Smart Home Security Integrating at Various Access Points

Stephie Rachel I [1], Sakthi Latha R [2], Thanusha S [3], Selva Prabha V [4]
[1] Teaching Fellow, University College of Engineering, Nagercoil, TamilNadu, India.
[2, 3, 4] Student, Department of CSE, University College of Engineering, Nagercoil, TamilNadu, India.

Abstract – To improve the home security, this paper proposes the use of logical sensing algorithm and explains various security issues in the existing home automation system. There are two natural access points, one is primary access point, and the other one is secondary access point. The normal user behavior at these two access points is identified by the logical sensing algorithm and also requesting user verification when necessary. In this home security system, various sensors are used to measure the change in temperature, humidity and carbon-monoxide level. The changing state of these various access points are considered by the user position. The user behavior at various access points are identified by the combination of sensors, microcontroller and zigBee communication and implemented by logical sensing algorithm.

Index Terms – ArduinoUNO, Sensors, Zigbee, IOT device, Temperature, Humidity, Carbon monoxide.

1. SCOPE AND PURPOSE

Home automation means the building function for a home. It is called a smart home or smart house.The control and automation of heating (such as smart_thermostats), ventilation, air conditioning (HVAC), and security (such as smart_locks), as well as home_appliances such as washer/dryers, ovens or refrigerators/freezers can be involved.Remote monitoring and control can be done by Wi-Fi.An important constituent of the Internet of Things are the home devices that can be remotely monitored and controlled through an internet. Modern systems generally consist of switches and sensors connected to a central hub sometimes called a "gateway" from which the system is interacted with a user_interface like a wall-mounted terminal, mobile phone software, tablet_computer or a web interface.

2. INTRODUCTION

Nowadays an electronic devices and internet became more developed and inexpensive in the improvement of technology. So, the people's expectation has dramatically changed in the concept of home automation. Modern smart home uses various computing devices and wireless sensors and actor networks.The concept of home automation security has improved with to detect, alert prevent intrusion for with time ,sensors and acutators were integrated into the home. The proposed work improves the smart home security by integrating logical sensing into smart home.And also it utilizes the combination of microcontrollers and sensors to detect user behaviour at various access points.

3. RELATED WORKS

B.N.Schilit et al.[11] proposed the use of infra-red grids and wearable identification. The location of the user at home can be identified by the infra-red grids and wearable id.IR grids are difficult to implement in a home environment. Wearable IDs are to be inconvenient and provided misleading information for inexperienced and careless users.

J.Choi[12] et al. proposed the system to predict and learn user context by body temperature, facial expression, room temperature, time and location. But there is a variation in user's body temperature, facial expression that depends on various other factors like state of mind, illness etc .So their work became failure.

O.Yurur et al.[13] proposed that context aware sensing vary depending upon user environment ,prior knowledge of recent event patterns. In home environment, it is unpredictable ,it is extremely challenging to predict the context of various user actions. It needs depth knowledge of context, and requires sophisticated sensing techniques and high processing power. , so it is impossible to gain access to the system and manipulate it for an eavesdropping attacker. So it is complex to implement.

Y.Zhao and Z.Ye[14] proposed a low cost and flexible home security system. In this an alert SMS is sent to the administrator if any intrusion is detected. Their approach lacks of any sophisticated intrusion detection algorithms to identify attack attempts.

S.Morsalin et al.[15] proposed a home security system that users Near Field Communication[NFC] tag, password, and fingerprint. Global system for Mobile module which also embedded in the system, that communicates with the logged password to a remote server using Machine to Machine communication .Each time the user wants to access his home he has to enter the password and verify the fingerprints. But it was inconvenience to use the NFC tag that mentioned in the work could be misplaced by careless user or stolen by an attacker.

4. IMPLEMENTATION

In this paper, two various were examined to identify different inauthentic scenarios within a smart home. Access points are built-in with the construction of the home,which can be used for go in and go out of the home.The two access points contributes four places which are front door,back door,balcony door and window.The window is not a normal access point, it is mostly used by an intruder to entering a home depending on the situation.These access points are only possible for physically gaining the access to a home unless serious construction adjustments are made to home.There are two access points that are primary and secondary based on the motive of the access points.The primary access points used by the occupier as a primary means to enter and exit from the home which categorized as a front door and back door.The window and balcony door are in secondary access points,these are rarely used for entering and exiting ,because there are convenient way for legitimate user.

