Improving Smart Home Security; Integrating Logical Sensing into Smart Home

Arun Cyril Jose, Reza Malekian, *Senior Member, IEEE*

Abstract—**The paper explains various security issues in the existing home automation systems and proposes the use of logic based security algorithms to improve home security. The work classifies natural access points to a home as primary and secondary access points depending on their use. Logic based sensing is implemented by identifying normal user behavior at these access points and requesting user verification when necessary. User position is also considered when various access points changed states. Moreover, the algorithm also verifies the legitimacy of a fire alarm by measuring the change in temperature, humidity and carbon monoxide levels, thus defending against manipulative attackers. The experiment conducted in this paper used a combination of sensors, microcontrollers, Raspberry Pi and ZigBee communication to identify user behavior at various access points and implement the logical sensing algorithm. In the experiment the proposed logical sensing algorithm was successfully implemented for a month in a studio apartment. During the course of the experiment the algorithm was able to detect all the state changes of the primary and secondary access points and also successfully verified user identity 55 times generating 14 warnings and 5 alarms.**

Index Terms— **Home automation, Smart homes, Wireless sensor networks, Access control, ZigBee.**

I. INTRODUCTION

RESEARCHERS have been experimenting and improving the concept of smart home since the late 1970s. As technology advanced with time, electronic devices and internet became more popular and affordable, so the concept of home automation and people's expectation from a smart home has changed dramatically. Modern smart home is a sophisticated combination of various Ubiquitous Computing Devices and Wireless Sensor/Actor Networks [1]. All these new user expectations, complicated electronics and unpredictable user behavior brought new security challenges to the home automation front. The concept of home automation security has also evolved with time, sensors and actuators were integrated into the home to detect, alert and prevent intrusions. In the past, an average home had to deal with common slash and grab criminals, while a modern home has to deal with sophisticated and tech savvy attackers who know how to find vulnerabilities and manipulate the security devices to gain access or cause distress to the inhabitants [2].

Despite smart home security being critical there are some vulnerabilities in the existing systems [3] [4]. Over the years researchers demonstrated various security issues associated with the devices and technology used in modern smart homes. The wireless sensor networks deployed in modern smart homes for device to device communication is vulnerable to various Routing [5] and Wormhole attacks [6]. Popular communication technologies like ZigBee and 802.15.4 used in smart homes are susceptible to Replay attacks [7]. All these factors contributed to the rapid rise in home burglaries over the past decade [8] [9] and demonstrates the importance of Home Security in the modern world. Our previous works in smart home security [10] [11] explains the changing role of modern home security systems and defines the role of a modern home automation system as, one capable of identifying, alerting and preventing intrusion attempts in a home at the same time preserving evidence of the intrusion or attempted intrusion so that the perpetuator or perpetuators can be identified and prosecuted.

Novelty: Ideal way to improve home security and defend against intrusion is to recognize a home's authorized inhabitants and identify their position inside a home at all times without inconveniencing its inhabitants. This is extremely challenging and complex, given the unpredictable nature of human behavior and home being occupied by guests and other trusted people. Identifying access points to a home and regulating access to them is the next logical step towards securing a home. The paper proposes that, normal user behaviour at access points to a home adhere to a set of predictable behaviours. These user behaviors when analyzed by our novel logical sensing algorithms can differentiate between normal and attack behaviors.

Objectives of the work:

- Distinguish between primary and secondary access points in a home based on how they are used. Detect all user actions at these access points.
- Understand user behavior after change in state of an access point.
- Identify and isolate attack behavior by analyzing the user behavior at various access points using our logical sensing algorithm. Trigger warning or raise alarms depending on the situation.

This work was supported in part by the National Research Foundation, South Africa, under Grant IFR160118156967, in part by the University of Pretoria's Post Graduate Research Support Bursary.

Arun Cyril Jose, is a PhD student at the Department of
Electrical Electronics and Computer Engineering, University of Pretoria,
South Africa.

Reza Malekian, is an Associate Professor with the Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa. (e-mail: reza.malekian@ieee.org, **Corresponding author**).

The proposed work uses Raspberry Pi, microcontrollers and sensors to detect and distinguish between normal and attack user behaviors at various access points.

Rest of the paper is organized as follows, Section II discusses different literatures on smart home security. Section III explains the methodology used to identify intrusions at primary and secondary access points. Section IV describes the experiment and hardware setup. Section V states the result of the experiment and discusses the experiment results along with advantage of the work. The paper concludes by stating future directions the research could take.

II. Related Works

The work of B.N. Schilit et al. [12] proposed the use of Infrared (IR) grids and wearable identification (ID) badges to identify the location of a user at home and predict the context of user actions. IR grid proved to be difficult to implement in a home environment while the wearable ID tags proved to be inconvenient and provided misleading information for inexperienced and careless users. The authors also proposed the use of static object checking in which an inhabitants location is identified with respect to a static object in a home. Static object checking severely limits the flexibility of the home environment and when these static objects are shifted the proposed system is easily fooled and is unable to adapt. The research of J. Choi [13] et al. utilized body temperature, pulse, facial expression, room temperature, time and location to predict and learn user context. Their work failed to take into account the fact that, user’s body temperature, pulse or facial expression may vary depending on various other factors like state of mind, illness etc. Moreover, their work uses cameras to read facial expressions which when compromised [14] by a tech savvy attacker brings new security and privacy issues to the home.

V. Bellotti et al. [15] suggested that, people tend to make impulsive decisions at times which can be unpredictable and unreasonable. Moreover, O. Yurur et al. [16] proposed that context aware sensing vary depending upon user environment, prior knowledge of recent event patterns, user perception and context. In a home environment where people are relaxed, impulsive and unpredictable it is extremely challenging to predict the context of various user actions. This makes context aware computing difficult to implement unless the system has in-depth knowledge of the context, which requires sophisticated sensing techniques and high processing power. Such advanced sensing techniques and high processing power makes context aware sensing an expensive proposition for smart homes. In addition, during context aware computing the system handles very intimate and private information about a user and his habits, which has to be shared for the concept to be implemented successfully, this raises serious privacy issues. The work of S. Saponara [17] demonstrated how an attacker can determine what devices are active in a home by looking at the power consumption at any given time. So it is risky and expensive to implement a completely context based security system in smart homes. So, this paper does not take into account the context in which the user makes a decision but focuses on user behaviours at various access points.

A. Alheraish [18] discussed a home automation security system using Short Messaging Service (SMS). The unauthorised access into the home is identified by monitoring the state of the home door using Light Emitting Diode (LED) and IR sensors. The proposed system also allows legitimate users to control home lights and set the 4 digit passkey using SMS. The LED and IR sensors used to identify intrusions could easily be spoofed by a sophisticated attacker. Informing the user about an intrusion via SMS is not a good practice, as the user may not be near to the phone to receive the alert on time.

In their work A.Z. Alkar and U. Buhur [19] developed a home automation system using Internet to provide remote access to homes and infrared technology for device communication within the home. They used RS232 as communication interface and proposed the use of SSL certificate to ensure server authenticity. The SSL certificate proposed by the authors opens the system up to issues like SSL certificate authority hacking, fake certificate authorities and certificate stealing. Moreover, username and password based access to home over the internet makes the home vulnerable to brute force [20], dictionary [21] and rainbow-table attacks [22].

S.R. Das et al. [23] proposed an iOS-based home automation security system using General Packet Radio Service (GPRS). The researchers developed an iOS application to run on the client device. The home devices and the iOS application are connected to the cloud which acts as the server. The system used video cameras, microphones, and motion sensors to provide security to the home. The video cameras are motion triggered and can be viewed by the user on their GPRS enabled devices using the client application or over a web browser. Accessing the security system over the web browser opens it up to a different set of browsing-related security issues like session hijacking, cookie stealing, and cross-site scripting [24] [25].

‘Smart Eye’ the central controller based security system proposed by K. Atukorala et al. [26] uses a real time home automation and monitoring system using GPRS. The proposed system alerts the user about an intrusion who in turn can view the home using a live camera. Each home is connected to the central server, the user sends control commands to server which the home system reads from the central server and executes. When a device at home changes state it sends the information to the central server, which the user can access. The central controller based security system proposed by S. Tsai et al. [27] called ‘Home Security System on Intelligent Network’ failed to implement any modern security hardware or did not consider defence against sophisticated intrusion attempts. A central controller based security system raises some serious privacy and security concerns considering the large scale user data available at the central controller and increases the potential for large-scale surveillance. Moreover, central controller based security systems are not feasible for single isolated home.

The work of D. M. Konidala et al. [28] suggested the use of

Radio Frequency Identification (RFID) tags for successfully identifying various items inside a smart refrigerator. This technique could be extrapolated to improve home security but it requires most items inside the home including home inhabitants fitted with RFID tags, which is inconvenient and difficult to implement considering forgetful human nature.

S. Lee et al. [29] used Infrared (IR) grid to identify inhabitant location inside a smart home. Their research used multiple IR sensors deployed on the ceiling to build an IR grid to predict inhabitant location inside a home. Later, H. H. Kim et al. [30] proposed the use of Bayesian classifier to improve the predicted inhabitant location accuracy inside the home. The work of P. Kumar and P. Kumar [31] utilized Arduino Uno microcontroller and IR motion sensor to identify intrusion attempts in a home, when an intrusion takes place the information is transmitted to the user using GPRS to their Personal Digital Assistant (PDA). In the proposed system, user has to be near their phone to be alerted to an intrusion attempt. Moreover, the IR sensors deployed by the researchers can be spoofed by skilled intruders. So, this paper, not only depends on IR motion sensor but also implements ultra-sonic proximity sensors, force sensors, contact sensors and gas sensors for intrusion detection.

Y. Zhao and Z. Ye [32] proposed a low cost and flexible home security system which alerts the administrator of an intrusion using SMS. Their approach lacks any sophisticated intrusion detection algorithms to identify attack attempts. The work of S. Morsalin et al. [33] suggested a home security system utilizing Near Field Communication (NFC) tag, passwords and fingerprints. The system also has an embedded Global System for Mobile (GSM) module which communicates the logged password to a remote server using Machine-to-Machine (M2M) communication. Each time a user wants to access his home he has to enter the password and verify his fingerprints which is an inconvenience. The NFC tag mentioned in the work could be misplaced by a careless user or stolen by an attacker.

P. H. Huang et al [34] proposed a fire detection and identification method by analysing video, which is expensive to be used in a smart home scenario. It also requires setting up video cameras inside the home which when compromised proves to be a serious threat to inhabitant privacy. The fire detection system used in this paper utilizes temperature and humidity sensors along with gas sensors to identify fire.

