International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Simulating Internet of Surveillance Using Packet Tracer

T. P. Deepa
Department of Computer Science and Engineering, School of Engineering and Technology, Jain University, Karnataka, India

ABSTRACT

In the current scenario, it is necessary to ensure safety and security due to influence of modern technology. Especially places like Airport, schools, colleges, Home etc where security is high priority, needs an intelligent system which detect intrusion and objectionable objects with less human intervention. Hence, camera helps to capture passenger from remote view and sensors can be used to sense objectionable objects. Though body scanners and detectors are available but passenger has to undergo multiple steps of security checks which is time consuming. Hence, there is a need for an integrated device which can perform various security check at the same time and ensures to wired or wireless network enables faster data transmission through wired or wireless network. This kind of systems can also help security agent to monitor and control the security remotely resulting in human error free system. Also, when such system is integrated with smart phone can result in fast notification and alert system. This paper simulates smart surveillance system using Internet of Things (IoT) with smart phone based alert system.

Keywords: Surveillance, Internet of Things, Wireline, Wireless

I. INTRODUCTION

Internet of things is a system of interrelated computing devices and plays a major role in monitoring of location, activities, person. When this monitoring, managing and detection of objectionable behaviour or objects are done through electronic components from a remote then it is called as Remote Surveillance system [1]. Even though, CCTV camera is mostly commonly used for surveillance, it is found to be costly, reserves too much of space in storing recordings and most importantly need human intervention to detect unauthorized activity [2]. Also, it becomes tedious when one has to undergo multiple types of security checks not just relying on CCTV footages for surveillance. The full body scanners used in Railway station, Airport has adverse health and privacy issues though they can detect objectionable objects when hidden behind clothes, in a bag or any other objects [3]. Also, some security system needs to undergo check for multiple stages like metal detection, body scanning, motion detection, camera surveillance etc which is frustrating to the person undergoing security checks and time consuming too. So, there is a need for fast integrated system or device which can perform all the types of security check at once. This system should create a suitable alert immediately even when single type of security check is not passed and should send notifications to concerned security agent even when he or she is not present at the security check site. That is, there is a need for remote surveillance system with less human intervention. This can ensure privacy issues which are complained more often at places like airports [3]. This kind of integrated system can be built by connecting different physical devices such as camera, motion detector, explosive detector, poisonous gas detector, metal detector and other smart devices like

smart phones etc. There is a need for common, interoperable environment which can connect and communicated between these devices for promised efficiency and accuracy. It will even more efficient when the range of coverage of these devices are more. It is possible to build using Internet of Things (IoT) which incorporates communication abilities to everyday things or objects through internet [2]. It is also advisable in this heterogenous environment to use IoT based applications to remotely control and notify activities when security breach is detected. This paper concentrates on simulating IoT based remote smart surveillance system which integrates different sensors and smart phone.

II. LITERATURE SURVEY

C M Srilakshmi et al proposed a IoT based Surveillance system which detects motion, capture image and sends GCM notification through Raspberry Pi. User could access image from remote place through internet. User could access location information of the object being checked. Authors in this paper concentrated on one type of security check that is remote camera-based surveillance [1].

In [4], authors developed an IoT based application which monitor human movement using PIR sensor and created notification on smart phone. Also, videos captured from camera was uploaded to cloud server for further monitoring and analysis by authorised person. The camera could be rotated 2700 remotely. The authors implemented this system mainly using Raspberry pi, solar and AC power supply, cloud server. They also included prevention system like automatic door lock and releasing fainting gases. This system involves human intervention to analyse captured images and considering only camera-based surveillance. Using fainting gas system as preventive device can be dangerous in case of false positivity.

Ravi Kishore Kodali et al in [5] proposed IoT based system which used PIR motion sensor at the entrance of the building. When intrusion is detected, it triggers voice call to the owner of the building, switching on lights and alarm in the building. Also, owner could send a message to police authority using simple SMS. This system used only motion sensors to detect intrusion.

III. METHODOLOGY

This method integrates different types of sensors like camera, motion detector, carbon-di-oxide detector, carbon monoxide detector, metal detector via IOT registration server /home gateway to smart phone and alert systems. The proposed method used CISCO Packet tracer (PT) to simulate Internet of surveillance system for better understanding and analysis of new integrated environment. The simulated environment includes a backbone network was used as network interface to connect required smart things and sensors. Smart things are the physical objects that was connected to registration server or Home gateway through network interface which can be wired or wireless. This work concentrated on both wired and wireless simulated environment for performance analysis.

