Indonesian Journal of Electrical Engineering and Computer Science
Vol. 23, No. 3, September 2021, pp. 1804~1813
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i3.pp1804-1813

Design and implementation of an adaptive multilevel wireless security system using IoT

Mohammed M. Sultan[1], Amer T. Saeed[2], Ahmed M. Sana[3]
[1]Tikrit University, Iraq
[2, 3]Department of Petroleum System Control Engineering, Tikrit University, Iraq

Article Info

Article history:

Received Oct 10, 2020
Revised Aug 4, 2021
Accepted Aug 8, 2021

Keywords:

Internet of things
Mobile application
Multilevel
Security
Wireless networks

ABSTRACT

Securing property plays a crucial role in human life. Therefore, an adaptive multilevel wireless security system (ML-WSS) based on the internet of things (IoT) has been proposed to observe and secure a certain place. ML-WSS consists of hardware and software components, such as a set of sensors, Wi-Fi module, and operation and monitoring mobile application (OMM). The OMM application is designed to remotely monitor and control the proposed system through the Internet and by using ThingSpeak cloud as a data store. The proposed scheme is based on dividing the required zone of the place into three regions (levels), low-risk region (LRR) as level-1, moderate-risk region (MRR) level-2, and high-risk region (HRR) as level-3. Each level may contain one or set of sensors, so the number of sensors, their placement, and under which level is labelled is specified according to the security requirements. Several processes are done based on these levels when a breach occurs in the system. Mathematical model and pseudocode were created to illustrate the mechanism of the proposed system. The results show that the proposed system has been implemented successfully and the number of breaches that occurs in level-3 area was reduced by 50% as compared to level-1.

Corresponding Author:

Amer T. Saeed
Department of Petroleum System Control Engineering
Tikrit University
40 St., Tikrit, Salahuddin, Iraq
Email: amer.saeed@tu.edu.iq

1. INTRODUCTION

Internet of things (IoT) is a promising technology and a hot topic in the information technology field [1]-[4]. It is defined as object sensing, controlling, and collecting information remotely through an exciting network or even without human intervention [5]. The "things" in IoT refers to physical devices, such as sensors which are used to collect data from their environment [6]. These devices are connected to small computers, i.e. Arduino and Raspberry that are responsible for processing, storing, and/or transmitting data through a network. IoT plays a crucial role in a wide range of fields, such as smart home, security, wearables, healthcare, forecast, retail, and farming. According to [7], numerous real-world applications of IoT are available with more than 20 billion IoT devices that have been installed between 2009 and 2020. This paper is concerned about IoT security systems where security is a major concern for individuals and business-companies. Several approaches with different technologies have been proposed to cover this issue, IoT has its decent share in this aspect. As for most security systems that are based on IoT technique, passive infrared (PIR) sensors, ultrasonic sensors, and surveillance cameras are used in these systems to detect unauthorized

presence. The mechanism of PIR sensors is based on sensing the variation of emitted heat from objects (people) movement and background heat while the ultrasonic sensors transmit ultrasonic sound waves into space and then measure the speed of returned waves. PIR sensors require a direct line of sight while ultrasonic sensors do not. In this paper, the ultrasonic sensors are used with the Arduino board as the main components of the proposed security system.

In [8], a wireless detection system based on Arduino with the android application for communication is proposed. The main components of this system are an Arduino with a passive infrared sensor (PIR), WiFi module, light-emitting diode (LED), and a buzzer. When the PIR sensor detects a movement in its coverage area, the Arduino will fire a local alarm sound through the buzzer. Although the wireless application in this paper could be used to turn off the alarm, no message or notification will be sent to the user. In addition to these, the communication with the system is established only in the range of the wireless module of the Arduino which is considered a small area, also the application has limited functionalities. Another approach is proposed in [9] where two Arduino boards are utilized with two PIR sensors and a camera. Short messages (SMS) through global system for mobile communications (GSM) networks are used for communication between the user and the system. When a movement is detected by any sensor, the system will start taking pictures through the camera which is pointed toward the sensors for a later check. A warning SMS is also sent to the user indicating which sensor observed the movement. After that, the alarm will be triggered by the system. The system can be turned off by sending back an SMS with "Buzof" code. The alarm system in this research depends only on one case without any differential technique to categorize the motions into several levels including dangerous levels. The system in this paper also has a limited communication method. An additional aspect is introduced by [10], [11] where they use a temperature sensor to observe the variation of room temperature in case of unauthorized presence. The mechanism of the system is to store the average value of the normal room temperature and to continuously compare it with the present. Also, a PIR sensor is implemented to detect movement while a GSM module is used for the communication between the user and the system. To control the security system, short messages are used. In this paper, authors didn't apply further conditional processes to increase the accuracy of the alarm system since the alarm system could be fired just according to temperature variation which is not a proper method.

