**KING’S OWN INSTITUTE\***

**Success in Higher Education**

# GROUP ASSIGNMENT COVERSHEET

Subject Code & Name: Lecturer’s/Tutor’s name:

ICT743 IoT Security

Dr. Prabhu Jyot Singh

Assignment Title:

Group Project: IoT Application for Controlling Home Appliances

**Declaration**

(This declaration must be completed by all students in the group or the assignment will not be marked.)

We, the undersigned, certify the following:

* We have read and understood the *Student Academic Misconduct Policy*
* This assignment is our own work based on our personal study and or research.
* We have acknowledged all material and sources used in the preparation of this assignment including any material generated in the course of our employment.
* **The assignment has not previously been submitted for assessment in this or any other unit.**
* We have not copied in part or in whole or otherwise plagiarised the work of other students.
* We have read and understand the criteria used for assessment.
* The assignment is within the word and page limits specified in the unit outline.
* The use of any material in this assignment does not infringe the intellectual property / copyright of a third party.
* We understand that this assignment may undergo electronic detection for plagiarism, and an anonymous copy of the assignment may be retained on the database and used to make comparisons with other assignments in future.
* By completing this coversheet in full and submitting this assignment electronically, we are bound by the conditions of the KOI's *Student Academic Misconduct Policy* and the declaration on this coversheet.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Family Name | Given Name(s) | Student ID | Tutorial Code | Contribution Percentage | Signature |
| Student 1 | Austria | John Benny | 12301175 | LB | 25% | J\_AUST |
| Student 2 | Catris | Rhayzon Jarielle | 12300512 | LB | 25% | R\_CATRIS |
| Student 3 | Cator | Beberly | 12203761 | LB | 25% | B\_CATOR |
| Student 4 | Paulino | Lovely | 12301035 | LB | 25% | L\_PAULINO |

**Assignment Receipt**

Subject Code & Name: ICT743 IoT Security

Lecturer’s/Tutor’s Name: Dr. Prabhu Jyot Singh

Assignment Title:

Group Project: IoT Application for Controlling Home Appliances

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Family Name | Given Name(s) | Student ID | Tutorial/ Code | Signature |
| Student 1 | Austria | John Benny | 12301175 | LB | J\_AUST |
| Student 2 | Catris | Rhayzon Jarielle | 12300512 | LB | R\_CATRIS |
| Student 3 | Cator | Beberly | 12203761 | LB | B\_CATOR |
| Student 4 | Paulino | Lovely | 12301035 | LB | L\_PAULINO |

GROUP ASSIGNMENT COVER SHEET \* AUSTRALIAN INSTITUTE OF BUSINESS AND MANAGEMENT PTY LTD PAGE **1** OF **1**

16 January 2023 CRICOS 03171A ABN: 72 132 629 979

**TABLE OF CONTENTS**

[GROUP ASSIGNMENT COVERSHEET 1](#_Toc177298883)

[TABLE OF CONTENTS 2](#_Toc177298889)

[LIST OF FIGURES 4](#_Toc177298890)

[LIST OF TABLES 5](#_Toc177298891)

[EXECUTIVE SUMMARY 6](#_Toc177298892)

[1.0. INTRODUCTION 7](#_Toc177298893)

[2.0. BACKGROUND AND LITERATURE REVIEW 8](#_Toc177298894)

[3.0. DESIGN AND DEVELOPMENT 9](#_Toc177298895)

[3.1. Requirement 9](#_Toc177298896)

[3.2. System and Application Architecture 9](#_Toc177298897)

[3.3. Main Components 10](#_Toc177298898)

[3.4. Introduction of Contiki and Cooja 12](#_Toc177298899)

[3.5. Application and System Development using Contiki 12](#_Toc177298900)

[3.5.1. Router Sky Mote (Platform Layer) 13](#_Toc177298901)

[3.5.2. Server Sky Mote (Network Layer) 14](#_Toc177298902)

[3.5.3. Smart Lights Sky Mote (Sensing Layer) 15](#_Toc177298903)