The following are the components of CISCO packet tracer used in Wired simulation Environment-

For Backbone Network-

1. DLC100 Home gateway – This is IoT registration server configured with Internet of Everything (IoE) services. The smart things can directly register to it for accessing IoE services. This gateway provides both ethernet ports (wired) and wireless access point with secured WEP / WPA-PSK / WPA2 enterprise. This gateway is connected to the Internet through Internet WAN ethernet port. This gateway host web interface through which all smart things connected to it can be remotely managed. This device is configured with ip address 192.168.25.1 and SSID=HomeGateway which will be used as IoT gateway address in smart things as shown in figure 1a. This is connected to IoT homepage http://index.html.

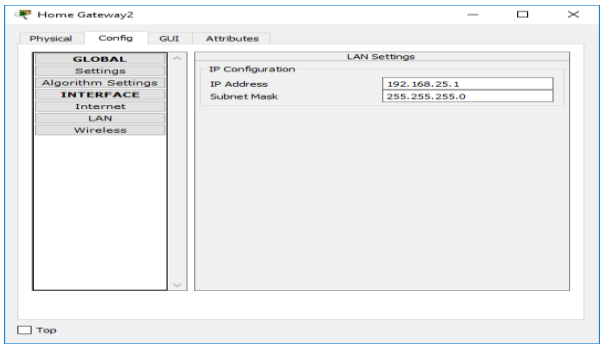

Figure 1a. IP address configuration of Home Gateway or IoT registration server.

2. Smart Phone - This is to simulate smart device at user end to receive notifications and also program logic to control and manage different smart things is placed in this device. This device is ip configured and connected to home gateway using SSID as shown in figure 1b.

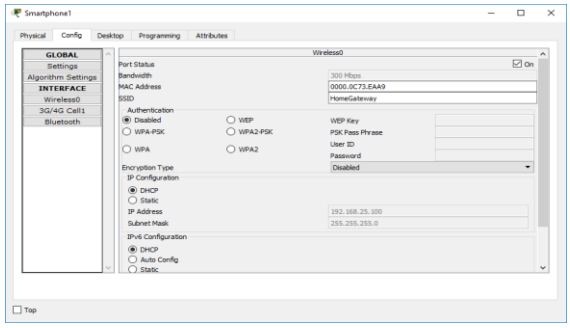

Figure 1b. Smart is connected to IoT registration server via Home Gateway SSID.

3. 2960 Switch- This is CISCO catalyst 2960 series switch which connects to home gateway via Fast ethernet ports. The configuration is as shown in figure 1c.

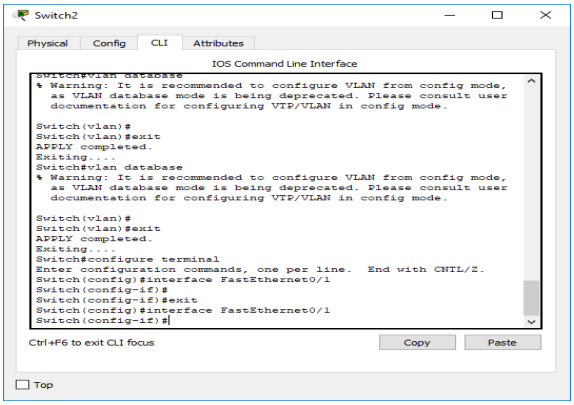

Figure 1c. Switch configuration with Fast ethernet ports to connect smart things to home gateway

Smart Things used in this work along with their specifications are as follows-

4. Siren – Alarm System

   Remote Control:

   Connect the device to Registration Server using Config Tab

   Data Specifications:

   Input Slot: D0

   Message Format: [state]

   state: 0 = closed, 1 = open

Three sirens were used in this work, Explosive detection, Motion detection and Metal detection sirens. This siren was connected to home gateway as shown in figure 2a so that it can be accessed through smart phone.

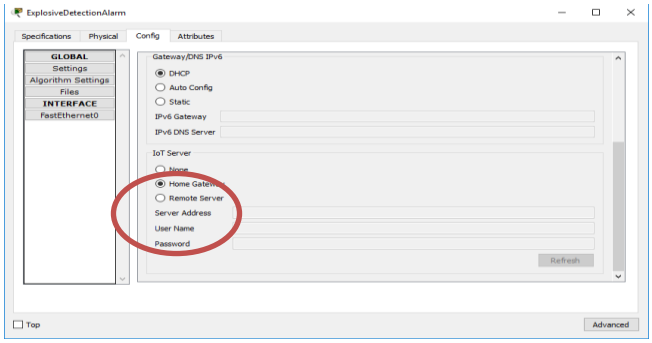

Figure 2a. Connect smart siren to IoT registration server using SSID of Home Gateway.