The more advanced technique was proposed by [12], [13] where the major concern of these papers is vehicle security and driver safety. The main component is an Arduino board with several peripherals, such as limit switch to detect door opening, PIR sensor for unauthorized presence detection inside the car and Tilt sensor for car towing. For the occupant's safety, an eye blink sensor is used to monitor the rate of the driver blinking. Therefore, in case of sleeping, the system reduces the car velocity and then an alarm sound is fired after a certain amount of time to notify the driver. A vibration sensor and a GSM module are proposed to estimate car accident and to establish a communication, respectively. The communication with users is conducted in case of car theft while with the authorities in case of an accident.

More sensors were attached to the Arduino board in [14], such as a fire sensor, door sensor, motion sensor, and vibration sensor with GSM communication method. Set of 5V relays were used to control other devices such a buzzer, led and direct current (DC) pump. DC pump is triggered when the fire sensor detects an elevated level of temperature to control fires and restrict the damaged area. The vibration sensor is equipped with industrial machines to avoid damage due to instability, and to trigger the buzzer and sends a notification to the customer through SMS. Both motion and door sensor is used to trigger the alarm and send notification messages to the owner. A multi-level home security system for developing countries was implemented in [15], [16]. It was built by using a novel, effective, and a simple method. This paper aims to build a reasonable, straightforward home security system. The system consists of a microcontroller, PIR motion detector sensors, fingerprint door lock, GSM module and a surveillance web camera. The purpose of the fingerprint door lock is to prevent unauthorized people from entering the house. Messages are sent to the owner through the GSM module when someone attempts to break into the house. The system is very cheap compared to home security systems, which provides security from different viewpoints. The result showed that the proposed security system has worked successfully.

Authors in [17], [18] focus on building home automation systems to control home appliances through Android application. The core purpose of home automation is to help disabilities and elderly people which will allow them to control their home facilities easily, such as turning off/on the light using android application. Alert is also activated through a mobile application in case of critical situations. When there is a gas leak, the smart home system turns on the buzzer as a warning sign. In [19], an operative and fee efficient method was projected to detect electrical theft by constructing and developing a wireless electricity theft detection and monitoring system with a suitable combination of both the hardware and the software. The numerous advantages of wireless network communication have been achieved by using IoT. Researchers in [20]-[24] and [25]-[29] have focused on the security system from different perspectives, such as utilizing

selection algorithm, physical layer technology and GSM. Vision-based technology is addressed in [25], so the image is classified by the trained network into six classes of gestures to monitor and encourage the worker to exercise hands and wrists frequently through playing the game. This paper has not focused on vision-based technology only because sensing the movement in this paper is enough to protect the dedicated area and it can be adapted with any other systems such as vision technology.

As they were presented above, the framework in the above papers, such as in [8]-[15] does not divide the secured area into levels. Instead, any sensor may start the local alarm which is inconvenient and mostly for the outdoor sensors where animals' movement are more frequent. The proposed methodology addresses this issue by splitting the secured area into three zones. The first and the second levels send silence waning with brief phone vibration to the user without firing the local alarm and let the user decides the right action. However, the third level covers the high-risk zone which adapts automatic actions. To sum up, all the aforementioned papers have several drawbacks as they were described. Therefore, to avoid these problems, adaptive wireless security approach based on IoT was designed and implemented in this article. The paper is organized as follow: the detail of the proposed method is explained in Section 2 and the results are demonstrated and discussed in Section 3. The last section which is section 4 includes the conclusion of the research.

2. RESEARCH METHOD

In this paper, a multilevel wireless security system (ML-WSS) has been proposed to monitor and secure a specific place and to ensure the safety is applied. ML-WSS consists of a set of sensors, Wi-Fi module (ESP8266), Arduino, dedicated power supply and operation and monitoring mobile application (OMM) as shown in Figure 1. The OMM application is built by authors to remotely monitor and control the proposed security system through the Internet and by using a ThingSpeak cloud service as a data store. The suggested scheme is based on dividing the danger zone of the place into three regions (levels); low-risk region (LRR) as level 1, moderate-risk region (MRR) level 2, and high-risk region (HRR) as level 3. Each level may contain one or set of sensors, so the number of sensors, their placement, and under which level is labelled is defined according to the security requirements. Several processes will be conducted based on these levels when there is a breach that occurs in this security system.