[3.5.4. Smart Fan Sky Mote (Sensing Layer) 16](#_Toc177298904)

[3.5.5. Smart Air Conditioning (AC) Sky Mote (Sensing Layer) 17](#_Toc177298905)

[3.5.6. Smart Washing Machine Sky Mote (Sensing Layer) 18](#_Toc177298906)

[3.6. Results 19](#_Toc177298907)

[3.6.1. Router (Platform Layer) 20](#_Toc177298908)

[3.6.2. Server (Network Layer) 22](#_Toc177298909)

[3.6.3. Smart Lights (Sensing Layer) 23](#_Toc177298910)

[3.6.4. Smart Fan (Sensing Layer) 25](#_Toc177298911)

[3.6.5. Smart Air Conditioning (AC) (Sensing Layer) 27](#_Toc177298912)

[3.6.6. Smart Washing Machine (Sensing Layer) 29](#_Toc177298913)

[4.0. SECURITY ISSUES OF PROPOSED APPLICATION AND SYSTEM 31](#_Toc177298914)

[4.1. Introduction of Threads Modelling Techniques 31](#_Toc177298915)

[4.2. System Architecture 31](#_Toc177298916)

[4.3. Analysis Security Issues Using Threats Model 32](#_Toc177298917)

[4.3.1. Identifying Assets 32](#_Toc177298918)

[4.3.2. Identifying Threats 33](#_Toc177298919)

[4.3.3. Analysing Vulnerabilities 34](#_Toc177298920)

[5.0. SECURITY SOLUTIONS 35](#_Toc177298921)

[5.1. Spoofing 35](#_Toc177298922)

[5.2. Tampering 36](#_Toc177298923)

[5.4. Information Disclosure 37](#_Toc177298924)

[5.5. Denial of Service 37](#_Toc177298925)

[5.6. Elevation of Privilege 38](#_Toc177298926)

[6.0. CONCLUSION 39](#_Toc177298927)

[REFERENCES 40](#_Toc177298928)

# LIST OF FIGURES

[Figure 3‑1. System Architecture 10](#_Toc177299949)

[Figure 3‑2. Creation of New Simulation 12](#_Toc177299950)

[Figure 3‑3. Router Sky Mote 13](#_Toc177299951)

[Figure 3‑4. Router - Add Motes 13](#_Toc177299952)

[Figure 3‑5. Server Sky Mote 14](#_Toc177299953)

[Figure 3‑6. Server - Add Motes 14](#_Toc177299954)

[Figure 3‑7. Smart Lights Sky Mote 15](#_Toc177299955)

[Figure 3‑8. Smart Lights - Add Motes 15](#_Toc177299956)

[Figure 3‑9. Smart Fan Sky Mote 16](#_Toc177299957)

[Figure 3‑10. Smart Fan - Add Motes 16](#_Toc177299958)

[Figure 3‑11. Smart Air Conditioning (AC) Sky Mote 17](#_Toc177299959)

[Figure 3‑12. Smart AC - Add Motes 17](#_Toc177299960)

[Figure 3‑13. Smart Washing Machine Sky Mote 18](#_Toc177299961)

[Figure 3‑14. Smart Washing Machine - Add Motes 18](#_Toc177299962)

[Figure 3‑15. Serial Socket (SERVER) for Sky Mote 1 19](#_Toc177299963)

[Figure 3‑16. Radio Messages 19](#_Toc177299964)

[Figure 3‑17. Terminal Router Connection 20](#_Toc177299965)

[Figure 3‑18. Serial Socket and Radio Messages of Router Sky Mote 21](#_Toc177299966)

[Figure 3‑19. Router Mote Output 21](#_Toc177299967)

[Figure 3‑20. Server Boot Up 22](#_Toc177299968)

[Figure 3‑21. Smart Lights Boot Up 23](#_Toc177299969)

[Figure 3‑22. Smart Lights Turning On 24](#_Toc177299970)

[Figure 3‑23. Smart Lights Turning Off 24](#_Toc177299971)