III. Method

In this paper, we analyzed various access points in a home to identify different improbable scenarios within a smart home during its operation. Access points are inherent in the structure of a home, which can be used for entering and exiting a home. In a typical home these natural access points are front door, back door, balcony doors and windows. Even though window is not a normal access point it can be used as one; most likely by an intruder depending on the situation. Physical access to a home is only possible through these access points unless serious structural alterations are made to a home. These serious structural alterations cannot be made without drawing attention to the act itself, like blasting or destroying a wall to create an entrance. So, managing access at these access points is crucial in securing a home. The paper proposes that, irrespective of the number and type of access points in a

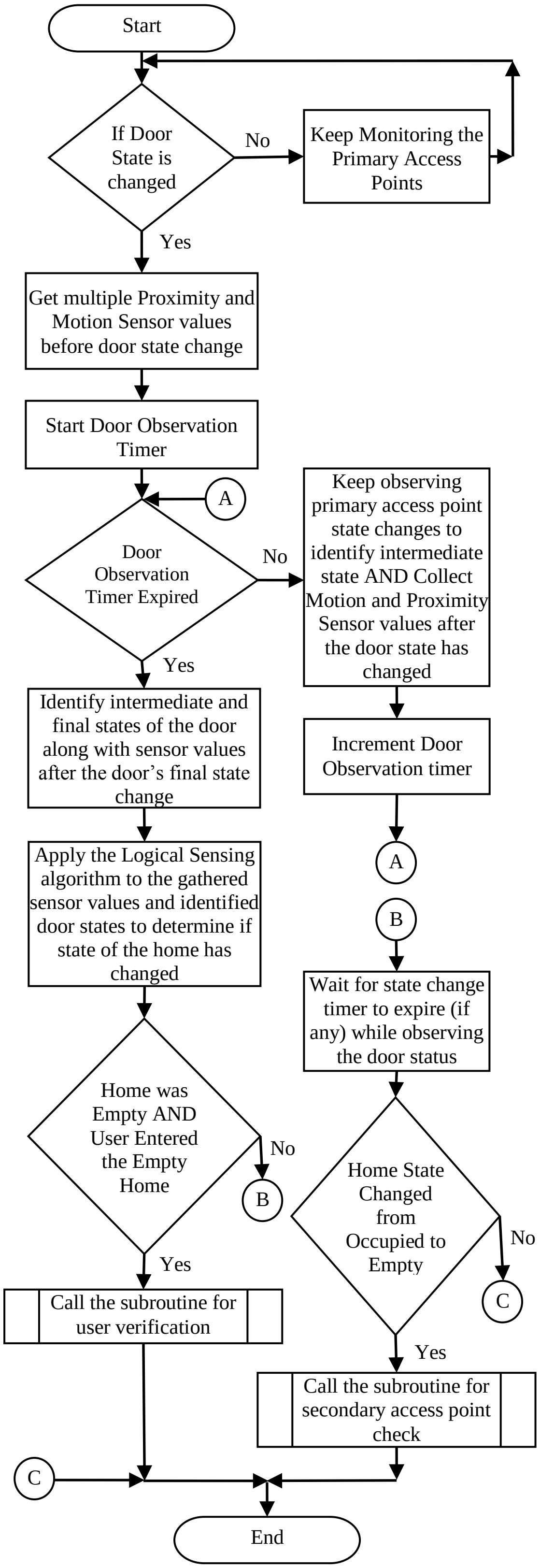

Start
If Door State is changed
No
Keep Monitoring the Primary Access Points
Yes
Get multiple Proximity and Motion Sensor values before door state change
Start Door Observation Timer
A
Door Observation Timer Expired
No
Keep observing primary access point state changes to identify intermediate state AND Collect Motion and Proximity Sensor values after the door state has changed
Yes
Identify intermediate and final states of the door along with sensor values after the door's final state change
Increment Door Observation timer
A
Apply the Logical Sensing algorithm to the gathered sensor values and identified door states to determine if state of the home has changed
B
Wait for state change timer to expire (if any) while observing the door status
Home was Empty AND User Entered the Empty Home
No
B
Home State Changed from Occupied to Empty
No
Yes
C
Call the subroutine for user verification
Yes
Call the subroutine for secondary access point check
C
End

Fig. 1. Flowchart showing door state changes and sensor operations of the primary access point.

home, the behavior of a legitimate user at these access points can be broken down in to a set of possible events which can be predicted.

Based on the purpose of the access points, the paper classifies access points into primary and secondary. In a home, when an access point is used by its inhabitants as a primary means to enter and exit from their home, it is categorized as primary access point like the front door, back door etc. On the other hand, secondary access points like the window, balcony door etc. also provide entry/exit to a home but they are rarely used for that purpose because there are other convenient ways in and out of a home for a legitimate user.

TABLE I
POSSIBLE STATES A MAIN DOOR COULD TAKE

State No	Initial State → Intermediate State	Final State	Motion Sensor Trigger		Proximity Sensor Trigger		Home Empty
			Before	**After**	**Before**	**After**	
1	C → O	O	✓	✓	✓	✓	F
2	C → O	O	✗	✓	✗	✓	F
3	C → O	O	✗	✗	✗	✗	F
4	C → O	C	✓	✗	✓	✗	F
5	C → O	C	✗	✗	✗	✗	F
6	C → O	C	✓	✓	✓	✓	F
7	O → C	C	✓	✓	✓	✓	F
8	O → C	C	✓	✗	✓	✗	F
9	O → C	C	✗	✗	✗	✗	F
10	O → C	O	✗	✗	✗	✗	F
11	O → C	O	✓	✗	✓	✗	F
12	O → C	O	✓	✓	✓	✓	F
13	C → O	O	✓	✗	✓	✗	F
14	O → C	C	✗	✓	✗	✓	F
15	C → O	C	✗	✓	✗	✓	F
16	O → C	O	✗	✓	✗	✓	F
17	C → O	C	✗	✓	✗	✓	T
18	C → O	O	✓	✓	✓	✓	T
19	C → O	O	✗	✓	✗	✓	T
20	C → O	O	✗	✗	✗	✗	T
21	C → O	C	✓	✗	✓	✗	T
22	C → O	C	✗	✗	✗	✗	T
23	C → O	C	✓	✓	✓	✓	T
24	O → C	C	✓	✓	✓	✓	T
25	O → C	C	✓	✗	✓	✗	T
26	O → C	C	✗	✗	✗	✗	T
27	O → C	O	✗	✗	✗	✗	T
28	O → C	O	✓	✗	✓	✗	T
29	O → C	O	✓	✓	✓	✓	T
30	C → O	O	✓	✗	✓	✗	T
31	O → C	C	✗	✓	✗	✓	T
32	O → C	O	✗	✓	✗	✓	T

A. Primary Access Point

Front door is the primary access point to any home, inhabitants use this door as the main way in and out of their home. Depending upon the architecture and inhabitant needs, there can be one or more primary access points. This paper proposes the use of motion and proximity sensors to detect user behavior at primary access points. When a user leaves an occupied home, the motion and proximity sensors placed near the access point inside the home are triggered before the door is opened. Once the user stepped out and closes the door the motion and proximity sensors will not be triggered. When someone enters an empty home, they are entering from outside so, the motion and proximity sensors will not be triggered before the door is opened. Once the door is opened and the user enters the home the motion and proximity sensors placed inside the home will be triggered. Fig. 1 shows the shows the flowchart of the door state changes and sensor operations of the primary access point.

Table I, shows all the possible initial states, intermediate states (represented by '→'), final states and motion and proximity sensor triggers before and after the state changes of the main door when the home is occupied and empty. Table II represents the special cases the algorithm could take during its operation. States in Table II are only triggered from a few particular previous state which are explained in this section (section III A). Motion and proximity sensors should be strategically placed so that, they will only be triggered by someone from inside the home and not by the act of opening or closing of the door. The sensor placements should also ensure that, anyone using the door to enter and exit the home cannot do so without triggering the motion and proximity sensors. The algorithm works by analyzing multiple proximity and motion sensor values before and after the door is opened or closed. The time period between the initial and final states of the door, the number of sensor values considered before the initial state and after the final states in the algorithm can vary depending upon the structure of the home and positioning of the motion and proximity sensors from the door.

Once the door state is changed the algorithm considers number of proximity and motion sensor values before the door state is changed to identify if the door was opened from the inside or outside. After the initial state change the algorithm keeps observing the door for a specific interval of time called 'door observation time'; the door state during this time is called intermediate state of the door. The algorithm observes the motion and proximity sensor values during the door observation time to identify user actions at an access point.

States 1 to 16 from Table I are triggered only when the home is occupied and states 17 to 32 occurs only when the home is empty. When the home is occupied and the user opens a closed door from the inside, the proximity and motion sensors are triggered on the way to open the door. After opening the door, the user can either:

(a) Leave the door open and come back into the house by triggering the motion and proximity sensors after opening the door (state 1 in Table I).

(b) Leave the door open and step outside the home without triggering the motion and proximity sensors after opening the door (state 13 in Table I). This leaves the home vulnerable to intruders, so after a fixed amount of time the home state is changed to empty, so a user will have to verify his identity upon re-entry into the home. The time taken by the algorithm to change the home state when the user steps out leaving the door open is called 'state change time'. Before changing the state of the home the algorithm issues a warning, informing the user about the impending state change. Depending on the physical location of the home, proximity of the door to public areas and user preference the state change time of the algorithm can vary.

(c) Step out and close the door behind him within door observation time allowed by the algorithm without triggering the motion and proximity sensors after the door is closed (state 4 in Table I). When state 4 occurs in a single person occupied home the state of the home changes from occupied to empty after the door observation timer has expired.

TABLE II
SPECIAL CASES

State No	Initial State → Intermediate State	Final State	Motion Sensor Trigger	Proximity Sensor Trigger	Home Empty	Algorithm Action
33	O → O	O	✓	✓	F	Reset/Start State Change Timer
34	O → O	O	✓	✓	T	Activate IVM

TABLE III
POSSIBLE NEXT STATE FOR A PARTICULAR STATE

State No	Possible Previous States	IVM Trigger	Timer Status
0	17, 19, 20, 27, 31, 32	No	None
1	0, 5, 6, 7, 9, 14, 15	No	None
2	5, 9	No	Reset State Change Timer
3	5, 9	No	Continue State Change Timer
4	0, 5, 6, 7, 9, 14, 15	No	None
5	5, 9	No	Continue State Change Timer
6	0, 5, 6, 7, 9, 14, 15	No	None
7	0, 1, 2, 10, 12, 16	No	None
8	0, 1, 2, 10, 12, 16	No	None
9	3, 10, 11, 13	No	Continue State Change Timer
10	3, 10, 11, 13	No	Continue State Change Timer
11	0, 1, 2, 10, 12, 16	No	Start State Change Timer
12	0, 1, 2, 10, 12, 16	No	None
13	0, 5, 6, 7, 9, 14, 15	No	Start State Change Timer
14	3, 10, 11, 13	No	Reset State Change Timer
15	5, 9	No	Reset State Change Timer
16	3, 10, 11, 13	No	Reset State Change Timer
17	4, 8, 17, 26, 22	Yes	Start Identity Verification Timer
18	Irrelevant	Alarm	Alarm triggered, so no Timer
19	4, 8, 22, 26	Yes	Start Identity Verification Timer
20	4, 8, 22, 26	No	None
21	Irrelevant	Alarm	Alarm triggered, so no Timer
22	4, 8, 22, 26	No	None
23	Irrelevant	Alarm	Alarm triggered, so no Timer
24	Irrelevant	Alarm	Alarm triggered, so no Timer
25	Irrelevant	Alarm	Alarm triggered, so no Timer
26	11, 13, 20, 27	No	None
27	11, 13, 20, 27	No	None
28	Irrelevant	Alarm	Alarm triggered, so no Timer
29	Irrelevant	Alarm	Alarm triggered, so no Timer
30	Irrelevant	Alarm	Alarm triggered, so no Timer
31	11, 13, 27	Yes	Start Identity Verification Timer
32	11, 13, 27	Yes	Start Identity Verification Timer
33	3, 10, 11, 13, 33	No	Reset/Start State Change Timer
34	20, 27	Yes	Start Identity Verification Timer

(d) Close the door from the inside within the door observation time allowed by the algorithm and comes back in, triggering the motion and proximity sensors after the door is closed (state 6 in Table I).

When the home is occupied and the door is open, it can be closed from the inside or from the outside. After closing the door depending on his position, user can either come back into the home or go out. These states are discussed below.

(e) User closes the door from the inside and comes back into the home. The motion and proximity sensors are triggered before and after the door is closed (state 7 in Table I).

(f) User closes an open door coming from inside and steps out of the home leaving the home empty. Since the door is closed coming from the inside motion and proximity sensors are triggered before the door is closed but the sensors are not triggered after the door is closed as the user has stepped out (state 8 in Table I). After triggering state 8, the state of the home changes from occupied to empty when the door observation timer expires.