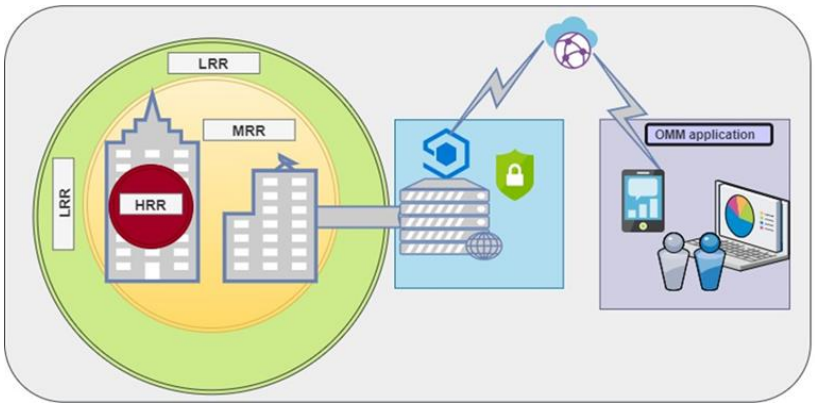


Figure 1. The multilevel wireless security system

The warning is classified under LRR when there is an abnormal movement indicted by level 1 sensors. In this case, the system delivers an alarm message to the OMM application which displays it with the breach time and sensor ID that detected the abnormal movement with a brief phone vibration. While the alarm is categorized under MRR when a breach is caught in case of unauthorized access in level 2 area. The system in this event sends an MMR alarm to the OMM app which contains the breach time and sensor ID and then the application will issue a 10 seconds vibration to inform the user. Whereas multiple steps are conducted in the case of the third level (HRR) which is the most critical case: an alarm buzzer is fired instantly in the secured location, OMM app will receive HRR message and then an intensive sound will start with continuous phone vibration. If the alarm is not turned off after a fixed amount of time, an automatic call will be established to inform the police centre about the breach by using a previously recorded voice message that contains the address of the secured location and describes the breach with the contact number and all other details of the focal point. The alarm mechanism is represented mathematically as:

If the status of the sensor 1, 2, 3,… m which are under level1 area is represented by $X_1, X_2, X_3, \ldots X_m$, $respecivelly$, the LRR alarm will depend on the (1):

$$L = \sum_{n=1}^{m} X_n = X_1 + X_2 + X_3 + \cdots + X_m \quad (1)$$

$X_{1,2,3\ldots m}$=1 when there is an abnormal movement, otherwise it equals 0. The alarm LRR is sent when (2) is verified:

$$L \geq 1 \quad (2)$$

Whereas the MRR alarm is based on (3):

$$\Omega = \sum_{n=1}^{k} Y_n = Y_1 + Y_2 + Y_3 + \cdots + Y_k \quad (3)$$

When Y_n represents the status of the n[th] sensor under level 2. The alarm MRR is classified under either type 1or 2 based on the result ($\acute{M}$) of (4) which is related to (1) and (3).

$$\acute{M} = \Omega + L * \Omega \quad (4)$$

The alarm MRR type 1 is sent when there is no abnormal movement detected by sensors of level 1, but there is unauthorized access detected by sensors of level 2, so $L = 0$, and then in (4) will become as:

$$\acute{M} = \Omega \quad (5)$$

However, the alarm MRR type 2 is sent when there are breaches under level 1 and 2. Therefore, in (4) becomes (6):

$$\acute{M} > \Omega \quad (6)$$

HRR alarm is indicated based on (7):

$$Z = \sum_{n=1}^{l} Z_n = Z_1 + Z_2 + Z_3 + \cdots + Z_l \quad (7)$$

Z represents the level 3 sensor status. In (7) will convert to (8) when taking calling the police in our account:

$$\tilde{H} = (Z + \tau)s \quad (8)$$

τ: The specific duration time to wait before calling the police, increment value will reach to 0 if the user does not cancel the alarm.

s: The setting value which is either 1 as default or 0 when the alarm is cancelled by the user before $\tau = 0$

The call will be conducted when the value of $\tau = 0$, and the user did not press the cancel bottom, so $s = 1$. The (7) becomes (8):

$$\tilde{H} = Z \quad (9)$$

The HRR alarm will be omitted when the alarm is cancelled by the user, so s=0:

$$\tilde{H} = (Z + \tau) * 0 = 0 \quad (10)$$

The pseudocode of the proposed method and equation is presented in Figure 2. To illustrate it in more details, several scenarios will be discussed. For instance, if an intruder breaches the level1 area and passes three sensors of level1 which lead to $\ell = 3$ and as result fulfils the condition $\ell \geq 1$. At this point, the system will connect to the cloud database and sends LRR alarm type, sensor IDs that detect movements, and the breach time, respectively. And if the intruder continues to level2 zone and breaks through one sensor, in this event $\Omega = 1$ which passes the rule $\Omega \geq 1$. The system instantly connects and sends MRR alarm with the sensor ID and the breach time to the central database. However, when reaching the level 3 area, and if two sensors detect unauthorized movement $Z = 2$, in such case, HHR alarm type, sensor IDs, and breach time are sent. Also, the system starts a local siren alarm at the secured location and waits for 30 seconds before notifying the police. If the user sends a cancel alarm request, the system will stop the local alert and return to