[Figure 3‑24. Smart Fan Boot Up 25](#_Toc177299972)

[Figure 3‑25. Smart Fan Turning On 26](#_Toc177299973)

[Figure 3‑26. Smart Fan Turning Off 26](#_Toc177299974)

[Figure 3‑27. Smart AC Boot Up 27](#_Toc177299975)

[Figure 3‑28. Smart AC Turning On 28](#_Toc177299976)

[Figure 3‑29. Smart AC Turning OFF 28](#_Toc177299977)

[Figure 3‑30. Smart Washing Machine Boot Up 29](#_Toc177299978)

[Figure 3‑31. Smart Washing Machine Turning On 30](#_Toc177299979)

[Figure 3‑32. Smart Washing Machine Turning Off 30](#_Toc177299980)

[Figure 4‑1. System Architecture Threat Modelling 31](#_Toc177299981)

# LIST OF TABLES

[Table 3‑1. IoT System Architecture 11](#_Toc177299982)

[Table 4‑1. Identifying Assets 32](#_Toc177299983)

[Table 4‑2. Identifying Threats 33](#_Toc177299984)

[Table 4‑3. Analysing Vulnerabilities 34](#_Toc177299985)

# EXECUTIVE SUMMARY

The paper talks about the development, benefits, and issues with an application of IoT on home device management besides mentioning a few security-related challenges. The Internet of Things (IoT) has changed the concept of home automation by bringing more and more ordinary household devices onto the internet so that users can easily control and monitor appliances from a remote location. IoT, thus applied in home appliances, makes life easier, power-saving, and user-oriented; hence, it leads to a smart and green living environment.

The study focuses on the detailed analysis of different IoT-based smart home devices and their efficiency in making life standards high at home. In addition to the benefits, the report also discussed some critical security and privacy related issues about IoT, which included vulnerability to cyber-attacks, unauthorized access, and data breach. This applies the STRIDE threat modelling framework to possible threats such as spoofing and tampering and those that cause denial of service.

Such threats are mitigated by the report with robust security measures: encryption, controlled access, intrusion detection, and incident response strategies. The future development of IoT with new frontiers in AI and 5G communication will bring enhancements in both security and functionalities of smart home systems. The project strongly emphasizes that integration of proper security protocols is required to not lose the trust of the customer and creates awareness on IoT technologies for home automation.

# INTRODUCTION

IoT in home automation has brought about a tremendous transformation in the interface between man and his ordinary appliances. The integration of IoT into ordinary devices will make it easy to control light systems, temperature regulators, and security mechanisms from remote areas toward value addition to the user experience and improvement of energy consumption efficiencies and space personalization. It's a technologically advanced feature that is going to connect all devices around us to the internet for their communication and response to commands through smartphones, tablets, or voice assistants, including Amazon Alexa and Google Home.

IoT adoption brought several benefits in home automation, energy use reduction using smart thermostats, increased security due to intelligent monitoring systems, and generally an improved quality of life. This advantage has also emerged with a lot of challenges, most of which relate to security and privacy aspects. The interlinked structure of the devices that make up the IoT exposes them easily to cyber-attacks, and therefore, safeguarding user data becomes extremely important to foster trust in these emerging technologies.

A literature review will discuss the numerous applications existing in the IoT domain for control of household appliances, examining benefits, challenges, and possible future development. With technology booming again, the field of IoT appears to go beyond even further improvements in home automation, thus providing an increasingly sophisticated and secure solution for modern living.

# BACKGROUND AND LITERATURE REVIEW

The technology of the IoT allows the user to remotely control and monitor household appliances using smartphones or other communicating devices. This brings in convenience and energy efficiency. For example, IoT-based thermostats can learn from user patterns and adjust heating or cooling of buildings accordingly, leading to significant energy savings (Bashir & Gill, 2016).

To the point, for example, home automation, innovative mechanisms supported by Amazon Alexa, and Google Home have become popular. The configuration of these systems combines many IoT-enabled devices to regulate lighting intensity, security systems, and household appliances via voice control or mobile applications (Darianian & Michael, 2008).

