020 9 (12) (2020), doi:10.3390/electronics9122152.

[3] Arduino Official Store, 2021. Boards, shields, kits, accessories. [Online]. https://store.arduino.cc/catalogsearch/result/?tab=store&q=arduino+uno. Accessed: 10/03/2021

[4] F.H. Arifin, M.Z. Hasan, I.S.A. Mahyudin, S.N.M. Arshad, Development of fault distance locator for underground cable detection, J. Phys. Conf. Ser. (2020) (2020) 1432, doi:10.1088/1742-6596/1432/1/012014.

[5] J. Arshad, M.A. Azad, R. Amad, K. Salah, M. Alazab, R. Iqbal, A review of performance, energy and privacy of intrusion detection systems for IoT, Electronics 2020 9 (629) (2020), doi:10.3390/electronics9040629.

[6] Bell, C., 2013. Arduino-based sensor nodes. beginning sensor networks with Arduino and raspberry Pi, 51–93. doi: 10.1007/978-1-4302-5825-4_3

[7] S.A.M. Chachuli, S.M. Nazri, N. Yusop, N.R. Mohamad, Cable theft monitoring system (CTMS) using GSM modem, J. Adv. Res. Appl. Sci. Sci. Eng. Technol. (Akademia Baru) 2 (1) (2016) 57–66.

[8] M.Y. Cho, H.Y. Huang, C.N. Chen, H.T. Thom, P.R. Wang, W.Y. Chang, C.T. Wang, The implementation and applications of low voltage distribution line theft supervisory system, in: Proceedings of the 3rd International Conference on Green Technology and Sustainable Development (GTSD), 2016, doi:10.1109/gtsd.2016.50.

[9] P. Dini, S. Saponara, Analysis, design, and comparison of machine-learning techniques for networking intrusion detection, Designs 2021 5 (1) (2021), doi:10.3390/designs5010009.

[10] D.Y. Dzansi, P. Rambe, L. Mathe, Cable theft and vandalism by employees of South Africa's electricity utility companies: a theoretical explanation and research agenda, J. Soc. Sci. (2014), doi:10.1080/09718923.2014.11893281.

[11] A. Galvan, E.D. Lozano, An approach to reduce copper theft in transmission line grounding systems, Proceeding of the 2013th International Symposium on Lightning Protection (XII SIPDA) at: Belo Horizonte, 2013, doi:10.1109/SIPDA.2013.6729183.

[12] M. Giridhar, K.S. Prem, A.S. Abid, Y. Ashok, T.R. Venkatesh, K. Kumar, GSM based electricity theft detection using Arduino, Sci., Technol. Dev. IX (IX) (2020) 308–311.

[13] L. Goswami, M.K. Kaushik, R. Sikka, V. Anand, K. Sharma, M. Solanki, IOT based fault detection of underground cables through node MCU module, 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), 2020, doi:10.1109/iccsea49143.2020.9132893.

[14] Jayant, 2016. Arduino vs raspberry Pi: differences between the two. [Online]. Available: https://circuitdigest.com/article/arduino-vs-raspberryp-pi-difference-between-the-two. Accessed: 10/03/2021.

[15] G. Jia, G. Han, H. Rao, L. Shu, Edge computing-based intelligent manhole cover management system for smart cities, IEEE Internet Things J. (2017), doi:10.1109/JIOT.2017.2786349.

[16] N. Kavya, G. Anitha, IoT based underground cable fault detection system, Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET) 8 (VIII) (2020), doi:10.22214/ijraset.2020.30863.

[17] Prakash. Kumar, Kumar Pradeep., Arduino based wireless intrusion detection using IR sensor and GSM, Int. J. Comput. Sci. Mobile Comput. 2 (5) (2013) 417–424.

[18] E. Lim, M.N. Norizan, I.S. Mohamad, N. Yasin, M. Zainol, A. Sohiful, A.N. Baharum, N. Jamalullail, Design of anti-theft/cable cut real time alert system for copper cable using microcontroller and GSM technology, in: Proceedings of AIP Conference at Krabi, 1885, Thailand, 2017, doi:10.1063/1.5002481.

[19] P. Mabadie, M.O. Odhiambo, Implementation of current capacitance resonant circuit to monitor telecommunication and utility cable tampering, in: Proceedings of the 2019 Conference on Information Communications Technology and Society (ICTAS), 2019, doi:10.1109/ictas.2019.8703615.

[20] Q.S. Mahdi, Survivability analysis of GSM network systems, Euras. J. Sci. Eng. 3 (3) (2018), doi:10.23918/eajse.v3i3p113.

[21] J.C. Mart ´ınez-Santos, O. Acevedo-Pati ño, S.H. Contreras-Ortiz, Influence of Arduino on the development of advanced microcontrollers courses, IEEE Revista Iberoamericana de Tecnologias del Aprendizaje, 11, 2017, doi:10.1109/RITA.2017.2776444.

[22] A.P. Matz, J. Fernandez-Prieto, J. Cañada-Bago, U. Birkel, A systematic analysis of narrowband IoT quality of service, Sensors 20 (1636) (2020), doi:10.3390/s20061636.