the initial state. Nevertheless, if no cancellation request received, the system will notify the authorities once the timer ends.

```
Define
ℓ = ∑_{n=1}^{m} x_n // ℓ is the status of Level1 sensors
Ω = ∑_{n=1}^{k} y_n // Ω is the status of Level2 sensors
Z = ∑_{n=1}^{l} z_n // Z is the status of Level3 sensors
// Where m, k, and z are the last number of sensors in each level (n^th)
τ = 30 seconds // τ is a predefined waiting time
if ESP8266 = 0 then // ESP8266 is the WiFi module, 0 = not connected
    set WiFi SSID & Password // SSID: Wi-Fi network name
    connectWiFi( ) // connect to the Internet
end
if ℓ ≥ 1 then // 1: movenment detection in Level1 sensors
    connectToCloud ( ) // connect to thingspeak cloud service
    sendDateToCloud(LRR, level1SensorID, breachTime) // LRR: low-risk region
        alarm type
end
if Ω ≥ 1 then // 1: movenment detection in Level2 sensors
    connectToCloud( ) ;
    sendDateToCloud(MRR, level2SensorID, breachTime) // MRR: moderate-risk
        region alarm type
end
if Z ≥ 1 then // 1: movenment detection in Level3 sensors
    connectToCloud ( ) ;
    sendDateToCloud(HRR, level3SensorID, breachTime) // HRR: high-risk region
        alarm type
    startBuzzerAlarm() // fire the local buzzer alarm
    countDownTimer(τ) start // loop for 30 seconds before calling police
        if receivedCancelOrder then // if user sent cancel order
            stopBuzzerAlarm( ) // turn off the buzzer alarm
            GoTo Step 6
        else if τ = 0 then
            callPolice( ) // no cancel order received and timer is ended, so
                call the police
        else
            GoTo Step 23
end
```

Figure 2. Pseudocode of the ML-WSS and equation

3. IMPLEMENTATION, RESULTS AND DISCUSSION

The implementation of the proposed system as well as results and discussions are presented in this section. The implementation in this research is divided into two stages, installing equipment in the secured area and then building a mobile application for end-users. The hardware is represented by the Arduino, ultrasonic sensors, Wi-Fi module, buzzer and power supply as shown in Figure 3. The Arduino is the main board where all the other peripherals are connected to. While the software part is represented by creating a mobile application OMM app.

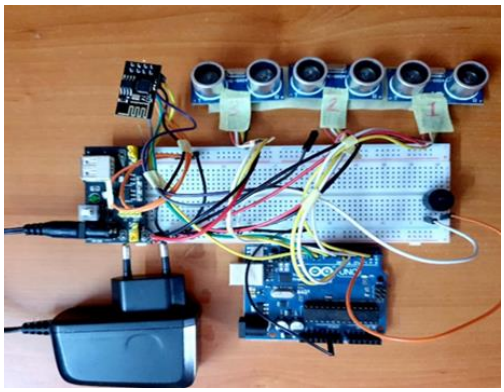


Figure 2. The implementation of the system

3.1. Hardware work

One Arduino and Wi-Fi module were used in this paper to control the connected devices and to exchange data among placed devices and the OMM application through the cloud (ThingSpeak), respectively. For the sake of the experiment, the authors used three ultrasonic sensors where each one represents one of the security levels. A buzzer is used to fire sound alarm in the same location when there is a breach. This side of the system also has a software part which is built in the Arduino to control and manage all the peripherals. Arduino IDE 1.8.12 was used to develop an alarm system and to program Arduino Uno with the ESP8266 Wi-Fi module and other components. The Arduino communicates with ESP8266 Wi-Fi using AT-Commands and at 9600 serial baud rate. The ultrasonic sensors programmed, and work as shown in Figure 4.

Once a sensor detects a movement, the Arduino transmits sensor ID with alarm type and the breach time to the cloud server. And if the alarm type is HRR, the system will fire an alarm sound at the secured area and waits for 30 seconds to receive a cancellation from the user. Otherwise, the system will call the police to notify them about the unauthorized movement.

```
int sensor1() {
  digitalWrite(triger,LOW); // turn off trigger pin.
  delayMicroseconds(2); // wait for 2 microseconds.
  digitalWrite(triger,HIGH); // send signal to sensor to send wave.
  delayMicroseconds(10); // wait for 10 microseconds to read wave back.
  digitalWrite(triger,LOW); // turn off trigger pin.
  duration = pulseIn(echo,HIGH);//receive sensor elapsed time to read returned wave.
  distance = duration*0.034/2; // calculate object distance from the sensor where 0.034cm/µs is the speed of sound.
  if(distance <=700)//if the distance is 7 meters or less trigger alarm
  {
  Serial.println("ALARM 1");//Show alarm message (in case of built-in display is installed)
  digitalWrite(alarm,HIGH); //supply 5v to buzzer pin to start alarm.
  return 1; // return 1 to indicate breach
  }else{
   digitalWrite(alarm,LOW); // turn off alarm.
   return 0;
  }
```