Such integration makes home management easy and convenient for users. In addition, these IoT applications in controlling appliances work toward effective energy use and sustainability. Real-time energy consumption information from smart meters and IoT-enabled appliances can help optimize operation with a view to spending on other things. Some researchers have indicated that such IoT-based energy management systems will lead to significant reduction in energy consumption—the classic win-win situation (Gungor et al., 2013).

While IoT holds numerous benefits, it also presents dangers to security and privacy. The interconnected nature of the IoT devices indeed exposes them to various hidden cyberpunks awaiting their turn for a bite. Ensuring the security of IoT systems is critical to protect user data and maintain trust in these technologies (Roman, Zhou & Lopez, 2013).With the development of artificial intelligence and machine learning technologies, the future of IoT in controlling appliances looks quite promising. These technologies with IoT will bring further sophistication in automation and predictive maintenance of appliances for their greater efficiency and usability (Sethi & Sarangi, 2017). Furthermore, 5G networks will also bring ease in communication between the IoT devices, and it would be faster and highly reliable.

# DESIGN AND DEVELOPMENT

## Requirement

Sometimes people leave their home appliances turned-on and forget to turn-off because of this it costs them a lot of money and wasted energy. To solve this problem, the team created a smart home appliance where it can control the switch of the appliances. A sensing layer, network layer, platform layer, and application layer are the requirements for smart home appliances.

## System and Application Architecture

For smart home appliances, its architecture is divided into four layers. Here's a breakdown of each layer and its roles. The actuators are connected to the network layer which is the zigbee through Bluetooth. The zigbee then sends the data to the platform layer through Wi-Fi.