5. Motion Detector - Detects motion from mouse movement.

   Features:

   Registration Server Compatible

   Automatically deactivates after 5 seconds without any mouse movement.

   Data Specifications:

   Message Format: [state]

   state: HIGH=activated, LOW=inactive

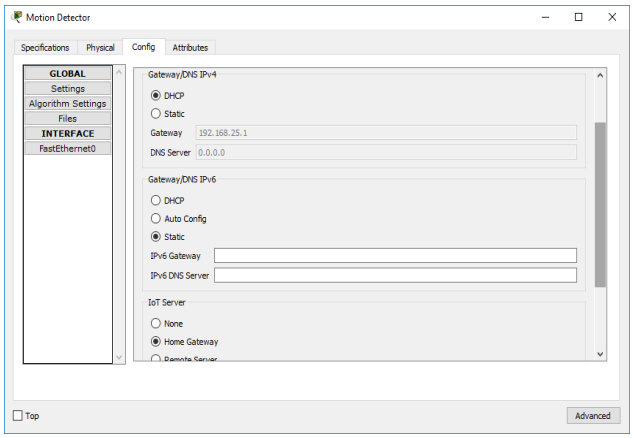

Figure 2b. Ip configuration and connecting Motion Detector to IoT registration server using SSID of Home Gateway

6. Webcam - A camera device that records and sends data

   Features:

   Registration Server Compatible

   Off, On, Video recording

   Data Specifications:

   Message Format: [state]

   state: 0 = off, 1 = on

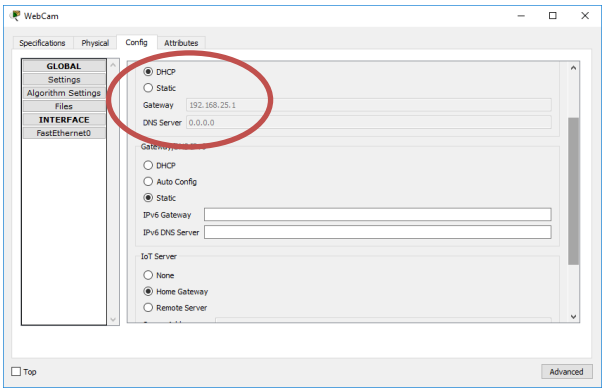

Figure 2c. Ip configuration and connecting Webcam to IoT registration server using SSID of Home Gateway

Old Car – A car having lots of problems. In this work it is used as a source of poisonous gases closely simulating source of explosives.

7. Carbon Monoxide Detector and Carbon Dioxide Detector - Detects the level of the carbon monoxide and carbon dioxide.

   Features:

   Registration Server Compatible

   Alarm will go off when it detects a Carbon Monoxide level of 20%. Integrated with old car for carbon monoxide source.

   Data Specifications:

   Message Format: [state], [level]

   state: 0 = alarm off, 1 = alarm on

   level: a positive number

8. Metal Sensor- Detects metal by checking for an alloy property and outputs the reading.

Usage: Objects near the sensor area with the alloy property will be detected. The detector sends and analog signal based on the alloy content.

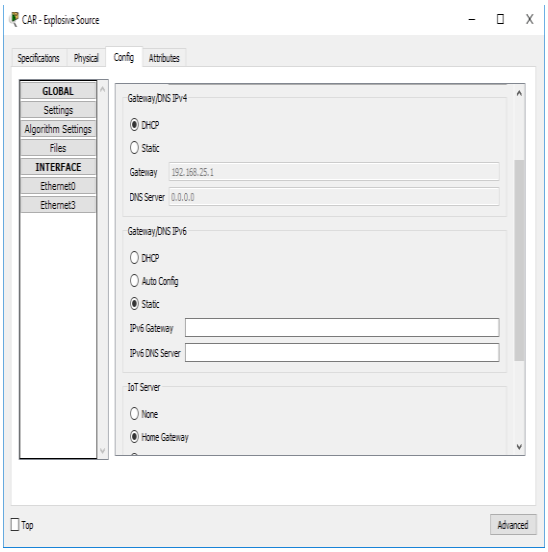

Figure 2d. Ip configuration and connecting Car which is used as source of explosives and poisonous gas to IoT registration server using SSID of Home Gateway