Figure 4. Arduino code

3.2. OMM app

The other aspect of the proposed security system is the operation and monitoring of mobile application (OMM). Android studio 3.5.3 with Java programming language is used to develop this application. JavaScript object notation (JSON) is used to communicate and to fetch data from the cloud server. The OMM application is shown in Figure 4. The main page contains three rows of text-view to show the status of level 1, level 2, and level 3 sensors, respectively. The application automatically communicates with the cloud server as soon as it starts running, and the status of each security level is updated every three seconds. The update time is shown in the bottom text-view to notify the user about the latest update time. A local database is utilized to store the previous values of each security level and to compare it with the new reading. When the system detects a movement at level 1 sensors, the application presents the breach time in the specified text-view in yellow colour with a brief phone vibration to get the user attention and as shown in Figure 6.

The vibration of level 2 breach goes for ten seconds as well as the breach time with a warning message in orange colour is displayed under the level 2 label. However, when the application receives an HRR alarm (level 3) from the server, several steps are performed and as follow: under level 3 sensor status label, a red warning message with the breach time will be shown, firing a loud sound alarm, continues phone vibration, and starting a countdown timer (30 seconds) to call the police and as showing in Figure 6. In case of any type of alarm, the user has the privilege to cancel it. Whereas, the cancel alarm module is used to stop the countdown timer for calling the police and terminates the vibration mode. However, it will not clear the alarm messages history. The reset alarm module performs just like the former in addition to resting the alarm messages and put the application in the initial state. The user does not need to put the application in the display mode to get warnings, it is designed to work in the background.

Numerous tests have been conducted in this research to assess the performance of the ML-WSS system and to analyze its efficiency. Some samples of these tests are shown in Figures 5 and 6. Figure 5 shows the

mode when there was no breach detected by the system while Figure 5.a and b illustrate the breaches in level 1 and 1-3, respectively by using yellow colour for level 1, orange for level 2, and red for level 3. A comparison between the hardware and software alarm (OMM app) was conducted also to test how fast the system is responding to the breach through the OMM application as compared to the same broken area.The comparison shows that the OMM app is very accurate and fast as compared to the installed alarm system.

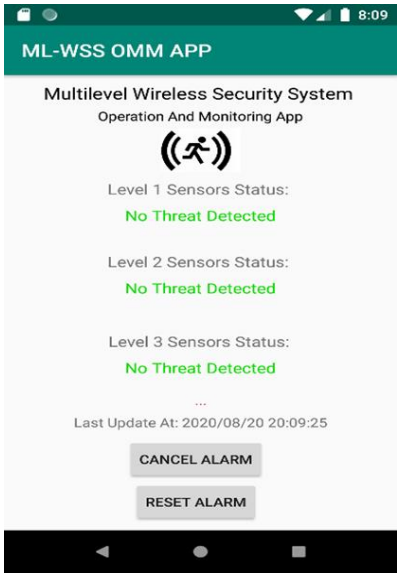
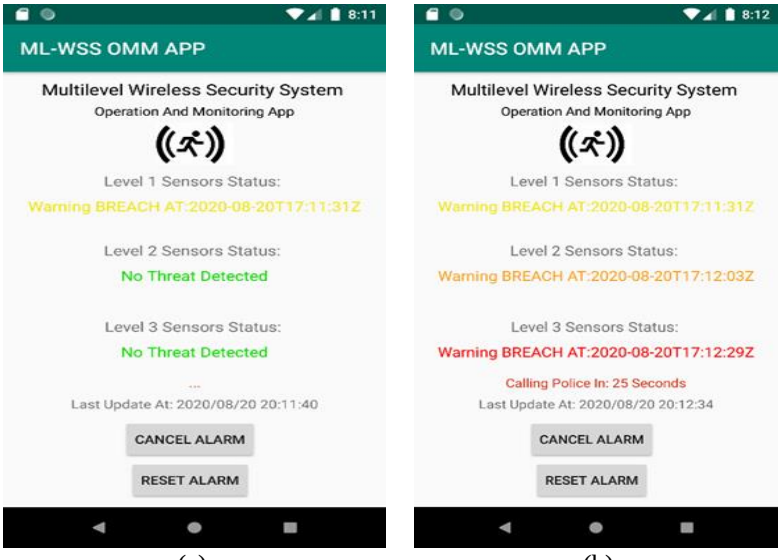