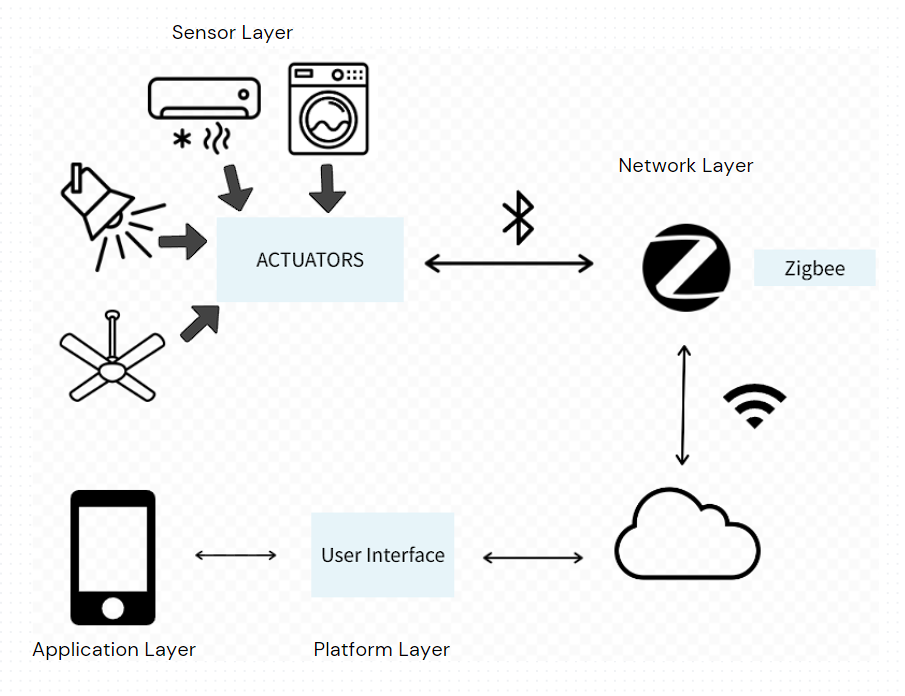


Figure 3‑1. System Architecture

## Main Components

|  |  |  |
| --- | --- | --- |
| IoT System Architecture | Description | Sample Image |
| Sensing Layer | This is the first layer in the system architecture of smart home appliances. Sensing Layer gathers the information acting as the main senses of the different appliance to pick up user input.  The sensors used are:  **Actuators** - device that makes something move or operate. It receives a source of energy and uses it to move something. | Actuators |
| Network Layer | The communication and gateway from appliances to devices is the network layer.  Zigbee sensors are going to be utilized and act as a router to connect the device.  Wi-Fi Connection will also serve as a secondary gateway to connect the light to the device. | Zigbee Router:  Mi Light Bluetooth Gateway, Zigbee Hub 3.0 For Sale | Miboxer |
| Platform Layer | The platform layer will be done via web service and mobile application to control the appliances wherever and whenever the user wants to switch on or off the lights.  Database and server is also setup via cloud service to store information within the system. |  |
| Application Layer | Monitoring: technical option to access the system on a mobile app or desktop device. Programmers can also choose the features for the user interface such as buttons, sliders or gauge.  Control: The web services can connect to web browsers and can use javascript-based Bootstrap to develop the website. |  |

Table 3‑1. IoT System Architecture

All these parts are working together. For example, when the user wants to access the appliance (application layer), it checks if it is an authorized user (platform layer). If an authorized user then it will send a packet and communicate to the cloud and router (network layer) to control the appliances (sensor layer).

## Introduction of Contiki and Cooja

Contiki is an operating system which is widely used for low-power wireless Internet of Things smart devices. The Contiki provides built-in and multitasking Internet Protocol process (Network Simulation Tools, 2021).

Ne3 Simulations (2021) describe the “Cooja as one of the network simulators of Contiki OS.” It allows small and large networks of IoT motes to be simulated in one simulation. Cooja is the sensor network simulator of Contiki and it is also known as the Contiki OS Java Simulator.

## Application and System Development using Contiki

In developing the application and system development of Smart Home Appliances, a simulation from Cooja using Contiki OS will be utilized. Our team named the Simulation as Smart Home Appliances. Figure 3-2 depicts the creation of the new simulation.