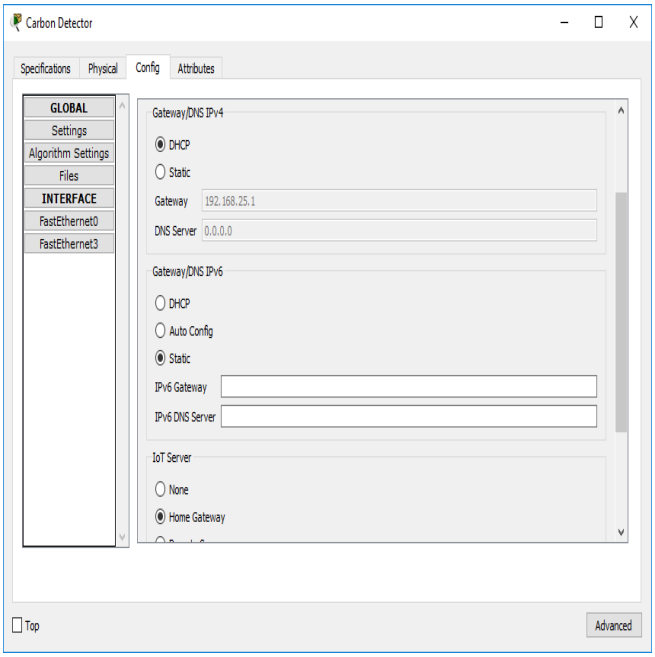

Figure 2e. Ip configuration and connecting Carbon monoxide and dioxide detection which was used to simulate explosive detector to IoT registration server using SSID of Home Gateway

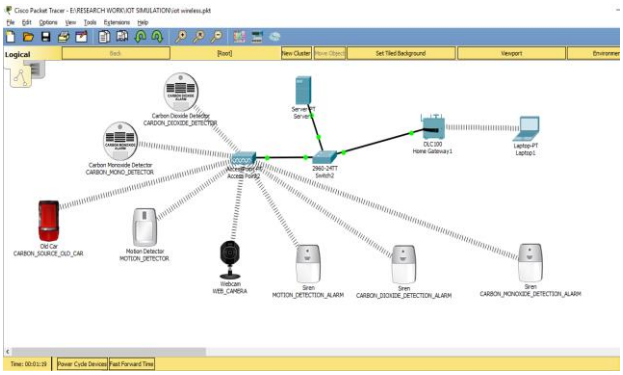

Figure 3. Internet of Surveillance in Wireline environment

The figure 3 shows simulation of internet of surveillance in wireline environment. The table 1 lists the components of CISCO packet tracer used in Wireless Simulation Environment-

TABLE 1. DESCRIPTION OF DEVICES USED FOR SIMULATION

Devices	Description
Explosive source	Analog, 5 watts, 10Mbps, Full duplex
Camera	Digital, 5 watts, 10Mbps, Full duplex
Motion detector	Digital, 5 watts, 10Mbps, Full duplex
Carbon monoxide detector	Digital, 5 watts, 10Mbps, Full duplex
Carbon dioxide detector	Digital, 5 watts,10Mbps, Full duplex
Metal Sensor	Digital, 5 watts, 10Mbps, Full duplex
MCU	Analog, 5 watts, 300Mbps
Metal sensor Alarm	Digital, 5 watts, 10Mbps, Full duplex
Access point	Switching Device, 20 watts, full duplex
Switch	Switching Device, 5 watts, 10Mbps, full duplex
Laptop	End device, 60 watts, full duplex
Smart Phone	End device, 15 watts, 300Mbps, full duplex
Home Gateway/ IoT Registration Server	IoT service provider, 20 watts, 2.4 Ghz Channel, full duplex, wireless coverage - 250meters
DHCP Server	Analog 200 watts

For Backbone Network-

1. DLC100 Home gateway – This is similar to that used in wired simulation environment except for wireless interface.
2. Smart Phone/Laptop- This is to simulate smart device at user end to receive notifications and also program logic to control and manage different smart things is placed in this device.

3. 2960-24TT Switch- This is CISCO catalyst 2960 series switch which connects wireless access point to home gateway and DHCP server.
4. DHCP server
5. Wireless access point

Things used in wireless environment are same as that of wired environment but they were used in wireless mode. The figure 4 shows simulation of internet of surveillance in wireless environment.

IV. RESULTS AND DISCUSSION

This section analyses performance of Internet of Surveillance simulation in wireless and wireline environment.

This simulation environment used Wireless infrastructure-based LAN with star topology. Different sensors mentioned in table1 were connected using wireless technology and intermittent connectivity to IOT registration server was wireless infrastructure. The table 2 list the type of connection used between different devices. It uses two types of connection – 1. Device-to-Device connection (D2D) 2. Server-to-server connection (S2S).