Figure 5. OMM app



(a) (b)

Figure 6. These Figures are; (a) level 1 alarm, and (b) level 2 and 3 alarm

Figure 7 shows the number of breaches of each level of sensors at certain times. Random unauthorized movements were used for about an hour-from 12:18 to 13:47-to test the proposed system and to calculate the number of breaches whereas this number is accumulative of each level. It is obvious to notice that level1 sensors spotted the highest number of breaches where these sensors are installed at the first lines of the secured area (i.e. building's fence). The number of breaks reached to 19 at 13:47 under this level. Level 2 sensors have a smaller number of breaches (14) as compared to level 1 (19) where they should be fixed in the area of medium security priority.

Level 3 sensors are designed to be mounted in the high-risk zones where no one should be accessed without authorization. The breaches number for level 3 reduced by 50% and became the lowest number (10) as compared to other levels since this area is a usually small zone that is located inside of further two other areas which are level 1 and 2. The purpose of placing level 3 region-the most dangerous area-inside level 1 and 2 is to protect it from the break and make it so hard to be breached.

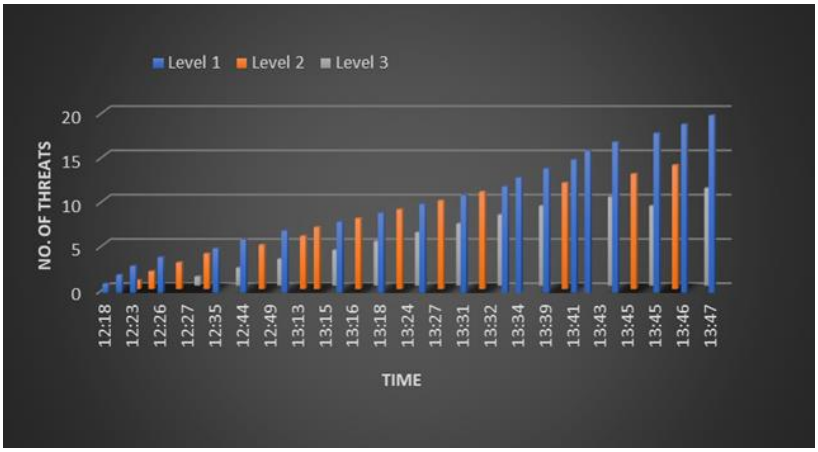


Figure 7. No of breaches over multilevel

The proposed system requires approximately two seconds to inform the user about a breach. This time mostly depends on the Internet quality. Figure 8 shows the duration utilized to notify the user about a detected movement within the three levels. The average recorded time values are 2038, 1855, 1916 milliseconds for level 1, level 2, and level 3 respectively. The total average time of the three levels is approximately 2 seconds. This time can be reduced with faster internet connection.

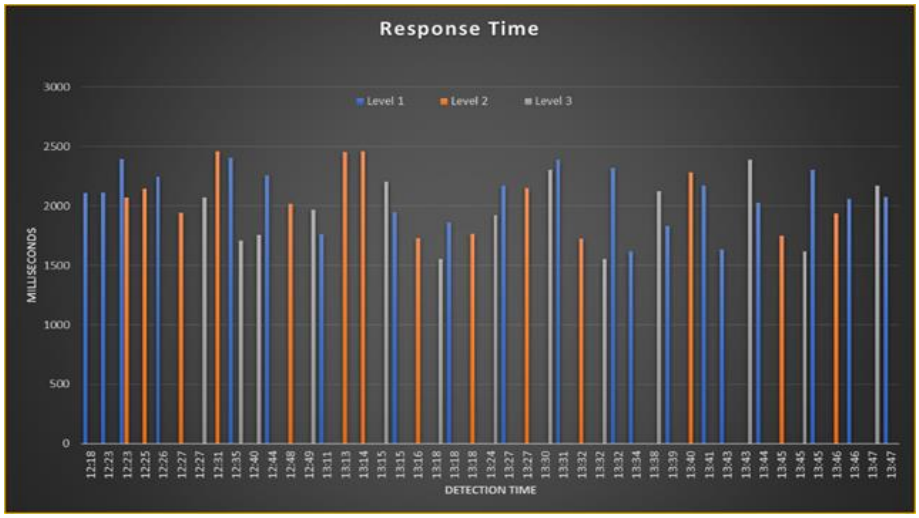


Figure 8. Response time of alert

4. CONCLUSION

In this paper, a multiple levels wireless security framework called ML-WSS based on IoT has been planned and implemented to secure a certain area of lively properties. The suggested scheme is based on dividing the area that is required to be protected into several sub-areas according to their level of risk. Each sub-area is monitored and controlled through a mix of physical and logical components such as Arduino, ultrasonic sensors and OMM application. Different alarm warnings will be displayed and delivered through the OMM application when there is a breach in any level (1, 2, and 3). Based on these warnings,

several steps are conducted to respond to the breach, such as the automatic call to the police, fire sound. Several mathematical equations and Pseudocode were also driven and written in this paper to illustrate the mechanisms of the proposed system. The result shows that the ML-WSS was successfully implemented and the number of breaches in level 3 area reduced by 50% (10 breached) as compared to level 1 (19 breaches) and level 2 (14 breaches). The least number of breaches occurred level3 region because the area is protected by further two regions level 1 and 2.