(g) User closes an open door coming from the inside and opens it again within the door observation time and steps out of the home leaving the door open. The motion and proximity sensors are triggered before the door is closed as the user walks towards the door from inside the home. The user then opens the door making the previous door state (closed) the intermediate state and the current state (open) the final state. Sensors are not triggered after the final state, as the user executes the final state from outside the home. Since the user has stepped outside the home leaving the door open the ‘state change timer’ is started, which upon expiry changes the home state to empty (state 11 in Table I).

(h) The user closes an open door from the inside and opens it within the door observation time and comes back into the home. Like in state 11, the door is closed and opened within the door observation time making the former (closed) the intermediate state and the later (open) the final state. Motion and proximity sensors are triggered before the door is closed (initial state) and after the door is open (final state), as the user initially came from inside to close the door and went back into the home after leaving the door open (state 12 in Table I).

The proposed algorithm keeps monitoring the door and sensor values for different state changes. Some states like state 2, 3, 5 and 15 in Table I are only triggered when their previous states are either state 5 or state 9. Fig. 2 demonstrates the states the proposed system goes through before states 2, 3, 5 and 15 are triggered. State 2 is triggered when the user opens the door from the outside. Fig. 2 (a) shows state 2 transition; state 2 is triggered when the home is occupied and a closed door is opened without triggering the motion and proximity sensors before opening the door but the sensors are triggered after opening the door. In a single person occupied home, such an event will only take place, when the user steps out of a home leaving the door open (state 11 and state 13 in Table I) and within the state change timer expiry period states 5 or 9 are triggered. When state 2 is triggered it means the user re-entered the home leaving the door open, so the state change timer can be reset. Fig. 2 (a) also shows the transition of states 9 and 10.

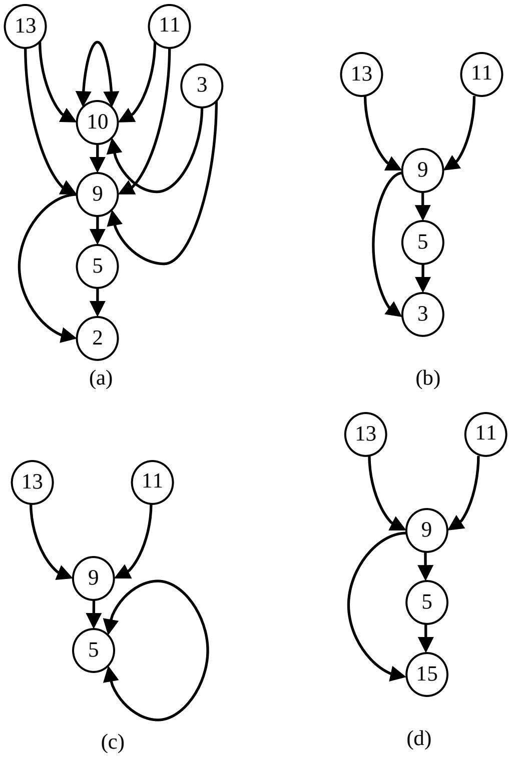


Fig. 2. (a) Shows State 2 transition along with state 9 and 10 transition; (b) State 3 transition; (c) State 5 transition (d) State 15 transition during the operation of the home.

Fig. 2 (b) shows state 3 transition; state 3 happens when the home is occupied and a closed door is opened without triggering the motion and proximity sensors before and after opening the door. In a single person occupied home, like state 2, state 3 will only be triggered if states 5 or 9 are triggered before the state change timer has expired. Fig. 2 (c) shows state 5 transition; state 5 transpires when the home is occupied and a closed door is opened and closed without triggering the motion and proximity sensors before or after closing the door. In a single person occupied home, similar to states 2 and 3, state 5 is only triggered if states 5 or 9 are triggered before the state change timer has expired. State 5 can be the previous state of state 5 or in other words state 5 can repeatedly happen until the state change timer has expired. Fig 2 (d) shows the transition of the system to state 15; state 15 is triggered when the home is occupied and a closed door is opened and closed. The motion and proximity sensors are not triggered before opening the door but the sensors are triggered after closing the door which indicates the user stepped back into the home after closing the door. So after triggering state 15, in a single person occupied home the state change timer is reset.

A single person occupied home becomes empty when states 11, 13, 4 and 8 are triggered. When states 11 and 13 are triggered the algorithm utilizes a state change timer as mentioned above in (b) and (g). When states 4 and 8 are triggered the home state is changed when door observation timer expires as mentioned above in (c) and (e). Door observation time is a relatively short period of time compared to the state change time.

When a particular state is triggered the previous state of the door is also considered to accurately determine the possible next states and the occupied status of the home. Table III shows the possible previous states for a particular state and timer actions in the proposed system when the home is occupied and empty. Whenever a home changes state from occupied to empty the algorithm checks if the secondary access points to the home are secure. If not it issues a warning to the user to secure the secondary access points. Fig. 3 shows the flowchart of the secondary access point checking when the home becomes empty.

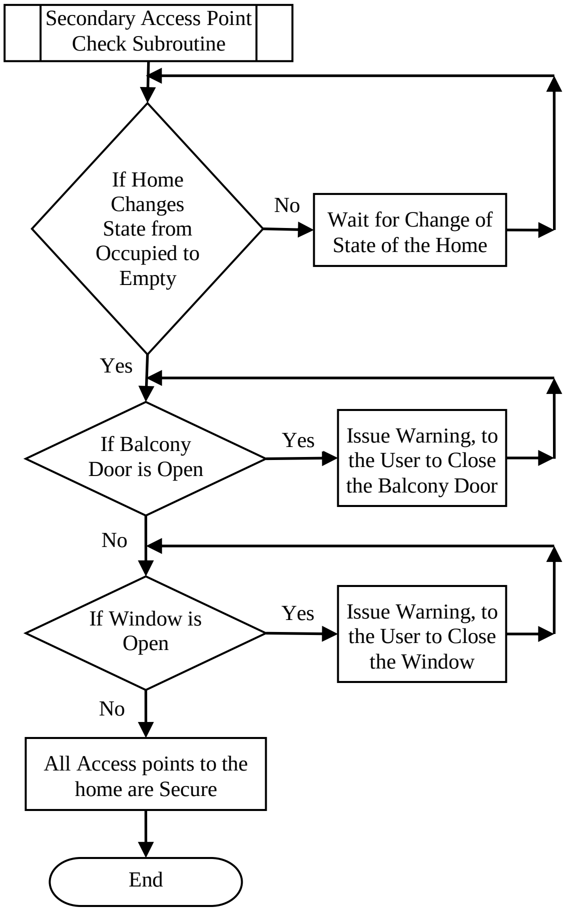

Secondary Access Point Check Subroutine
If Home Changes State from Occupied to Empty
No
Wait for Change of State of the Home
Yes
If Balcony Door is Open
Yes
Issue Warning, to the User to Close the Balcony Door
No
If Window is Open
Yes
Issue Warning, to the User to Close the Window
No
All Access points to the home are Secure
End

Fig. 3. Flowchart demonstrating secondary access point check when home becomes empty

State 10 is triggered when an open door is first closed then opened from outside without triggering the motion and proximity sensors before or after the initial and final states. State 10 is triggered when the previous states are states11, 13 or 3 and with state change timer still running. State 10 can also be the previous state of state 10 i.e. state 10 can repeat itself until the state change timer has expired. Similarly, states 9, 14 and 16 are only triggered when their previous states are either are 3, 10, 11 or 13. In a single person occupied home, triggering states 14 and 16 means the user has re-entered the home so the state change timer is reset.

Whenever states 3, 10, 11 and 13 are triggered (the door remains open and the state change timer is running) the algorithm keeps monitoring the front door and the sensors until another door state is triggered or until the state change timer is expired. When the user re-enters the home by triggering the motion and proximity sensors before the state change timer has expired without changing the door state (door still remains open), state 33 from Table II is triggered. As the user re-entered the home, the algorithm stops and resets the state change timer. Upon resetting the state change timer, the algorithm keeps observing the sensor values as the door is still open. When the user steps out of the home again without changing the state of the door (door still remains open), triggering the sensors state change timer is started, which on expiry changes the home state to empty. So state 33 can be its own previous state.

When a home changes its state from empty to occupied, the identity of the person causing the state change has to be verified. The techniques used for verifying user identity [35] can vary from simple 4 digit pin, facial recognition, retinal scan verification, fingerprint verification to sophisticated biometric gait recognition, vein recognition and voice recognition. There can be one or more Identity Verification Mechanism (IVM) depending on area secured, user preferences and security requirements. The user identification should be done within a fixed time period called the 'verification time period'. The verification timer stars once the door to an empty home is opened and someone enters, it stops when a valid user identity is confirmed. When the timer exceeds the verification time period an intruder alert is triggered. Depending upon the level of security and user preference the intruder alert can be an audible alarm to scare off intruders and alert the neighbors, silent alarm to alert the authorities or any other defensive measures. The 'verification time period' is subjective to user habits and location of the IVM. Fig. 4 explains the algorithm when door to an empty home is opened. Fig. 5 shows the identity verification process in the algorithm.

When the home is empty and the closed main door is opened from outside without triggering the motion and proximity sensors. After opening the door the user can either:

(i) Close the main door within the door observation time allowed by the algorithm and enter the home, triggering the motion and proximity sensors while walking into the home after closing the door (state 17 in Table I). When the home is empty and the user comes in after opening the door he will have to confirm his identity within the verification time period.

(j) Leave the door open and enter the home triggering the motion and proximity sensors while moving into the home (state 19 in Table I). The verification timer is triggered as soon as the door is opened so the user have to verify his identity using the IVM.

(k) Leave the door open and decides to stand at the door or go out of the house, without triggering the motion and proximity sensors (state 20 in Table I). After triggering state 20 the door remains open, so the algorithm keeps monitoring the motion and proximity sensors

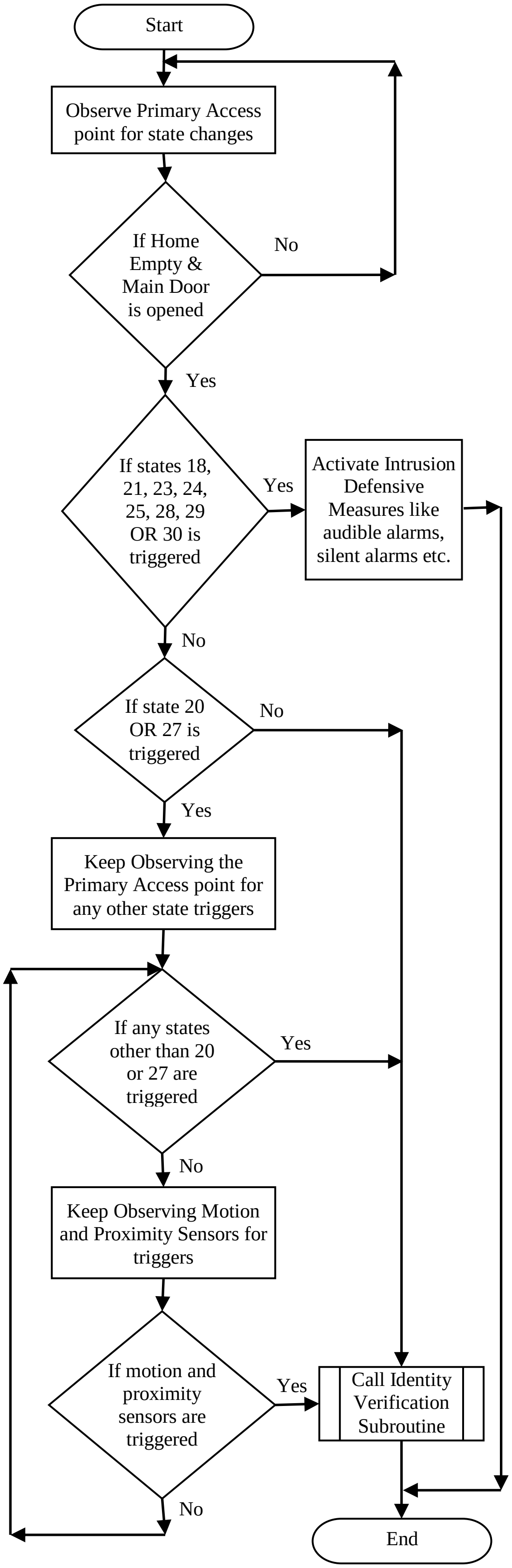

Start
Observe Primary Access point for state changes
If Home Empty & Main Door is opened
No
Yes
If states 18, 21, 23, 24, 25, 28, 29 OR 30 is triggered
Yes
Activate Intrusion Defensive Measures like audible alarms, silent alarms etc.
No
If state 20 OR 27 is triggered
No
Yes
Keep Observing the Primary Access point for any other state triggers
If any states other than 20 or 27 are triggered
Yes
No
Keep Observing Motion and Proximity Sensors for triggers
If motion and proximity sensors are triggered
Yes
Call Identity Verification Subroutine
No
End

Fig. 4. Flowchart explaining the algorithm when door to an empty home is opened

until another door state is triggered; whenever motion and proximity sensors are triggered immediately after state 20, it means someone entered the home through the open door triggering state 34 from Table II, so IVM is activated and user identity is verified.