Fig 1(a).shows sensors,board and microcontroller deployment in primary access point.

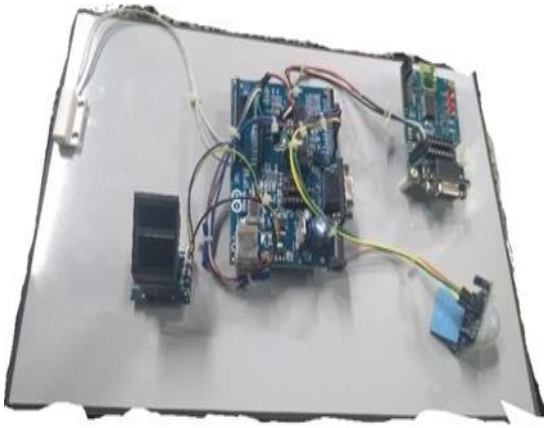

Fig1(b).shows sensors,board and microcontroller deployment in secondary access point

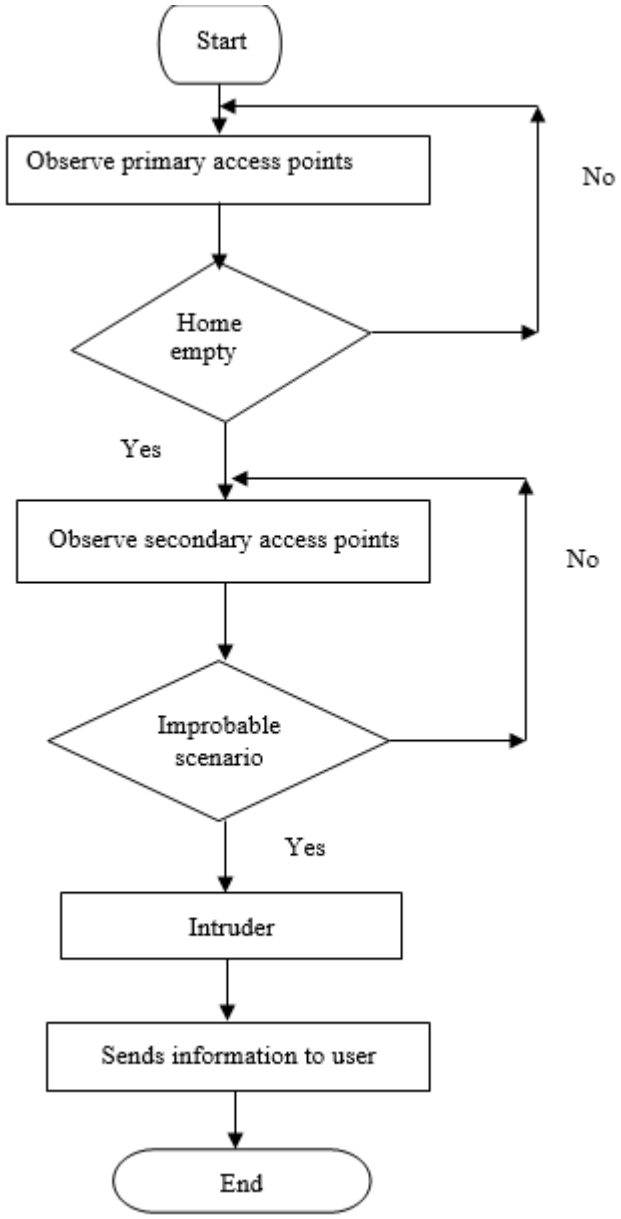

Fig.2 Flowchart explaining the algorithm when door to an empty home is opened

4.1.Primary Access Point

The primary access point to a home is front door,an inhabitants use this door as the main way in and out of their home. Depending upon the architecture and inhabitant can be used one or more primary access points depending on their needs. This paper proposes the use of motion and proximity sensors to detect user behavior at primary access points. The motion and proximity sensors placed near the access point inside the home are triggered when a user leaves an occupied home. The motion and proximity sensors will not be triggered once the user stepped out and closes the door. When someone enters an

empty home, they are entering from outside so, before the door is opened the motion and proximity sensors will not be triggered. Once the door is opened and the user enters the home the motion and proximity sensors placed inside the home will be triggered. Fig2 shows the flowchart of the door state changes and sensor operations of the primary access point.