REFERENCES

[1] A. Luigi, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787-2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[2] S. Farzad, L. Bauer, and J. Henkel, "IoT technologies for embedded computing: A survey," In *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*, Pittsburg, pp. 1-10, 2016, doi: 10.1145/2968456.2974004.

[3] M Noor, M. Hassan, and W H., "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, 4, pp. 283-294, 2019, doi: 10.1016/j.comnet.2018.11.025.

[4] T. S Amer, R. S. Zaid, M. S. Ahmed, and H. A. Musa., "Eliminating unwanted signals in sound by using digital signal processing system," *Indonesian Journal of Electrical Engineering and Computer Science (IJECE)*, vol. 18, no 2, pp. 829-834, 2020, doi: 10.11591/ijeecs.v18.i2.pp829-834.

[5] G. Pradyumna, O. Bhat, and S. Bhat, "Introduction to IOT," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41-44, 2018, doi: 10.17148/IARJSET.2018.517.

[6] A. F. Ayotunde, M. O. Ibrahim, A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 5, no. 88, pp. 10-28, 2017, doi: 10.1016/j.jnca.2017.04.002.

[7] S. O. Dea, "tuse worldwide from 2009 to 2020.", Dec 2019, [online] Available: https://www.statista.com/statistics/764026/number-of-iot-devices-in-use-worldwide, [accessed on July,23 2020).

[8] S. S. Syazlina Mohd Soleh, M. M. Som, M. H. Abd Wahab, A. Mustapha, N. A. Othman and M. Z. Saringat, "Arduino-Based Wireless Motion Detecting System," *2018 IEEE Conference on Open Systems (ICOS)*, 2018, pp. 71-75, doi: 10.1109/ICOS.2018.8632703.

[9] B. S. Jeffri, and M. A. Novradin, "Design and implementation of modular home security system with short messaging system," *EPJ Web of Conferences*, vol. 68, no. 4, 2014, doi: 10.1051/epjconf/20146800025.

[10] S. S. Bhavya, S. S. Varun, and Knhn G. Debarshi, "Home monitoring and security system," In *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, 2016, pp. 1-5, doi: 10.1109/ICTBIG.2016.7892665.

[11] M. Andriansyah, M. Subali, I. Purwanto, S. A. Irianto and R. A. Pramono, "e-KTP as the basis of home security system using arduino UNO," In *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, 2017, pp. 1-5, doi: 10.1109/CAIPT.2017.8320693.

[12] S. Senthilkumar, K. Brindha, and S. Bhandari, "Vehicle accident management and control system using MQTT," *International Journal of Advances in Applied Sciences (IJAAS)*, vol. 9, no. 1, pp. 1-11, 2020, doi: 10.11591/ijaas.v9.i1.pp1-11.

[13] S. Warankar, S. Nawale, T. Bardeskar, and A. Mhatre, "Arduino based Car Security System," *International Journal of Engineering Technology Science and Research*, vol. 4, no. 4, pp. 32-43, 2017.

[14] S. Raut, A. Gaikwad, M. Raghurajan, and P. Patil, "Industry based security system using gsm and arduino," *International Journal of Advance Scientific Research and Engineering Trends*, vol. 5, no. 3, pp. 14-23, 2020.

[15] N. Tejashwini, S. Kumar, and K. Satyanarayana, "Multi-stage secure clusterhead selection using discrete rule-set against unknown attacks in wireless sensor network" *International Journal of Electrical and Computer Engineering (IJECE)*," vol. 10, no. 4, pp. 4-12, 2020, doi: 10.11591/ijece.v10i4.pp4296-4304.

[16] H. U. Zaman, T. E. Tabassum, T. Islam and N. Mohammad, "Low cost multi-level home security system for developing countries," In *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2017, doi: 10.1109/ICCONS.2017.8250522.

[17] D. Javale, M. Mohsin, S. Nandanwar, and M. Shingate, "Home automation and security system using Android ADK," *International journal of electronics communication and computer technology (IJECCT)*, vol. 3, no. 2, pp. 382-385, 2013.