(l) Closes the door within the sensing time allowed by the algorithm and steps out of the home without triggering the motion and proximity sensors after the door is closed (state 22 in Table I). So sensors are not triggered before the initial state or after the final state of the door and no one entered the home, so user identity is not verified, home remains empty and the door is closed.

State 18 is triggered in an empty home when the closed door is opened by triggering the motion and proximity sensors before and after the initial and final states. Similarly, state 23 happens when a closed door is opened and closed by triggering motion and proximity sensors before and after the initial and final states. State 24 is triggered when an open door is closed and the motion and proximity sensors are triggered before and after the initial and final states. Likewise, state 29 happens when an open door is closed and then opened triggering the sensors before and after the initial and final states. All the above states 18, 23, 24 and 29 occurs when the proximity and motion sensors are triggered before the door is opened, this will not happen in an empty home. So, when any of these states are triggered irrespective of the previous state, intrusion defense mechanisms are triggered without waiting for user identity confirmation.

States 21, 25, 28 and 30, occurs when the home is unoccupied and the closed door is opened from inside. In an empty home, this only happens when someone gains access to the home using a secondary access point or using some other means. So irrespective of previous states, intrusion defense mechanisms are triggered without activating IVM to confirm user identity.

When the state change timer expires after triggering states 11 or 13 the door is left open and the home becomes empty; the user can then trigger either states 26, 27, 31 or 32. State 26 is triggered when the user closes the open door without triggering the motion or proximity sensors, which means the door is closed from the outside and user stayed outside. Since there is no entry into the home the home status remains empty and there is no need for user identification. In state 27, the user closes and opens the door without triggering any sensors before or after the initial states, which indicates the door is closed and opened from the outside and no one has entered the empty home. Similar to state 26, in state 27 the home remains empty and no one enters the home so no user identification is necessary. State 27 can be its own previous state making it repetitive. After triggering state 27 the door remains open, so the algorithm keeps monitoring the motion and proximity sensors until another door state is triggered. Similar to state 20, whenever motion and proximity sensors are triggered immediately after state 27, it means someone entered the home through the open door, so IVM is activated and user identity is verified.

State 31 occurs in the system when the user closes an open door and comes back into the home triggering the motion and proximity sensors. The system is not sure about the identity of the person reentering the home so the IVM is activated to verify user identity. In state 32, the user closes an open door and then opens it and comes back in to the home triggering the motion and proximity sensors. Similar to state 31, after triggering state 32 user identity has to be verified.

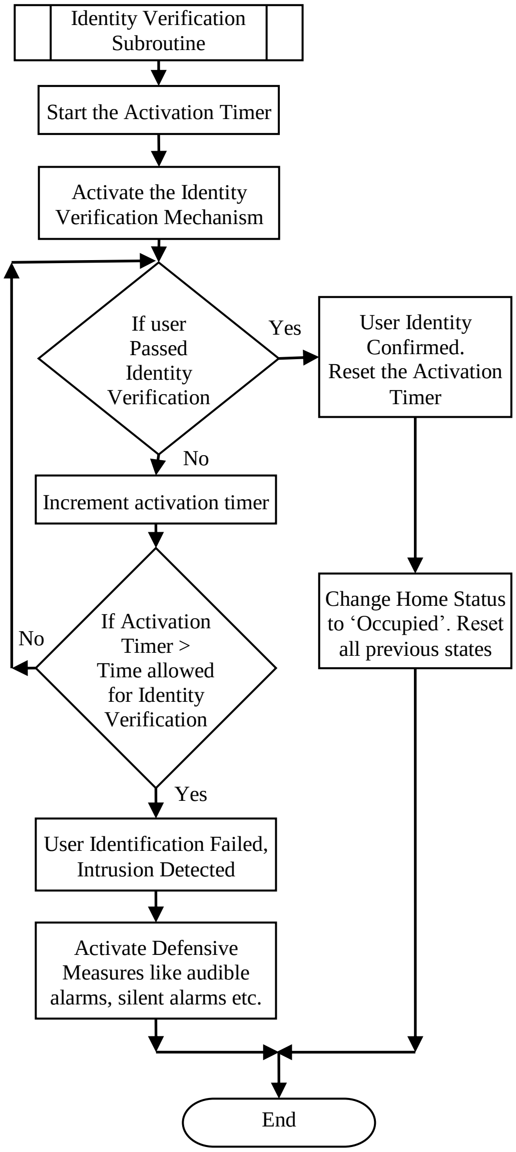

Identity Verification Subroutine
Start the Activation Timer
Activate the Identity Verification Mechanism
If user Passed Identity Verification
Yes
User Identity Confirmed. Reset the Activation Timer
No
Increment activation timer
If Activation Timer > Time allowed for Identity Verification
No
Change Home Status to 'Occupied'. Reset all previous states
Yes
User Identification Failed, Intrusion Detected
Activate Defensive Measures like audible alarms, silent alarms etc.
End

Fig. 5. Flowchart showing Identity Verification Process

After states 11 and 13, if user re-enters the home triggering the sensors after the state change timer has expired without changing the state of the door (door left open) the algorithm will activate the IVM to verify the identity of the user. The IVM is placed inside the home so whenever the user identity is successfully verified the home becomes occupied and all the previous states of the door are cleared and the current state is set to state 0.

If there are multiple primary access points in a home, in order to determine user actions at various access points, motion and proximity sensors has to be deployed at each of the access points. In a single person occupied home the user can only use one primary access point at a time to enter or exit from a home. The algorithm can be implemented at each of the primary access points independently. When more than one primary access point is open and user stepped out of the home leaving the door open, state change timer is started, the algorithm observes motion and proximity sensor readings at each of the open primary access points because the user can enter the home through any of the open primary access points. If the proximity and motion sensors are triggered at any of the open access points state change timer is reset. If none of the proximity and motion sensors are triggered then upon expiry of the state change timer the algorithm changes the home state to empty. When user reenters the home without changing the state of the door, special case 34 from Table II is triggered for that particular access point and IVM is activated and user is asked to confirm his identity. When primary access point states are changed by the reentering user, then corresponding state from Table I is triggered for that particular access point.

Status of other primary access points are only checked when the user closes a primary access point and the home state is changed to empty. If the user closes a primary access point and the home state is changed it could mean the user is leaving the vicinity of the home, so the algorithm checks the status of other primary and secondary access points and warns the user to secure them if they are open. If the user is leaving the primary access point open and stepped out through it and the home state is changed to empty after the expiration of the state change timer, it means user is likely close to the home, so other primary access point status is not checked to warn the user. When he reenters the empty home, IVM is triggered and user identity is verified regardless of the state of any other primary access points.

When multiple access points are open and the user stepped out of the home through one access point leaving it open and enters the home through another open access point without changing its state before the state change timer expires triggering special state 33 from Table II for that particular access point. If user changed the state of the primary access point through which he entered corresponding states from Table I are triggered for that access point. The time difference between the motion and proximity sensor triggers from each of the access points used by the user to exit and enter the home is considered along with the distance between access points to distinguish between normal user behavior and sneaky attack behavior. The algorithm takes into account the minimum time required by the user to move between the access points to identify attack behaviors.

B. Secondary Access Points

The balcony door and windows form the secondary access points in a home. 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, these balcony doors can remain open for long periods of time when the house is occupied. 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, balcony doors must be closed when the home becomes empty. Moreover, when the home is empty the balcony door should not be opened under any circumstances. The algorithm keeps monitoring the state of the balcony door, so in an empty home when the balcony door is opened the system triggers intrusion defense mechanisms without waiting for any identity verifications.

In a typical home windows are opened from the inside under normal circumstances. So, by placing motion and proximity sensors near the window inside the home we can identify if windows are opened from inside or outside. The proximity and motion sensors should be strategically deployed so that the window cannot be opened from inside without triggering them. Similar to balcony doors, windows in a home should not be opened when the home is empty, so when the home is empty and the window is opened the system triggers the intrusion defense mechanisms without waiting for identity confirmation. 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.

The proposed system also observes the bed in which a user sleeps in to determine if the user is in bed or not. The algorithm observes reading from the force sensors placed underneath the mattress to determine if a user is occupying the bed. Various force sensors are placed underneath the mattress to identify force at different areas of the bed. The algorithm considers these sensor readings to distinguish between users occupying a bed and foreign objects placed on the bed. Highly accurate measurement of force underneath the bed is not necessary to identify when a bed is occupied and distinguish between user and foreign objects on the bed. When the bed is empty the force on the bed is significantly less compared to when it is occupied by the user.

In a single person occupied home if any of the access point states are changed when the user is in bed it indicates an intrusion to the home. The chance of intrusion significantly increases if this happens during night as most intruders prefer the cover of darkness to infiltrate their targets. So, if the user is in bed and any of the primary or secondary access point states are changed during night between 10:00 p.m. and 6:00 a.m. the algorithm activates intrusion defense mechanisms without waiting for identity verification. When this happens during the day between 6:01 a.m. and 9:59 p.m. the algorithm triggers a warning indicating the change of state of the access point and the user is asked to confirm his identity. The time of the day for alarm trigger can be varied depending upon user preference, location of the home, outside accessibility to secondary access points etc. In some cases an open balcony door or window may be closed without user interference even when the user is in bed due to wind, so in the proposed system this scenario is also considered before identifying intrusion.

Even when there are more than two secondary access points, the algorithm can identify intrusion attempts in real time by observing each secondary access points individually and implementing the logical sensing algorithm for windows and doors and considering user position in bed when necessary.

C. Fire Alarm

The work of B. Fouladi [2] discussed the weakness in the existing smart home architecture and demonstrated how an attacker will compromise various networked elements in a home. The easiest way to get the inhabitants out of a home is to trigger an emergency alarm like the fire alarm. When a fire alarm is triggered all the automatic locks of a home are disabled. During home fire the carbon monoxide and the ambient temperature levels in the area of the fire will go up and inversely the humidity in and around the area will go down. If there is no change in humidity, temperature or carbon monoxide levels, the algorithm warns the user about a possible attack attempt which the user can verify.