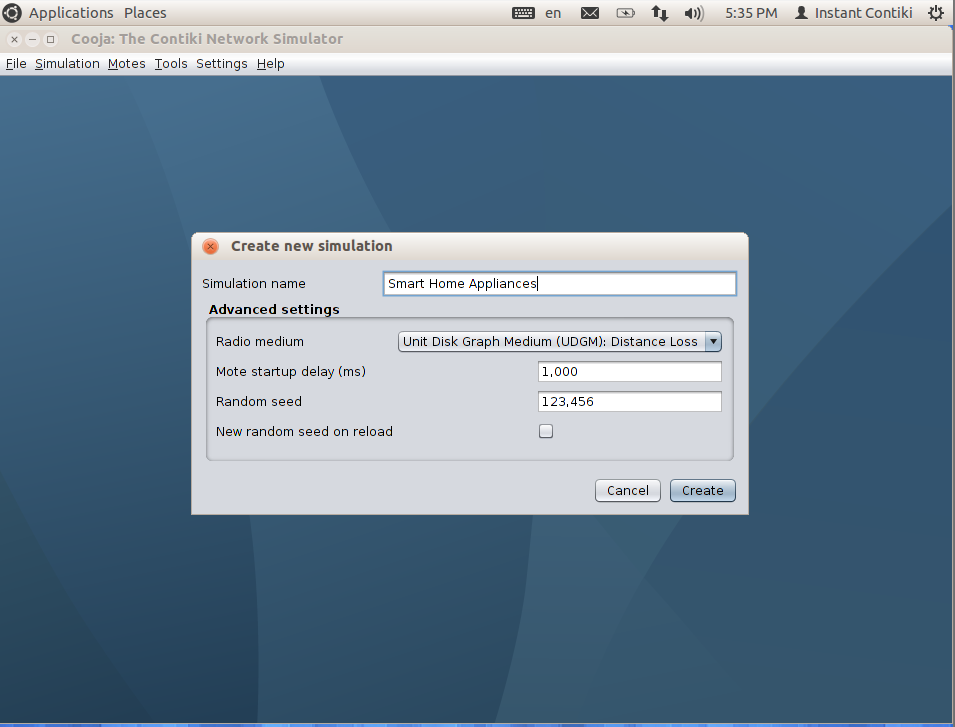


Figure 3‑2. Creation of New Simulation

### Router Sky Mote (Platform Layer)

The Sky Mote for our router is based in rpl-border-router which stands for Routing Protocol for Low-Power and Lossy Networks. This router is aimed for low power consumption and susceptible to packet losses. We made the router as the first sky mote to be able to connect easily and act as the router towards the other motes. We noticed that if didn’t make the router as the first sky mote, the terminal of Contiki doesn’t connect to the router. Figure 3-3 depicts the creation of Router Mote in the simulation.

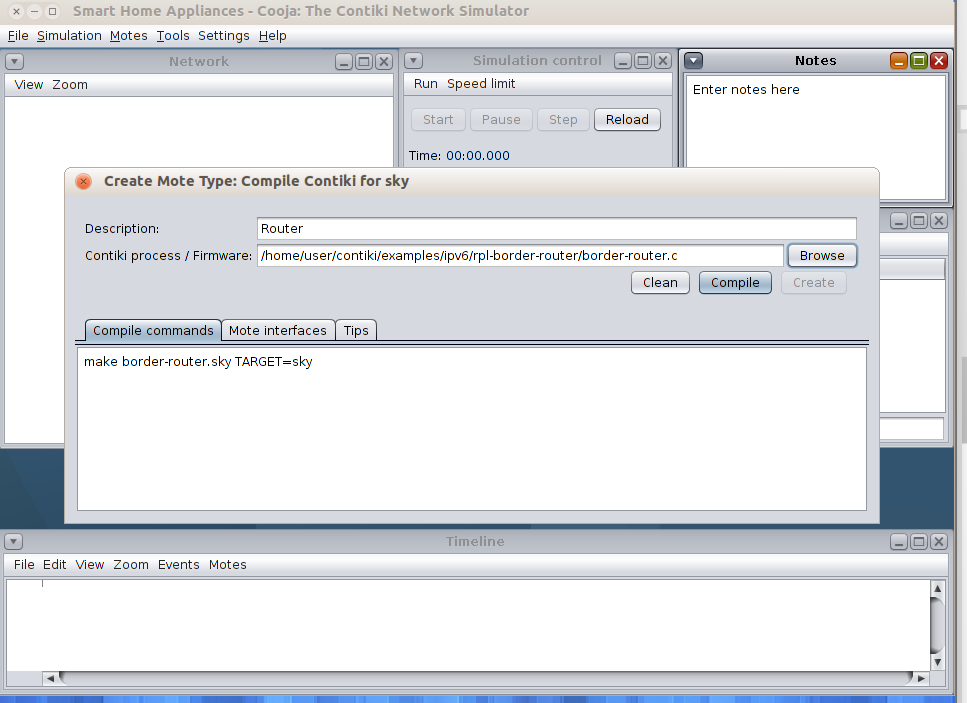


Figure 3‑3. Router Sky Mote

In this simulation, only 1 sky mote for router is going to be utilized.