[18] A. S. Romadhon,"System Security And Monitoring On Smart Home Using Android," *Journal of Physics: Conference Series*, vol. 953, no. 1, pp. 1-5, 2018.

[19] R. Meenal, K. M. Kuruvilla, A. Denny, R. V. Jose, and R. Roy, "Power Monitoring and Theft Detection System using IoT," *Journal of Physics: Conference Series*, vol. 1362, no. 1, pp. 1-7, 2019, doi: 10.1088/1742-6596/1362/1/012027.

[20] M. Zeyad, S. Ghosh, and K. M. Ahmed, "Design prototype of a smart household touch sensitive locker security system based on GSM technology," *International Journal of Power Electronics and Drive Systems (IJPEDS)*, vol. 10, no. 4, pp. 1923-1930, 2019, doi: 10.11591/ijpeds.v10.i4.

[21] W. Andre, and O. Couillard, "Design and Implementation of a New Architecture of a Realtime Reconfigurable Digital Modulator (DM) into QPSK," *International Journal of Reconfigurable and Embedded Systems (IJRES)*, vol. 7, no. 3, pp. 167-179, 2018, doi: 10.11591/ijres.v7.i3.pp167-179.

[22] Y. A. S. Aldeen, and H. M. Abdulhadi, "Secure and reliable wireless advertising system using intellectual characteristic selection algorithm for smart cities," *Telecommunication, Computing, Electronics and Control (TELKOMNIKA)*, vol. 18, no. 5, pp. 2401-2411, 2020, doi: 10.12928/telkomnika.v18i5.14859.
[23] N. S. Ali, H. A. Kadhim, and D. M. Abdulsahib, "Multi-function intelligent robotic in metals detection applications," *Telecommunication, Computing, Electronics and Control (TELKOMNIKA)*, vol. 17, no. 4, pp. 2058-2069, 2019, doi: 10.12928/telkomnika.v17i4.11822.
[24] H. A. Kadhim, N. S. Ali, and M. A. Dheyaa, "Management and achieving system for metal detection robot using wireless-based technology and online database registry," *International Journal of Power Electronics and Drive System (IJPEDS)*, vol. 10, no. 1, pp. 219-229, 2019, doi: 10.11591/ijpeds.v10.i1.pp219-229.
[25] M. Rungruanganukul, and T. Siriborvornratanakul, "Deep Learning Based Gesture Classification for Hand Physical Therapy Interactive Program," In *International Conference on Human-Computer Interaction*, 2020, pp. 349-358, doi: 10.1007/978-3-030-49904-4_26.
[26] A. Tedeschi, S. Calcaterra, and F. Benedetto, "Ultrasonic RAdar System (URAS): Arduino and Virtual Reality for a Light-Free Mapping of Indoor Environments," *IEEE Sensors Journal*, vol. 17, no. 14, pp. 4595-4604, 2017, doi: 10.1109/JSEN.2017.2708840.
[27] A. Singh, A. Pal, and B. Rai., "GSM based home automation, safety and security system using android mobile phone," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, no. 5, 2015.
[28] K. I. Bokad, N. M. Deepak, G. A. Ajinkya, M. Y. Birhade, and S. Ritika, "Power Theft Detection And Monitoring Using Gsm Technology," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 3, pp. 2237-2240, 2018.
[29] S. Arivazhagan, A. A. Tsegaye, and A. S. Mohammed, "GSM and Arduino based power theft detection and protection," *International Journal of Advanced Research, Ideas and Innovations in Technology*, vol. 5, no. 4, pp. 581-588, 2019.

BIOGRAPHIES OF AUTHORS

Mohammed M. Sultan is an instructor at Tikrit University. He has a master's degree in computer science from Oklahoma City University, the USA in 2017. His main research area includes Radio Frequency Identification, Programing, Computer Network and Internet of Thing.

Amer T. Saeed is an instructor/lecturer at Tikrit University–College of Petroleum processes. He holds M.Sc. degree in electrical engineering from the University of New Haven, the USA in 2016 and received B. S. Degree in Electrical Engineering from Tikrit University-Iraq in 2009. He is highly interested in 4G & 5G communications systems, wireless networking and communications, digital signal processing (DSP). He has published many papers in high reputed international and local conferences and journals.

Ahmed M. Sana received a B. Sc. degree in electrical engineering from Tikrit University, Iraq, in 2011 and M. Sc. degree in electronics and communications engineering from Baghdad University, Iraq, in 2014. In 2015, he worked as a power electronic engineer in the power department orient-telecom internet service company in Baghdad. Since 2017 and till now, He is working as a lecturer at Tikrit University, College of Petroleum Processes Engineering, Petroleum Systems Control department. His research interests include Power Electronics, Digital Signal Processing, and 4G & 5G communications systems.