Each twelve second average of the temperature, humidity and carbon monoxide sensor readings are compared to detect fire. If there is more than 2^o difference between the twelve second average temperatures and more than 3% difference in twelve second average humidity then the triggered fire alert is validated. It takes around 24 hours for the carbon monoxide sensor to stabilize, so carbon monoxide readings are only considered once the system had been activated for at least 24 hours. If the average Rs/Ro resistance value of the MQ 9 gas sensor employed is less than 8.9 over the twelve second period, the fire alarm triggered is confirmed. Whenever a fire alarm is triggered the proposed algorithm checks the carbon monoxide, temperature and humidity levels in the area of the fire to make sure the alarm is triggered by fire and not by a manipulative attacker. The proposed system implements MQ 9 gas sensors, temperature and humidity sensors to detect fire in the home.

Warnings are triggered as a means to get user attention when something out of the ordinary happens. In the proposed system warnings are generated when: (a) user leaves the door open to a home and steps outside, also the state change timer is about to expire; warning is triggered when there is 20 seconds remaining in the state change timer as a means to let the user know, the home is about to change its state to empty soon. Upon receiving the warning user can either, step back into the home triggering the motion and proximity sensors or choose to ignore the warning and let the home become empty when the state change timer runs out. (b) The home becomes empty and at least one of the secondary access points are unsecure; the algorithm warns the user about the open secondary access point. Upon receiving the warning the user comes back into the home and secures the secondary access point. The warning will not stop until all the secondary access points are secured. (c) One or more of the secondary access point windows are opened from the outside when the home is occupied. Identity verification timer is activated and the user is asked to confirm his identity because under normal operating conditions windows are rarely opened from the outside. (d) Any of the secondary access points changed states between 6:01 a.m. and 9:59 p.m. when the user is in bed. User is asked to confirm his identity and identity verification timer is started because during the day when the user is in bed it is unlikely that secondary access points changes states when the user is in bed. (e) Fire alarm is triggered without sufficient change in humidity, ambient temperature or carbon monoxide levels. The warning informs the user about a possible fire alarm manipulation which user can verify on sight.

An alarm is triggered when the algorithm is sure there is an intrusion in the home. Alarms are usually triggered when the user fails to confirm their identity within the identity verification time or failed thrice consecutively with their identity verification attempts. When the primary access point is opened from the inside when the home is empty the algorithm doesn’t wait for any identity verification to sound the alarm. Similarly, when any of the secondary access points are opened when the home is empty alarm is triggered without waiting to confirm user identity. When the user is in bed and any of the closed secondary access points changed states between 10:00 p.m. and 6:00 a.m. alarm is activated without waiting for user identity confirmation. The algorithm uses alarm as the primary intrusion alert mechanism.

When there are multiple occupants in a home the states of the main door remains the same. When a situation arises that changes the home state to empty, the user is asked to confirm the empty state change. When the home is non-occupied the user confirms the state as empty and the algorithm changes the home state to empty. When the home is empty irrespective of the number of inhabitants the defensive mechanisms proposed in Section III are applicable. When there is an additional inhabitant in the apartment the secondary access point behavior during day and night changes. If the inhabitants are using the same bed to sleep in, then the corresponding force sensor values when they both occupy the bed together and individually is analyzed to determine the occupancy of inhabitants in the bed during night. If both of them are in bed and any of the closed secondary access points are opened during the night (10:00 p.m. and 6:00 a.m.) alarm is triggered and if it happens during the day (6:01 a.m. and 9:59 p.m.) a warning is triggered and the algorithm asks the user to confirm their identity. If inhabitants are using different beds, force sensor readings from different beds are considered to determining user occupancy in bed.

IV. Hardware and Experiment Setup

The proposed access monitoring and control mechanism at home is implemented using Raspberry Pi 3 which has 4× ARM Cortex-A53 processor operating at 1.2GHz, Broadcom VideoCore IV graphics processor, 1GB LPDDR2 (900 MHz) built in RAM, one 10/100 Mbps Ethernet port, 2.4GHz 802.11n built in wireless adapter and a 32GB class 10 micro Secure Digital (SD) Card as the hard disk storage. The Pi works on a Raspbian Operating System (OS) optimized for Raspberry Pi. The OS is burned on to the SD card from a laptop which is then inserted into the Pi. The algorithms are implemented using Java as the programming platform and MySQL as the database. Java 7 JDK (Java Development Kit) and MySQL are installed in the Raspberry Pi from Debian repositories using the APT (Advanced Packaging Tool) commands with root user permissions.

At the access point Arduino Uno microcontroller with ATmega328P IC is used to gather data. Arduino Uno module has fourteen digital input/output pins (6 of which 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 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 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).

A Micro Contact/Limit Switch is used at the doors and windows to sense the state of doors and windows. Adjustable Passive Infrared (PIR) Motion Sensors and HC-SR04 ultrasonic range sensors capable of noncontact measurement from 2 cm to 400 cm are used to identify user activities inside the home near an access point. Every living thing with temperature above absolute zero emits heat energy in the form of radiation, this may be invisible to the naked eye but can be detected by PIR sensors. The PIR sensors implemented here has a field of view less than 180^o.

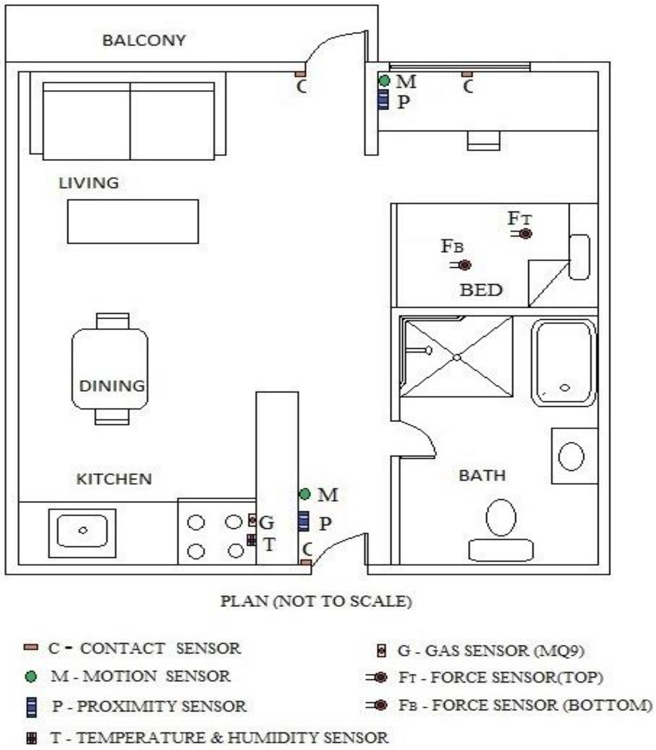


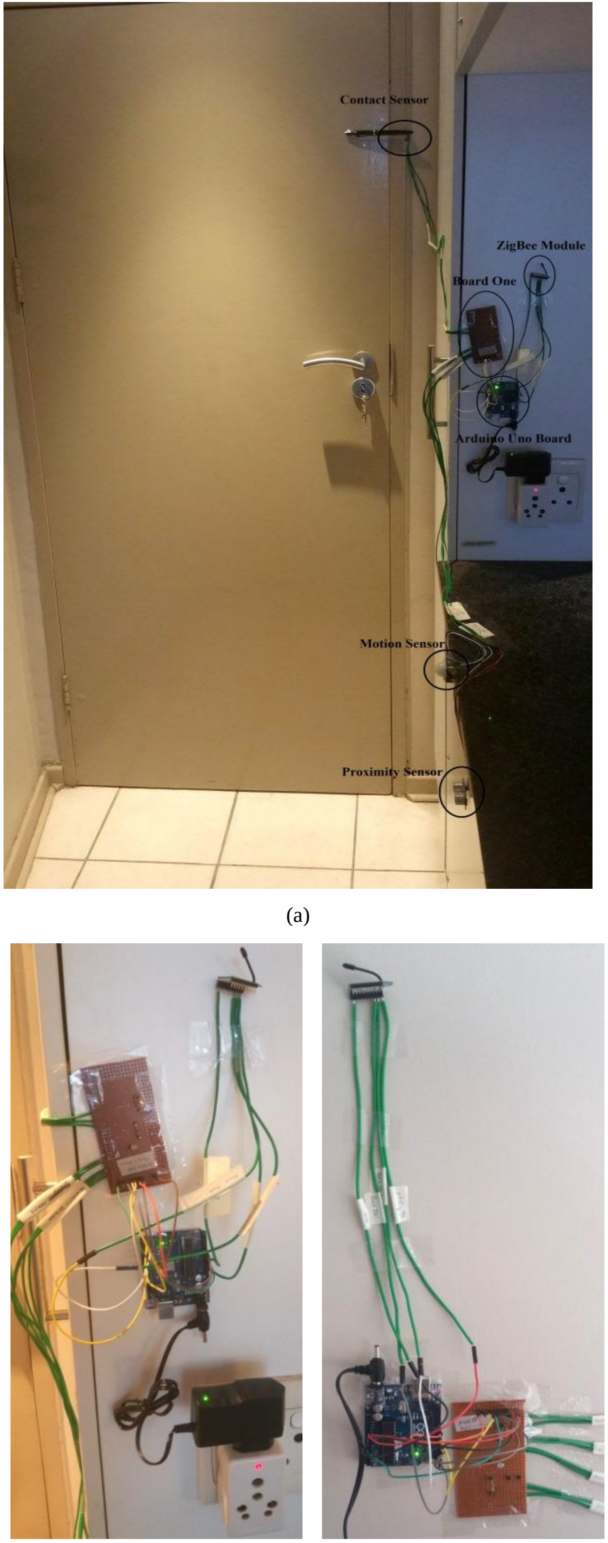
Fig. 6. Plan and location of the sensor deployments in the apartment.

The communication between the microcontroller and the Pi is wireless. Wireless communication technology is easy to install and reduces system cost. We considered various wireless technologies like Wi-Fi and Bluetooth. Wi-Fi was discarded because of its high power consumption and high cost, while Bluetooth was discarded because of high power consumption, limited range and security issues [36]. The proposed system is implemented using ZigBee technology based on the IEEE 802.15.4 standard with a communication range varying from 10 – 100m. ZigBee allows large-scale network configurations and utilizes low power radio with a data-rate capability of 250 kb/s. These features makes ZigBee the ideal communication technology in smart home networks. Moreover, many secure communication techniques with ZigBee [37] – [39] were suggested and successfully implemented. This makes ZigBee a comparatively secure wireless communication technology.

The experiment is conducted in a studio apartment over one month time period. The apartment is situated on the second floor of a six story flat complex. The balcony door opens to a 15 square feet small balcony on the second floor. Physical access to the balcony is only possible through the home or by scaling the building. The front door opens to a common area which all the inhabitants of the flat complex has access to. The window of the apartment is on the second floor so under normal circumstances it will not be opened from the outside. An open balcony door or window has a chance of being closed by wind but under no circumstances a closed window or door will be opened without human interference. The main door which is the primary access point cannot be closed or opened without user interference. Four major points in the home were considered to obtain logical sensing parameters [40, 41], namely; primary access point (the main door to and from the apartment), secondary access points (balcony door and window), the bed in which user sleeps on, the kitchen where the fire detection parameters are collected. Fig. 6 shows the plan and location of the sensor deployments in the apartment during the experiment.

Four boards are designed to obtain logical sensing parameters. Board I is deployed near the primary access point. It consist of wires to proximity, motion and contact sensors to obtain various logical sensing parameters. The board is connected to the Arduino Uno module which supplies the power to the sensors. The Arduino Uno microcontroller is then connected to a ZigBee communication module [42, 43]. Fig 7 (a) shows the board I and microcontroller deployment at Primary Access Point and Fig. 7 (b) shows board one installation at the primary access point [44]. Board II is deployed near the secondary access point. It is connected to two contact sensors, a motion and proximity sensors. Each of the contact sensors are connected to window and balcony door. The motion and proximity sensors are deployed near the window to identify user movements before the window is opened. Board II also has provisions to be connected to Board IV which is connected to the force sensors in the bed. Similar to board I, board II is also connected to Arduino Uno microcontroller which powers the board and communicates the sensor values to the Pi using ZigBee module. Fig. 7 (c) shows board two installation at secondary access points and Fig. 8 (a) shows board II and microcontroller deployments at secondary access point.