TABLE 2: CONNECTION TYPE BETWEEN DIFFERENT SENSORS AND DEVICES IN WIRELESS ENVIRONMENT

Connection type	Source Device	Destination Device
D2D	Explosive source	Carbon monoxide and dioxide detector
D2S	Camera	Motion detector
D2S	Motion detector	Motion detection alarm
D2S	Carbon monoxide detector	Carbon monoxide detection alarm
D2S	Carbon dioxide detector	Carbon dioxide detection alarm
D2S	Metal Sensor	Metal detection alarm
D2D	Metal sensor	MCU
S2S	Access point	Switch
S2S	Switch	Home gateway / IoT registration server
D2S	Smart phone	Home gateway / IoT registration server

TABLE 3: DIFFERENT PERFORMANCE PARAMETERS EVALUATED IN WIRELESS ENVIRONMENT.

Start device	End device	Intermediate devices	Type of connectivity	Transfer time	Packet type	Simulation Time (sec)
Motion Detector	Camera	switch	Wireline	0.007	ICMP	2.001
Motion Detector	Motion Detector alarm	Access point	Wireline	0.025	ICMP	2.689
Carbon dioxide source	Carbon dioxide detector alarm	Carbon dioxide detector, access point, smart phone	wireline	0.025	ICMP	2.689
Carbon monoxide source	Carbon monoxide detector alarm	Carbon monoxide detector, access point, smart phone	wireline	0.025	ICMP	2.689
Access point	Switch	Direct	Wireline, Point-to-point	0.028	STP	2.689
Home gateway	Switch	Direct	Wireline, Point-to-point	0.785	STP	2.689

TABLE 4: DIFFERENT PERFORMANCE PARAMETERS EVALUATED IN WIRELINE ENVIRONMENT

Start device	End device	Intermediate devices	Type of connectivity	Transfer Time (sec)	Packet type	Simulation Time (sec)
Motion Detector	Camera	access point	Wireless	0.025	ICMP	0.788
Motion Detector	Motion Detector alarm	Access point	Wireless	0.025	ICMP	2.689
Carbon dioxide source	Carbon dioxide detector alarm	Carbon dioxide detector, access point, smart phone	Wireless + wireline	0.025	ICMP	2.689
Carbon monoxide source	Carbon monoxide detector alarm	Carbon monoxide detector, access point, smart phone	Wireless + wireline	0.025	ICMP	2.689
Access point	Switch	Direct	Wireline, Point-to-point	0.028	STP	2.689
Home gateway	Switch	Direct	Wireline, Point-to-point	0.785	STP	2.689

Performance of Internet of surveillance in Wireline simulation environment

This simulation environment used Wireline infrastructure-based LAN with star topology. The devices and sensors used in wireless environment were as shown in table1. Different sensors mentioned in table1 were connected and intermittent connectivity using wireline technology.

Table 2 and 4 shows different performance parameters in Internet of surveillance system in wireless and wireline simulation environment, it is clear that the transfer time between different sensors is almost same in both the environment. But guarantee of service was good in wireline environment compared to wireless.

V. CONCLUSION

This paper proposed an internet of surveillance system which connects different security devices and sensors. Authors used CISCO packet tracer simulation environment to analyse the performance of proposed system in wireless and wireline environment. Other authors and researchers worked on surveillance system for home using CCTV. This paper concentrates of addition of different sensors like motion detection sensors, explosive detection sensors making it more suitable for real time and environment where security is the priority for example airport. During simulation it was found that the transfer time between devices did not exhibit much different in both wireline and wireless environment. But guarantee of service and reliability was ensured in wireline environment compared to wireless. As a future work, this method can be implemented using actual sensors and devices in physical environment using Cloud based IOT interface kits by evaluating more performance parameters.

VI. REFERENCES

[1] C M Srilakshmi, Dr M C Padma, IOT Based Smart Surveillance System, International Research Journal of Engineering and Technology (IRJET), Volume 4, Issue: 5, May -2017.

[2] Priya B. Patel, Viraj M. Choksi, Swapna Jadhav, M.B. Potdar, Smart Motion Detection System using Raspberry Pi, International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868, Foundation of Computer Science

FCS, New York, USA Volume 10 – No.5, February 2016.

[3] Julie Accardo, M. Ahmad Chaudhry, Radiation exposure and privacy concerns surrounding full-body scanners in airports, Journal of Radiation Research and Applied Sciences 7 (2014) 198-200.

[4] Haribaabu. V* and Joseph James. S, Intelligent Surveillance System using Internet of Things, I J C T A, 9(37) 2016, pp. 313-317 © International Science Press

[5] Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana, IoT Based Smart Security and Home Automation System, International Conference on Computing, Communication and Automation (ICCCA2016), ISBN: 978-1-5090-1666-2/16/$31.00 ©2016 IEEE, page 1285-1289