Once the door state is changed, if the door was opened from an inside or outside to identify, the algorithm considers number of proximity and motion sensor values before the door state is changed . After the initial state change the algorithm keeps observing the door for a specific interval of time. It is confessed as "door observation time"; the door state during this time is called intermediate state of the door. During the door observation time, the algorithm observes the motion and proximity sensor values to identify the user actions at an access point. Leave the door open and the motion and proximity sensors after opening the door can be triggered to come back into the house. Leave the door open and step outside the home ,the motion and proximity sensors after opening the door without triggered. This leaves the home vulnerable to intruders, the home state is changed to empty so after a fixed amount of time, so a user will have to verify his identity upon re-entry into the home. Before changing the state of the home the algorithm issues a warning,the impending state change can be inform to the user.The proximity of the door to public areas and user preference the state change time of the algorithm can vary depending on the physical location of the home .The algorithm allows the step out and close the door behind him within door observation time after the door is closed without triggering the motion and proximity sensors. Close the door from the inside within the door observation time allowed by the algorithm and comes back in,after the door is closed triggering the motion and proximity sensors.

Primary Access:

Fig.3(a) plan of the sensor deployments in the primary access

4.2.Secondary Access Points

The secondary access points are in a home like the balcony door and windows. In a typical home, the balcony door is not used as the main access point to and from a home. Usually balcony door opens into a relatively secure and private area, sometimes even a few floors up. So, when the house is occupied ,these balcony doors can remain open for long periods of time. When the home becomes empty an observant, resourceful and proficient intruder can use this door to gain access to the home, in order to avoid that, when the home becomes empty,the balcony doors must be closed. Moreover, the balcony door should not be opened under any circumstances when the home is empty. When the balcony door is opened the system triggers intrusion defense mechanisms without waiting for any identity verifications,the algorithm keeps monitoring the state of the balcony door in an empty home.

Windows are opened from an inside under normal circumstances in a typical home. So, we can identify if windows are opened from inside or outside by placing motion and proximity sensors near the window inside the home. The strategical deployement of proximity and motion sensors should be the window cannot be opened from inside without triggering them. Similar to balcony doors, when the home is empty , windows in a home should not be opened, so the system triggers the intrusion defense mechanisms without waiting for identity confirmation when the home is empty and the window is opened. In addition, when the home is occupied and the window is opened from the outside without triggering the motion and proximity sensors placed near the window, the system triggers a warning and asks the user to confirm his identity because under normal circumstances windows are rarely opened from the outside.

Secondary access:

Fig.3(b) plan of the sensor deployments in the secondary access

5. HARDWARE AND EXPERIMENT SETUP

The data can be gathered by using of Arduino Uno microcontroller with ATmega328P IC at the access point. Arduino Uno module has fourteen digital input/output pins (6 of that can be used as Pulse Width Modulation (PWM) outputs), six analog inputs, a USB connector port, a 16 MHz ceramic resonator, a power jack, an In-Circuit Serial Programming (ICSP) header, and a reset button. Arduino Uno is flexible and offers a variety of digital and analog pins, it can be connected to a PC using USB, and it can run in standalone mode or as an interface connected to a PC. Arduino Uno is cost effective and is an open-source project backed up by a strong online community. Each microcontroller in the experiment is

connected to a PC using USB and programmed using the Arduino Interactive Development Environment (IDE).At the doors and windows to sense the state of doors and windows are used by Micro Contact/Limit Switch . The user activities inside the home near an access point can be monitored by using of Adjustable Passive Infrared (PIR) Motion Sensors and HC-SR04 ultrasonic range sensors capable of noncontact measurement from 2 cm to 400 cm.To obtain the various logical sensing parameters in the primary access point consist of wires to proximity, motion and contact sensors. The board is connected to the Arduino Uno module and the power can be supplied by Arduino Uno to the sensors.Arduino Uno microcontroller and ZigBee communication module are connected together. Board I is deployed in the primary access, it is connected to MQ 9 carbon monoxide sensor, DHT 11 temperature and humidity sensor Fig.1(a) shows the board I and microcontroller deployment at Primary Access Point and Fig.1(b) shows Board II is deployed near the secondary access point.Two contact sensors, a motion and proximity sensors are banded together with Board II.Out of these contact sensors,one is connected to window and another one is coupled balcony door. All the ZigBee modules implemented by using AES encryption, to enhance security, the coordinator is configured not to allow unsecured joins to the network, so under no circumstances the encryption key is sent as plain text over the air.