Board III is deployed in the kitchen, it is connected to MQ 9 carbon monoxide sensor, DHT 11 temperature and humidity sensor. Board III is designed to measure the carbon monoxide, temperature and humidity levels in the area to detect fire.

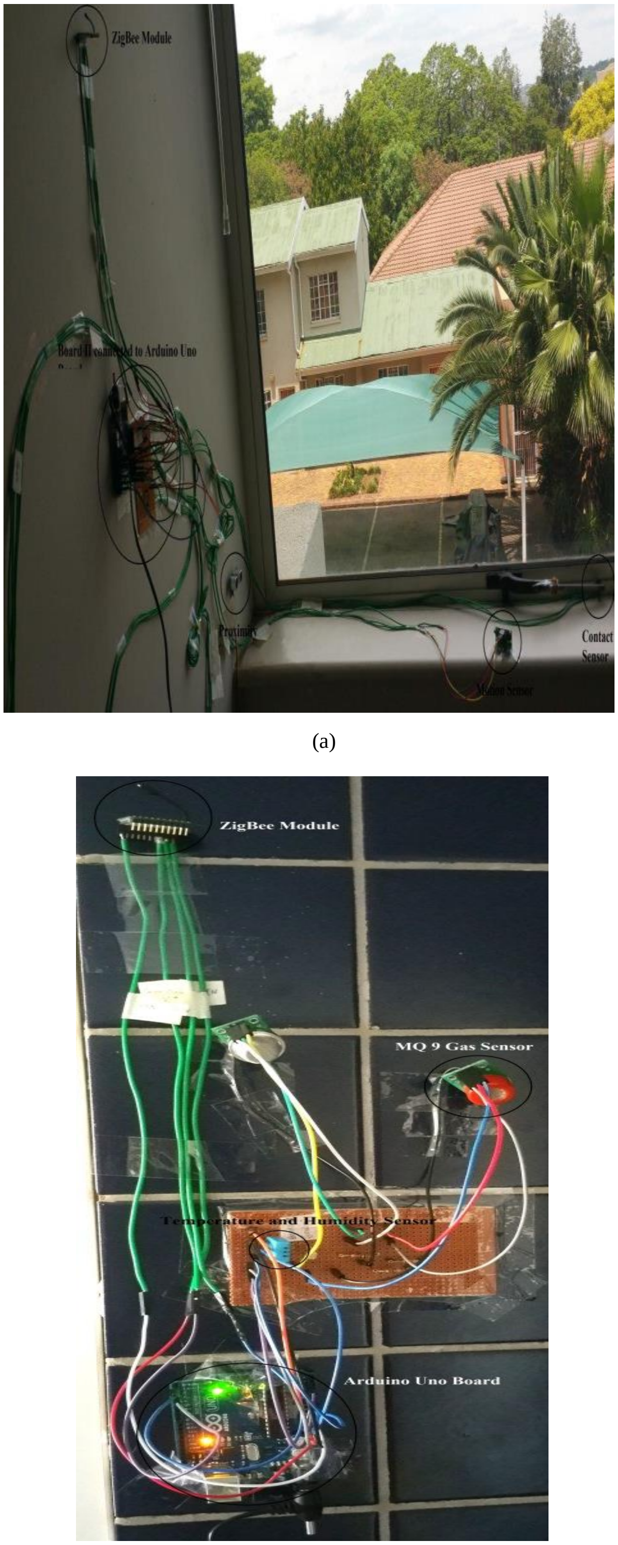


(a)

(b)

(c)

Fig. 7. (a) Shows Sensors, board and microcontroller deployment at Primary Access Point; (b) Board One installation at Primary Access Point; (c) Board Two installation at Secondary Access Points in the experiment setup.



(a)

(b)

Fig. 8. (a) Shows Sensors, board and microcontroller deployments at Secondary Access Point; (b) Board Three installation in the Kitchen; in the experiment setup.

Similar to board I and II board III relies on Arduino Uno module for power and ZigBee module for communication. Fig. 8 (b) board three installation in the kitchen. Board IV is deployed near the bed it is connected to two circular 0.5 inch diameter force sensing resistors. Both force sensors are deployed underneath the mattress. One in a region where the user places his shoulder and another close to the middle where the user's abdomen and pelvic region usually rests. Both force sensors has a full scale measurement accuracy of ±5%. Moreover, force sensors used in the experiment are readily available, cost effective, flexible and provides un-obstructive force measurements.

Board IV is connected to board II through wires, like board II it also draws power from the Arduino module connected to board II and uses the same ZigBee module to communicate values to the Pi. In short, the experiment setup consist of one Raspberry Pi 3 which acts as the central server connected to a ZigBee module to receive sensor data from various boards and a buzzer alarm to signal intrusion; four boards connected to various sensors to collect logical sensing parameters; three Arduino Uno boards with their own power supply connected to ZigBee communication modules to send sensor data to the Pi.

The power to each of the Arduino Uno boards is routed through a power bank. The power banks needs to provide a 9V–1000mA DC output to the Arduino boards. Any reliable power bank which has 5000mAh or higher capacity with 5V–1000mA USB power output would be enough to provide the power backup. The 5V output power from the power bank is boosted to 9V when connected to the Arduino board through a USB to 2.1mm DC 9V Booster Cable. The power bank is plugged into the apartment's 230V–50Hz AC power supply through a 5V–1000mA AC to DC adapter. Even when the power to the apartment is cutoff the Arduino Uno boards and the sensors are still active and will be able to identify intrusion attempts by drawing power from the power bank. Compared to AA or AAA batteries power banks offers reliable and durable power supply over time without replacement. Moreover, power banks are relatively cheap, readily available and can supply power to the Arduino boards and sensors for a week without recharging.

All the ZigBee communication is implemented using ZigBee Series 1 module. ZigBee module at the Pi is configured as the ZigBee Coordinator (ZC) while the modules attached to the microcontrollers is configured as the ZigBee End Device (ZED). The data rate of all the ZigBee modules are set at 9600 bits per second (bps).

All the ZigBee modules implemented uses 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. Each ZigBee module is programmed using a free XCTU software utility which allows communication with Digi RF modules.

MQ 9 sensor uses a supply voltage of 5V and a load resistance of 10 kΩ, it can measure carbon monoxide concentration from 200 ppm to 1000 ppm along with LPG and methane gases. MQ 9 sensor can work under temperatures from -20^{o}C to 50^{o}C, relative humidity of 95% and oxygen concentration ranging from 2% to 21%. As the concentration of carbon monoxide gas increases the measured voltage also goes up.

The ratio of air resistance Rs to Ro gives the concentration of measured gasses. Air resistance Rs, can be calculated using the equation:

$$\mathrm{s} = \frac{(\mathrm{Vcc} - \mathrm{V})}{\mathrm{V}}$$

Where Vcc is the supply voltage and V is the voltage measures across the sensor.

From the MQ 9 sensor data sheet it is clear that the ratio of Rs to Ro in clean air is 9.9, so the value of Ro is obtained from the Rs value calculated by putting the sensor in clean air, using the equation:

$$\mathrm{o} = \frac{Rs}{9.9}$$

The sensor was left in clean air for 24 hours to be stabilized before Ro value is calculated; the calculated Ro value is 2.05. The sensor board is then moved and installed to its working area. The calculated Ro value is used to calculate the Rs to Ro ratio during its operation.

The force sensor is connected to the board using a 10 kΩ resistance and uses a 5V supply voltage. Force sensor is made of Polymer Thick Film (PTF) which decrease in resistance when pressure is applied to the surface of the sensor. In the experiment, bed occupancy is determined by measuring the voltage across the resistance. Force Sensor Resistance (FSR) is calculated using the equation:

$$\mathrm{FSR} = \frac{(\mathrm{Vcc} - \mathrm{V}) *}{\mathrm{Vcc}}$$

Where Vcc is the supply voltage, V is the voltage measures across the sensor and R is the connected resistance. Using FSR, conductance and the applied force is calculated.

The motion sensor is deployed 2.5 ft. from the front door and proximity sensor at 3 ft. from the front door so they will only sense activities inside the home. The verification of the user is done using a laptop connected to the Pi using a wireless modem. The Pi is accessed from the laptop by means of Secure Shell (SSH) via a username and password. The user enters an eight character password to verify his identity. Once the alarm is triggered it can be killed using a 12 character password. The door observation time for the main access door is set as 15 seconds, identity verification timer is set as 90 seconds and the time for the user to get back into the home after stepping out leaving the main door open before changing home state (home state change timer) is set as 120 seconds.

V. Results and analysis

A. Results

During the one month period the main access point changed state 305 times. The algorithm was able to detect all these and reduce them to 190 state changes by identifying and eliminating the intermediate state changes mentioned in Table I. The most common state triggered was state 4 in Table I, it was triggered 46 times. While state 17 was triggered 33 times making it the second most popular. State 13 was triggered 20 times making it the third most triggered state. State 6 and state 1 were triggered 12 and 11 times respectively. State 31 happened 6 times, State 19 was triggered 13 times, States 9 and 16 were triggered five times; states 7, 14, and 15 were triggered four times; states 5, 11, 20, 22 and 26 were triggered thrice; states 2, 8 and 12 were triggered twice; states 3, 10, 18, 21, 27 and 32 were triggered only once during the one month time period. States 23, 24, 25, 28, 29 and 30 were not triggered during the one month time period.

The algorithm generated 14 warnings, 8 regarding the open primary access point, 3 for not securing the secondary access point before leaving the home and another 3 warnings for opening the balcony door during day when the bed was occupied. Intruder alarm was triggered 5 times during the experiment, 4 were related to primary access points while one was related to secondary access points. IVM was triggered 59 times and user successfully verified his identity 55 times. Alarm was killed using the 12 character password five times. The state change timer was activated 23 times while the user re-entered the home before the state change timer expired 15 times, so the home state changed due to state change timer expiry 8 times. The graph in Fig. 9 shows the number of state changes for primary access point, total number of warnings generated, IVM triggers, number of user identity verifications and number of alarms generated. Fig. 10 shows the number of state triggers for frequently triggered states namely State 1, 4, 6, 9, 13, 17, 19 and 31.

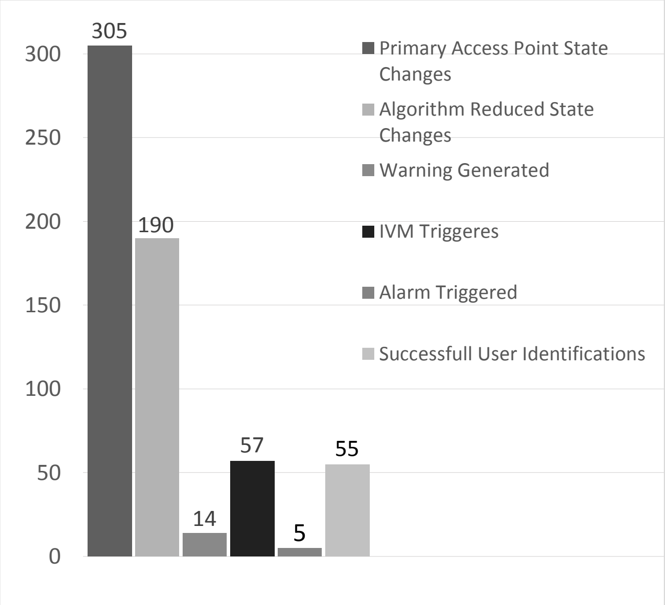


Fig. 9. Graph showing the number of state changes for primary access point, algorithm reduced state changes, total number of warnings generated, IVM triggers, number of user identity verifications and number of alarms generated.