[23] K. Mekki, E. Bajic, F. Chaxel, F. Meyer, A comparative study of LPWAN technologies for large-scale IoT deployment, ICT Express. Vol. 5 (1) (2019) 1–7, doi:10.1016/j.icte.2017.12.005.

[24] Microchip, 2021. ATmega328P. Datasheet. [Online]. Available: http://ww1.microchip.com/downloads/en/DeviceDoc/ATmega48A-PA-88A-PA-168A-PA-328-P-DS-DS40002061A.pdf. Accessed: 10/03/2021.

[25] Muhamba V., 2020. TelOne lost ZWL$50 million to vandalism and theft in 2020. [Online]. Available: https://www.techzim.co.zw/2020/12/telone-lost-zwl50-million-to-vandalism-and-theft-in-2020/. Accessed: 26/02/2021.

[26] N. Murugan, J.S. Kumar, T. Thandapani, S. Jaganathan, N. Ameer, Underground cable fault detection using internet of things (IoT), J Comput Theor Nanosci 17 (8) (2020) 3684–3688, doi:10.1166/jctn.2020.9261.

[27] S.B.M. Nazri, Cable Theft Monitoring System using GSM Modem, Faculty of Electronic and Computer Engineering, Universiti Teknikal Malaysia Melaka. Melaka, 2014 2014.

[28] M. Nkwana, L. Mpuru, Copper cable theft and the perpetrators in South Africa, Servamus Community-Based Saf. Secur. Mag. 112 (6) (2019).

[29] N.M. Norizan, R. Jamaludin, I.S. Mohamad, T.C. Li, M.Z. Shamian, GSM remote sensing for copper cable transmission line monitoring system using FPGA, in: Proceedings of the 2nd International Conference on Electronic Design (ICED), 2014 Vol. 2(7015842).

[30] G. Ofualagba, O. Ejofodomi, Automated oil and gas pipeline vandalism detection system, Proceeding of: SPE Nigeria Annual International Conference and Exhibition, 2020 August 11–13, 2020, Virtual, doi:10.2118/203695-MS.

[31] N. Oliveira, I. Praça, E. Maia, O. Sousa, Intelligent cyber attack detection and classification for network-based intrusion detection systems, Appl. Sci. 2021 4 (2021), doi:10.3390/app11041674.

[32] G. Organtini, Arduino as a tool for physics experiments, J. Phys.: Conf. Ser. 1076 (2018) (2018) 012026, doi:10.1088/1742-6596/1076/1/012026.

[33] S. Otoum, B. Kantarci, H.T. Mouftah, A novel ensemble method for advanced intrusion detection in wireless sensor networks, 2020 IEEE International Conference on Communications (ICC), 2020, doi:10.1109/icc40277.2020.9149413.

[34] D.R.P. Patnaikuni, A comparative study of Arduino, raspberry Pi and ESP8266 as IoT development board, Int. J. Adv. Res. Comput. Sci. 8 (5) (2017) 2350–2352.

[35] B.A. Praveena, P.S. Balachandra, S.S.K. Murthy, S.Y. Shivpratap, P. Mahadeva, M.N. Sujith, R. Naresh, L. Mallikarjun, Design and development of smart manhole, IOP Conference Series: Materials Science and Engineering 1013, 2021 (2021) 012006, doi:10.1088/1757-899X/1013/1/012006.

[36] J. Purdum, Beginning C for Arduino, Profession. Appl. Comput. (2015) 23–44, doi:10.1007/978-1-4842-0940-0.

[37] P.P. Purpura, Critical infrastructure protection and cybersecurity, Secur. Loss Prevent. (2019) 513–568, doi:10.1016/b978-0-12-811795-8.00016-3.

[38] A. Rahman, A.T. Asyhari, L.S. Leong, G.B. Satrya, M.H. Tao, M.F. Zolkip, Scalable machine learning-based intrusion detection system for IoT-enabled smart cities, Sustain. Cities and Soc. 6 (2020), doi:10.1016/j.scs.2020.102324.

[39] A. Sidebottom, M. Ashby, S.D. Johnson., Copper cable theft: revisiting the price–theft hypothesis, J. Res. Crime Delinq. 51 (5) (2014) 684–700, doi:10.1177/0022427814521216.

[40] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646.

[41] N. Sundari, S. Revathi, J.I. Jacob, IoT based underground cable fault detection, Int. J. Eng. Techn. 5 (2) (2019).

[42] Vosloo, H., Mhaule, D., 2016. Metal theft in South Africa. [Online]. https://www.tdworld.com/substations/article/20967431/metal-theft-in-south-africa. Accessed: 26/02/2021.

[43] D.M. Ward, The effect of weather on grid systems and the reliability of electricity supply, Clim. Change 121 (1) (2013) 103–113, doi:10.1007/s10584-013-0916-z.
[44] R. Yao, N. Wang, Z. Liu, P. Chen, X. Sheng, Intrusion detection system in the advanced metering infrastructure: a cross-layer feature-fusion CNN-LSTM-based approach, Sensors 21 (2) (2021) Doi:3390/s21020626.
[45] GPP, New work item: narrow band IOT (NB-IOT), TSG RAN meeting no. 69, 2015, http://www.3gpp.org/FTP/tsgran/TSGRAN/TSGR69/Docs/RP-151621.zip.