6. PROPOSED SYSTEM

During the operation,the various access points in a home to identify different improbable scenarios within a smart home. Entering and existing of a home can be done by access points are inherent in the structure of a home. These natural access points are front door, back door, balcony doors and windows in a typical home.Thus proposing a smart home security by means of Integrating Logical Sensing. The user behaviors at various access points are detected and difference between normal and attacker are predicted by using various microcontrollers and sensors. Based on the usage of certain places primary and secondary access points in a home are determined. In these access points all user actions are recognized. Understanding user behavior at each succeeding stages of an access point.By utilizing our logical sensing algorithm, the user behavior at various access points are analyzed and attack behavior is identified .When the door closed,then the motion sensor will gets trigger and start monitoring .The microcontroller gets multiple Proximity and Motion Sensor values afer that the Door State is changed.When the door is opened it Starts Door Observation Timer. Continue supervising the Primary Access points. After the door's final state change ,the values of intermediate and final states of the door along with sensor are identified. To identify the changes in intermediate state, we need to keep observing primary access point state continuously. After the door state changes, Motion and Proximity Sensor values are collected. Whether the state of the home is empty or not, that can be determined by applying the Logical Sensing algorithm in the gathered sensor values .Then if the Home was Empty and User Entered the Empty Home, by passing the fingerprint verification. When the home State Changed from Occupied to Empty, the secondary access point starts its monitoring process for intrusion detected .Finally the process terminates.To implement the verification subroutine, we need to start the activation timer. After that the mechanism is activated.When the user Passed fingerprint authentication, User Identity Confirmed. Reset the door state.Change Home Status to, "Occupied". Reset all previous states.Finally ends the process.The proposed work observes primary and secondary access points to identify logical sensing parameters and detect intrusion and does not cause inconvenience to the user with wearable tags or id. It offers implementation ease and flexibility compared to the previously proposed security system. The system requires minimal user input to identify when the home becomes empty or occupied, it was able to observe various access points in the home and deduce the change of state of the home. The algorithm was able to successfully predict home state changes and activate identity verification mechanisms when necessary. All the ZigBee wireless communication used in the work is encrypted using 128 bit AES encryption and the encryption key is never exchanged in clear text over the air, so an eavesdropping attacker will not be able to gain access to the system and manipulate it. Utilized the context aware computing to improve home security.The privacy and security concerns raised in the user context is identified by saving, analyzing and sharing data regarding user behavior and context . The algorithm was also able to identify secondary access point actions initiated by the user and was able to distinguish them from intruder action Verification of user from remotely control via an Internet of things.

7. RESULT AND ANALYSIS

The primary and secondary access points were observed by the proposed work to identify logical sensing parameters and to detect an intrusion.It doesnot cause any inconvenience to user with wearable tags or laser grids.When comparing with security system proposed by B.Schilit[] ,this offers easy implementation and flexibility.To identify whether the home empty or not,it requires minimal input.It was able to follow different access point and draw as conclusion from known facts the change of state.The home state changes and identify verification mechanism verified and activated by the algorithm.

In their research, B. Fouladi [2] gained access and manipulate the system by eavesdropping on the ZigBee communications in the home network and was able to capture the encryption key in plain text. All the ZigBee wireless communication used in the work is encrypted using 128 bit AES encryption and the encryption key is never exchanged in clear text over the air, so it is impossible to gain access to the system and manipulate it