Secondary access points changed states 56 times; balcony door changed state 27 times and window state was changed 29 times. All of the 27 times balcony door changed state the user was at home but 3 of them happened when the user was in bed, so these 3 times warnings were generated and IVM was activated along with the identity verification timer, which was reset when the user conformed their identity. Once the open balcony door was closed due to wind when the user was in bed, so no identity verification mechanism was initiated. The home was occupied all 29 times when the state of the balcony window was changed. Once the window was opened from the outside when the user was in bed during night; the intrusion defense mechanisms (audible alarm) were triggered without waiting for any user identity verifications. Fig. 11 shows the total number of state changes for secondary access points, balcony door and window state changes, secondary access point triggered IVM, warnings and alarms generated due to secondary access points.

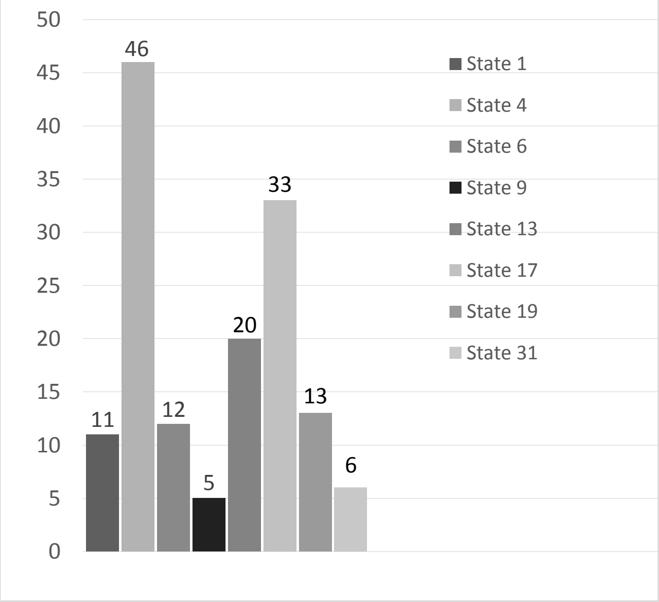


Fig. 10. Graph showing number of state triggers for State 1, State 4, State 6, State 9, State 13, State 17, State 19 and State 31 during the experiment.

MQ 9 sensor values are only considered after the sensor is allowed to be stabilized for 24 hours. Voltage measured when there is no carbon monoxide detected varied from 0.23V to 0.21V, calculated Rs value ranged from 20.73 to 22.27 and Rs to Ro ratio ranged from 10.11 to 10.86. Multiple matches are lit in an enclosed space near the sensor to determine sensor values during the presence of fire. Measured voltage when there is fire and carbon monoxide detected varied from 0.26V to 0.28V, calculated Rs value ranged from 16.85 to 18.24 and Rs to Ro ratio ranged from 8.22 to 8.9.

During fire the twelve second average value of temperature and humidity sensors were also noted. Before the fire the twelve second average temperature inside the apartment was 24^{o}C, the average temperature increased by 2.5^{o}C to 26.5^{o}C within 12 seconds and further increased to 30^{o}C within 36 seconds. 12 second average humidity in the apartment before fire was 32% it decreased by 3% to 29% within 12 seconds of the fire and after 36 seconds it further declined to 25.5%. Fig. 12 shows the measured voltage, Rs value, Rs to Ro ratio of the of MQ 9 sensor along with temperature and humidity sensor values under normal operational conditions and during fire.

When the bed was unoccupied, the force sensor at the bed top gave average readings between 0 and 2 Newton, the force sensor at the bed bottom gave average readings between 0 and

3 Newton. When objects like stack of books or some heavy boxes are placed on various areas of the bed, the average force at the shoulder region was between 1 and 3 Newton and average force at the abdominal region was between 2 and 4 Newton. When the user occupied the bed, the average force sensor values deployed at the shoulder region varied between 5 and 8 Newton, while force sensor values deployed at the abdominal region shifted between 7 and 10 Newton.

B. Discussing the Experiment Result

States 1 to 16 occurred when the home was occupied. The most common state triggered was state 4, which happened when the home was occupied and user opened a closed primary access point from the inside triggering the motion and proximity sensors and stepped out of the home and closed the door behind him. State 4 is usually triggered when the user leaves the home. After the door was closed the algorithm waited for 15 seconds for any intermediate state changes and since door remained closed, it changed the state of the home to empty. State 1 is triggered when the user opened the home from the inside triggering the motion and proximity sensors and came back into the home leaving the door open again triggering the sensors. State 7 happened when the user closed the open door from the inside and came back into the home, motion and proximity sensors are triggered before the initial state and after the final state.

State 8 occurred when the user walked from inside the home and closed an open door and stepped out, the motion and proximity sensors are triggered before the door is closed when the user walked towards the door; sensors are not triggered after the door is closed. After state 8 the algorithm waited until the door observation timer expired and changed the home state to empty. State 6 is triggered when the occupant came in from inside the home and opens a closed door and before the door observation timer expires closed it again and goes back into the home, making the open state of the door an intermediate state. Motion and proximity sensors are triggered before the door was opened and after it was closed. State 12 occurred when an open door is closed and opened by a user coming from inside the home and after opening the user went back inside. The motion and proximity sensors are triggered before the door is closed and after the door was opened.

State 11 happened when the user came from inside the home triggering the motion and proximity sensors and closed an open door and then opened it again before the door observation timer expired and stepped outside the home without triggering the sensors after the final state of the door. After state 11 the door is left open and the home is vacant, so the home state change timer is started which upon close to expiry warned the user about the impending home state change and when expired changed the home state to empty. State 13 occurred when the user comes in from the home and opens a closed door triggering the motion and proximity sensors and leaves the door open and exits the home. Similar to state 11, after state 13 is triggered the door is left open and the home is empty so the home state change timer is started which warns the user and changes home state to empty when expired. During the experiment State 11 and state 13 were triggered a combined 23 times. Whenever states 11 or 13 is triggered state change timer is started, so home state change timer was started 23 times.

State 9 occurred when the open door is closed from the outside and user stays outside, so motion and proximity sensors are not triggered before or after closing the door. When state 9 is triggered the running state change timer is not reset but it continues as the user did not re-enter the home, so when it expires home state is changed to empty. State 10 is triggered when an open door is closed and opened from the outside without triggering any motion or proximity sensors before closing the door or after opening the door. Similar to state 9, after triggering state 10 state change timer is not reset but it continues and upon expiry home state is changed to empty. Both states 9 and 10 are only triggered when previous states are either 3, 10, 11 or 13. State 3 happened when a closed door is opened from the outside without triggering the motion or proximity sensors before the initial state or after the final state. State 3 happened when the state change timer was running and the previous state was either 5 or 9. Since the user stayed outside the home in state 3, the state changer timer was not reset and allowed to continue.

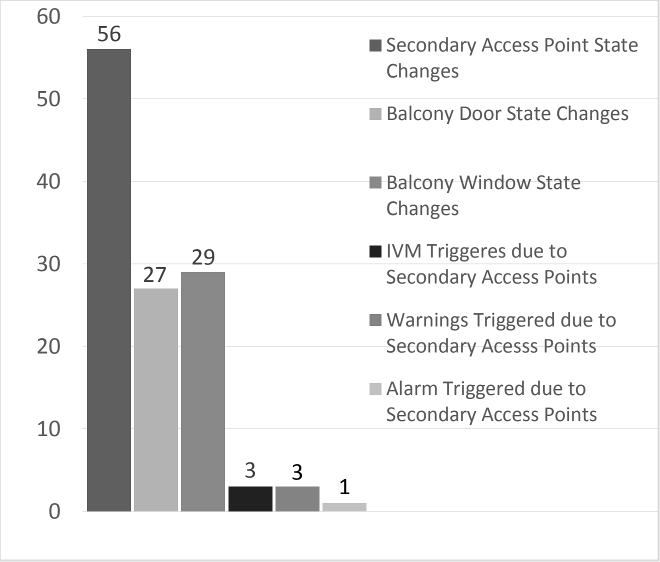


Fig. 11. Graph showing the number of state changes for secondary access points, balcony door state changes, balcony window state changes, IVM triggers due to secondary access points, warnings generated due to secondary access points and number of alarms generated due to secondary access points.

State 14 happened when an open door is closed and the user came back into the home from the outside. Motion and proximity sensors were not triggered before the door is closed but they were triggered as the user walked into the home after closing the door. After triggering state 14 as the user reentered the home state change timer was reset without changing the state of the home to empty. State 2 was triggered when the user opened a closed door and came back into the home. State 2 happened when the state change timer was still running and user re-enters the home (previous states are either 5 or 9), so the state change timer was reset without changing the home state.

State 15 was triggered when a closed door was opened and closed while the state change timer was still running and previous states were either 5 or 9. Motion and proximity sensors were not triggered before opening the door but as the user re-enters the home the sensors were triggered after the door was closed. Like in states 14 and 2 state change timer was reset without changing the home state. State 16 occurred when the open door was closed and then opened with the home state change timer still running. As user entered the home from the outside, motion and proximity sensors were not triggered before closing the door but they were triggered when the user came in after opening the door. Like in states 14, 2 and 15 the state change timer was reset without changing the home state. Whenever states 14, 2, 15 or 16 were triggered state changer timer was reset without changing the home state to empty. During the experiment, states 14, 2, 15 and 16 occurred a total of 15 times. So state change timer was reset 15 times. Home state changed from occupied to empty due to expiration of the state change timer 8 times, this accounted for 8 of the 14 warnings generated by the algorithm. When user re-entered the home these 8 times IVM was activated and he was asked to confirm his identity. Twice the user forgot to confirm his identity upon re-entry, which accounted for 2 of the 5 intrusion alarms raised.

States 17 to 32 are triggered when the home is empty and the main access point state is changed. State 17 was triggered when the home is empty and someone opens the main door from the outside and enters the home after closing the door behind them triggering the motion and proximity sensors. When state 17 occurred someone entered the empty home, so IVM was triggered. If user verification is not done within identity verification time period (90 seconds) or if verification fails alarm is triggered. If the algorithm confirms user identity, then the state of the home is changed from ‘empty’ to ‘occupied’.

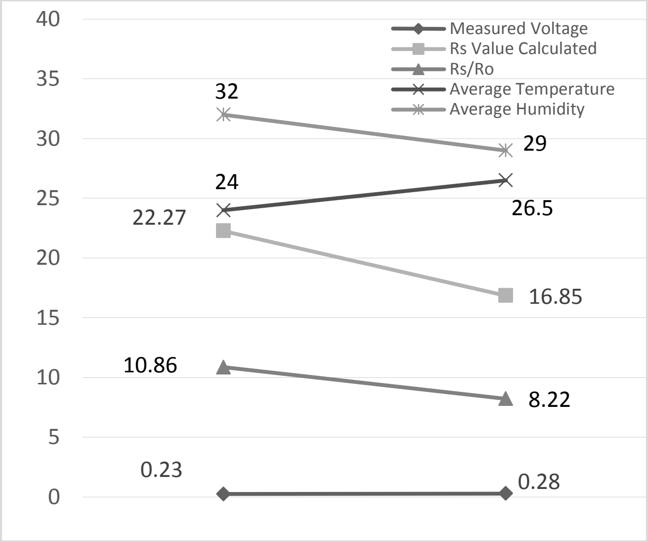


Fig. 12. Graph showing Measured Voltage, Rs Value, Rs to Ro Ratio of the of MQ 9 sensor along with temperature and humidity values under normal operational conditions and during fire.

State 19 occurred when a closed door was opened from the outside and the user left the door open and came into the home triggering the motion and proximity sensors. User identity has to be verified as the user entered an empty home, so IVM was activated. States 17 and 19 were triggered 46 times, which accounted for 46 of the 57 IVM activations. Out of all the 46 IVM activations after states 17 and 19, the user identity was successfully verified 46 times without triggering any alarm. State 22 happened when the closed main door was opened and closed from the outside without the user entering the home. Motion and proximity sensors were not triggered before opening the door or after closing the door. IVM was not activated because no one entered the home, door remains closed so algorithm waited for another state change of the door. After triggering state 22, states 17, 19, 20, 22 could be triggered.

State 26 is triggered when the open main door is closed from outside without triggering the motion and proximity sensors before or after closing the door. After state 26 was triggered, no one entered the home, so no user identification was necessary. State 27 was triggered when the open main access point was closed then opened from the outside without triggering the motion and proximity sensors before closing the door or after opening the door. After state 27 was triggered the primary access point remained open, so the algorithm kept observing the motion and proximity sensors until another state change was triggered to determine user entry into home. States 26 and 27 were only triggered when the previous states were either 11, 13, 27 or 20.

State 20 was triggered when a closed door was opened from the outside and left open. Motion and proximity sensors were not triggered before or after opening the door, so nobody entered the home when state 20 was triggered hence IVM was not activated. Like in case 27, after triggering state 20 the algorithm kept observing the motion and proximity sensors until another state change was triggered to determine user entry into home. State 20 was triggered thrice during the experiment; out of the 3 times once user re-entered the home without changing the door state triggering special case 34 in Table II. The algorithm identified this action by motion and proximity sensor triggers, so IVM was immediately activated and user identity was confirmed. Twice state 31 was triggered after state 20 when user closed the door and entered the empty home.

State 31 was triggered when the user closed an open door and entered an empty home triggering the motion and proximity sensors after closing the door. Identity of the user was verified as the user entered an empty home. State 32 occurred when an open main door was closed and opened by the user as he entered the home. Motion and proximity sensors were triggered after the door was opened as the user walked into the empty home, so user identity was verified. State 31 and 32 occurred 7 times which accounted for seven of the IVM activations.

Each of the states 21 and 18 were triggered once. When these states were triggered motion and proximity sensors were triggered before the door was opened. This will not happen in an empty home. So intrusion alarm was activated without waiting for user identity confirmation. This accounted for 2 of the 5 intrusion alarms generated. Thrice balcony door was opened when the user was in bed during day time, this happened due to the presence of a second person in the apartment; 3 of the IVM and warnings were triggered as a result of this. User confirmed his identity before user verification timer was expired. Once after state 13 and after expiration of the state change timer (home state changed to empty) when user re-entered the home by triggering state 31 he forgot to confirm his identity so the intrusion alarm was activated after identity verification timer was expired. Similarly, once after state 13 and expiration of the state change timer user re-entered the home triggering state 27 and forgot to confirm his identity so intrusion alarm was triggered. Once the balcony window was opened from the outside without triggering the motion or proximity sensors deployed inside the home near the window during night when the user was in bed. A window will never be opened from the outside when the user is in bed, so without waiting for identity confirmation the intrusion alarm was triggered.

The measured voltage across the MQ 9 sensor went up when there was fire, the Rs to Ro ratio varied from 10.86 when there was no fire to 8.22 when there was fire. 12 second average temperature showed a spike of 2.5^{o}C and average humidity showed a 3% decline within 12 seconds when there was fire. When the bed was unoccupied the force sensors gave a reading because they are triggered by the weight of the bed mattress, as they are placed underneath the mattress. When objects like stack of books and heavy boxes are placed on various parts of the bed the sensor values increased due to their weight but value of bed top and bottom sensor did not increase simultaneously as the placed objects did not have the weight distribution to trigger both sensors. When objects are placed close to the top of the bed, force sensor values at the shoulder region increases but force value at the abdominal region of the bed remained constant with minimal variation. Similarly, when objects are placed close to the bottom of the bed force sensor values at the abdominal region varies while force detected at the shoulder region of the bed remained constant.

C. *Features and Comparison*

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 laser grids. It offers implementation ease and flexibility compared to the security system proposed by B. Schilit et al. [12]. 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.

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 an eavesdropping attacker will not be able to gain access to the system and manipulate it. O. Yurur et al. [16] utilized context aware computing to improve home security, user context is identified by saving, analyzing and sharing data regarding user behavior and context which raised security and privacy concerns. In the proposed work, access point data is stored in a data base on Raspberry Pi which is kept inside the home and secured using physical locks with access limited to authorized personals. Moreover, the stored data is never shared and it can be encrypted to further improve security.

Morsalin et al. [33] utilized NFC tags to predict user location in a home and the user had to verify his fingerprint and enter the password each time when the user wants to access their home. The security algorithm proposed in the paper, did not utilize NFC communication tags which reduces the complexity of the system and improves user convenience. Moreover, the IVM is only triggered when someone enters an empty home. The algorithm was also able to identify secondary access point actions initiated by the user and was able to distinguish them from intruder actions.

VI. 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 experiment, our proposed algorithm was able to successfully identify all 305 state changes of the main access point and reduce them to 190 user behaviors while the secondary access point changed state 56 times. The alarm was triggered five times when the user failed to confirm his identity. Six of the fourteen warnings generated were regarding secondary access points while the other eight were relating to primary access point when the home became empty. 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, we plan to improve user behavior prediction by analyzing various user actions inside the home to further improve smart home security.

Acknowledgment

I would like to thank Ms. Minna Roselin Cherian for proof reading the paper.

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] Wenye Wang, Zhuo Lu, “Cyber security in the Smart Grid: Survey and challenges,” *Computer Networks*, Volume 57, Issue 5, Pages 1344-1371, April 2013.

[4] 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. 1933-1954, Fourthquarter 2014.

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

[6] 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.

[7] Y. Mo and B. Sinopoli, "Secure control against replay attacks," *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, pp. 911-918, 2009.

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

[9] UNODC, “International Burglary, Car Theft and Housebreaking Statistics,” *United Nations Office on Drugs and Crime (UNODC)*, Technical Report, 2015.

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

[11] A.C Jose, R. Malekian, "Smart Home Automation Security: A Literature Review", *Smart Computing Review*, Vol. 5, No. 4, pp. 269-285, August 31, 2015.

[12] 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.

[13] 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.

[14] British Broadcasting Corporation (BBC) - Andrew Silke, "Webcams taken over by hackers, charity warns", [Online]. Available: http://www.bbc.com/news/uk-22967622

[15] V. Bellotti, K. Edwards, "Intelligibility and Accountability: Human Considerations in Context Aware Systems," *Human-Computer Interaction*, vol. 16, issue 2, pp. 193-212, Dec. 2001.

[16] 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.

[17] S. Saponara and T. Bacchillone, "Network architecture, security issues, and hardware implementation of a home area network for smart grid," *Journal of Computer Networks and Communication*, vol. 2012, pp. 534512-1–534512-19, 2012.

[18] A. Alheraish, "Design and Implementation of Home Automation System", *IEEE Transactions on Consumer Electronics*, vol. 50, no. 4, pp.1087-1092, Nov. 2004.

[19] 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.

[20] A. De Santis, A. G. Gaggia, U. Vaccaro, "Bounds on entropy in a guessing game", *IEEE Transactions on Information Theory*, Vol. 47, Issue. 1, pp. 468 - 473, Jan 2001.

[21] D.C. Feldmeier, P.R. Karn, "UNIX Password Security - Ten Years Later", *Lecture Notes in Computer Science*, Vol. 435, pp 44-63, 1990.

[22] E.I Tatli, "Cracking More Password Hashes With Patterns", *IEEE Transactions on Information Forensics and Security*, Vol. 10, Issue. 8, pp. 1656 - 1665, April 2015.

[23] 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.

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

[25] M.R Faghani, U.T Nguyen, "A Study of XSS Worm Propagation and Detection Mechanisms in Online Social Networks", *IEEE Transactions on Information Forensics and Security*, Vol. 8 (11). pp. 1815 - 1826, 2013.

[26] K. Atukorala, D. Wijekoon, M. Tharugasini, I. Perera, C. Silva, "SmartEye - Integrated solution to home automation, security and monitoring through mobile phones," *Third International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST '09*, pp. 64-69, Sep. 2009.

[27] S.-M. Tsai, P.-C. Yang , S.-S. Wu , S.-S. Sun, "A Service of Home Security System on Intelligent Network," *IEEE Transactions on Consumer Electronics*, vol. 44, no. 4, pp. 1360-1366, Nov. 1998.

[28] 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.

[29] S. Lee, K. N. Ha, and K. C. Lee, "A pyroelectric infrared sensor-based indoor location-aware system for the smart home," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 4, pp. 1311–1317, Nov. 2006.

[30] H. H. Kim, K. N. Ha, S. Lee and K. C. Lee, "Resident Location-Recognition Algorithm Using a Bayesian Classifier in the PIR Sensor-Based Indoor Location-Aware System," in *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 39, no. 2, pp. 240-245, March 2009.

[31] P. Kumar and P. Kumar, "Arduino based wireless intrusion detection using IR sensor and GSM," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 5, pp. 417–424, 2013.

[32] 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.

[33] 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.

[34] P. H. Huang, J. Y. Su, Z. M. Lu, J. S. Pan, "A fire-alarming method based on video processing," *Intelligent Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 359-364, Dec. 2006.

[35] M. O. Oloyede and G. P. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review," in IEEE Access, vol. 4, no. , pp. 7532-7555, 2016.

[36] M. Ryan, "Bluetooth: With Low Energy comes Low Security," *WOOT'13 Proceedings of the 7th USENIX conference on Offensive Technologies*, pp. 4-4, 2013.

[37] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi and W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," *IEEE Systems Journal*, vol. 8, no. 2, pp. 509-520, June 2014.

[38] A. P. Melaragno, D. Bandara, D. Wijesekera and J. B. Michael, "Securing the ZigBee Protocol in the Smart Grid," in *Computer*, vol. 45, no. 4, pp. 92-94, April 2012.

[39] B. Al Baalbaki, J. Pacheco, C. Tunc, S. Hariri and Y. Al-Nashif, "Anomaly Behavior Analysis System for ZigBee in smart buildings," *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, Marrakech, 2015, pp. 1-4.

[40] Zhongqin Wang, Ning Ye, Ruchuan Wang, Peng Li,"TMicroscope: Behavior Perception Based on the Slightest RFID Tag Motion", Elektronika ir Elektrotechnika (Impact factor: 0.561), Vol.22, No.2, pp.114-122, 2016.

[41] Zhongqin Wang, Ning Ye, Fu Xiao, Ruchuan Wang, "TrackT: Accurate Tracking of RFID Tags with mm-level Accuracy Using first-order Taylor series approximation", AD Hoc Networks, Elsevier, Vol.53, pp.132-144, 2016.

[42] Tianhe Gong, Haiping Huang, Ping Chen, Tao Chen, "Secure Two-party Distance Computation Protocol Based on Privacy Homomorphism and Scalar Product in Wireless Sensor Networks", Tsinghua Science and Technology (IEEE), Vol.21, No.4, pp. 385-396, 2016.

[43] Xiangjun Jin, Jie Shao, Xin Zhang, Wenwei An, "Modeling of nonlinear system based on deep learning framework", Nonlinear Dynamics, Springer, Vol.84, No. 3, pp.1327-1340, 2016

[44] R. Malekian, Abdul Hanan Abdullah, "Traffic Engineering Based on Effective Envelope Algorithm on Novel Resource Reservation Method over Mobile Internet Protocol Version 6", International Journal of Innovative Computing, Information and Control, Vol.8, No.9, 2012