for an eavesdropping attacker. O.Yurur et al.[13] proposed that context aware sensing vary depending upon user environment ,prior knowledge of recent event patterns. In home environment, it is unpredictable ,it is extremely challenging to predict the context of various user actions. It needs depth knowledge of context, and requires sophisticated sensing techniques and high processing power. So this smart home system with context aware sensing became high expensive because of breakthrough sensing techniques and high processing power . So it is complex to implement. S.Morsalin et al.[15] proposed a home security system that users Near Field Communication[NFC] tag, password, and fingerprint. Global system for Mobile module which also embedded in the system, that communicates with the logged password to a remote server using Machine to Machine communication .Each time the user wants to access his home he has to enter the password and verify the fingerprints. But it was inconvenience to use the NFC tag that mentioned in the work could be misplaced by careless user or stolen by an attacker.In our proposed work,Arduino Uno is kept inside the home as a database to store the data.And the data is secured with authorized access using some physical locks.To improve the security ,the data can be encrypted and the stored data can be never shared.

8. CONCLUSION

The paper detects user actions at primary and secondary access points in a home using different sensors. These detected user actions and behaviors are compared with normal user behavior at various access points to identify intrusions or intrusion attempts. In the webpage user was able to view the intrusion attempts and the presence of fire.

It is possible for the user to control the door opening from anywhere through the internet. The alert was send to the user if any one attempts to enter the home without authentication. By implementing these, fourteen alert generated. Out of these six regarding secondary access points and the other eight were relating to primary access point when the intrusion detected. In addition to identifying intrusions in home, the algorithm also warns user about imminent and live potential security vulnerabilities by identifying the status of various access points, user position and behaviors.

For future works, to improve smart home security, we plan to improve user behavior prediction by analyzing various access points inside the home.

REFERENCES

[1] C.Suh and Y.B.Ko,"Design and implementation of intelligent home control systems based on active sensor networks," *IEEE transactions on consumer electronics*,vol .54,no.3,pp.1177-1184,2008.

[2] B.Fouladi, S. Ghanoun, "Security Evaluation of the Z-Wave Wireless Protocol," *Black hat USA*, Aug. 2013

[3] N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 19331954, Fourthquarter 2014.

[4] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", *Ad Hoc Networks*, vol. 1, pp. 293–315, 2003.

[5] Y. Hu, A. Perrig, D. Johnson, "Wormhole attacks in wireless networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–380, Feb. 2006.

[6] D.Deadman, "Forecasting residential burglary," *International Journal of Forecasting*, vol. 19, no. 4, pp. 567–578, 2003.

[7] A.C Jose, R. Malekian, N.Ye, "Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home", *IEEE Access*, vol. 4, October 2016

[8] D. M. Konidala, D.-Y. Kim, C.-Y. Yeun, and B.-C. Lee, "Security framework for RFID-based applications in smart home environment," *Journal of Information Processing Systems*, vol. 7, no. 1, pp. 111–120, 2011.

[9] S.R. Das, S. Chita, N. Peterson, B. Shirazi, "home automation and Security for Mobile Devices," *IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp. 141-146, 2011.

[10] S. Saha, "Consideration Points: Detecting Cross-Site Scripting", (IJCSIS) *International Journal of Computer Science and Information Security*, Vol. 4, No. 1 & 2, 2009.

[11] B. Schilit, N. Adams, R. Want, "Context-Aware Computing Applications," *WMCSA '94 Proceedings of the 1994 First Workshop on Mobile Computing Systems and Applications*, pp. 85-90, 1994.

[12] Jonghwa Choi, Dongkyoo Shin and Dongil Shin, "Research and implementation of the context-aware middleware for controlling home appliances," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 1, pp. 301-306, Feb. 2005

[13] O. Yurur, C. H. Liu and W. Moreno, "A survey of context-aware middleware designs for human activity recognition," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 24-31, June 2014.

[14] Y. Zhao and Z. Ye, "A low cost GSM/GPRS based wireless home security system," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 2, pp. 567–572, 2008.

[15] S. Morsalin, A. M. J. Islam, G. R. Rahat, S. R. H. Pidim, A. Rahman and M. A. B. Siddiqe, "Machine-to-machine communication based smart home security system by NFC, fingerprint, and PIR sensor with mobile android application," *3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, Dhaka, Bangladesh,2016, pp.1-6

[16] A.Z. Alkar, U. Buhur, "An Internet Based Wireless Home Automation System for Multifunctional Devices"*IEEE Transactions on Consumer Electronics*, vol. 51, no. 4, pp.1169-1174, Nov. 2005