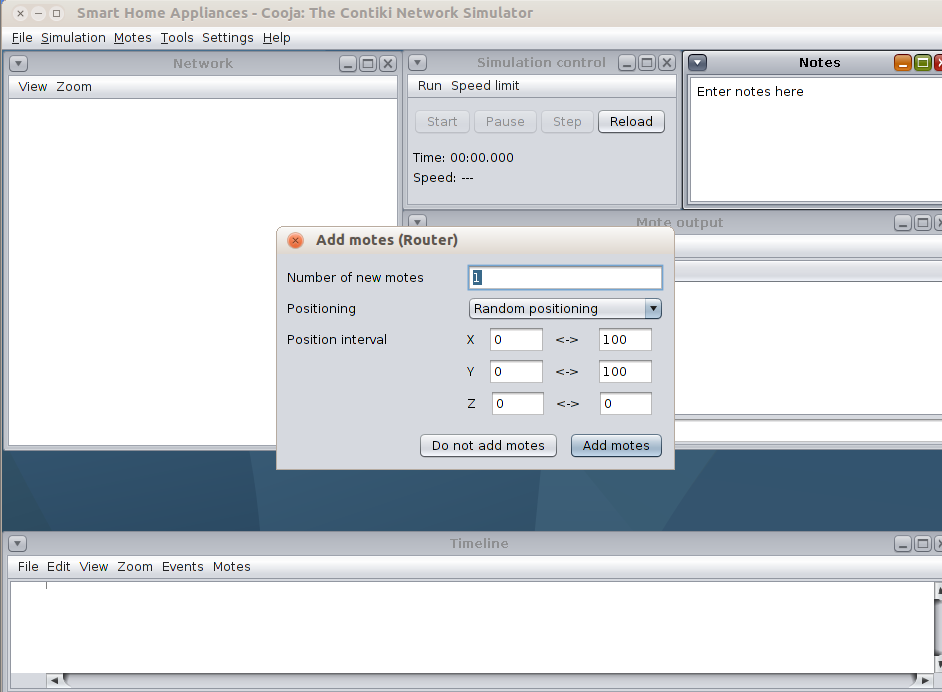


Figure 3‑4. Router - Add Motes

### Server Sky Mote (Network Layer)

The server sky mote is derived from udp-server.c of ipv6/rpl-udp in Contiki. Our group utilized the code and modified it to receive incoming messages from the smart devices and display the latest message. This server does not display the messages every second compared to udp-server but only capture and display the message if the smart device communicated to the server. Figure 3-5 displays the creation of Server Sky Mote.

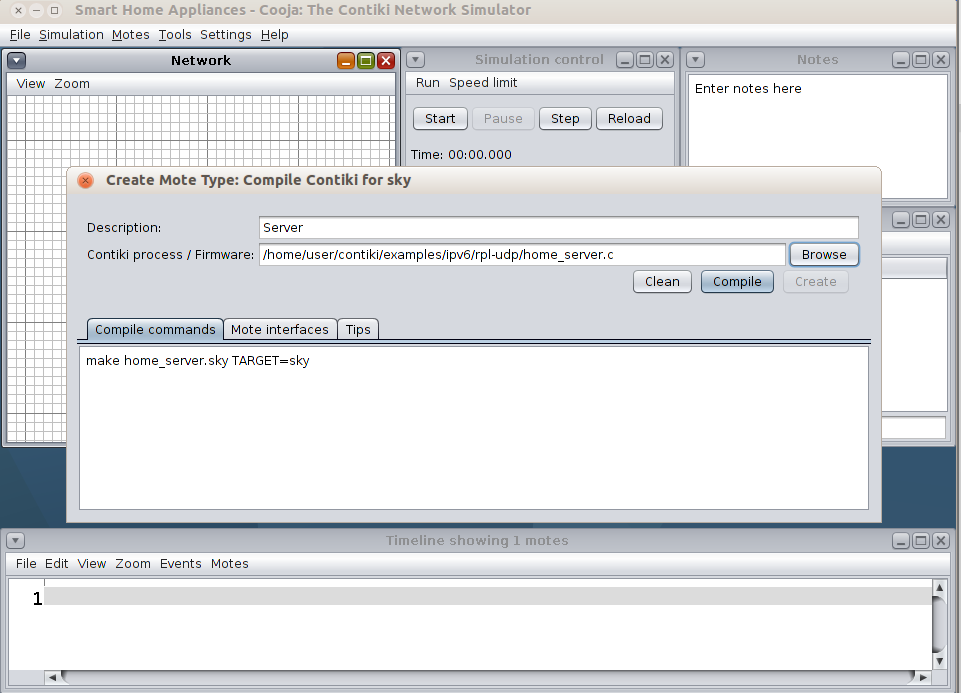


Figure 3‑5. Server Sky Mote

One Sky Mote Server is created in this simulation.

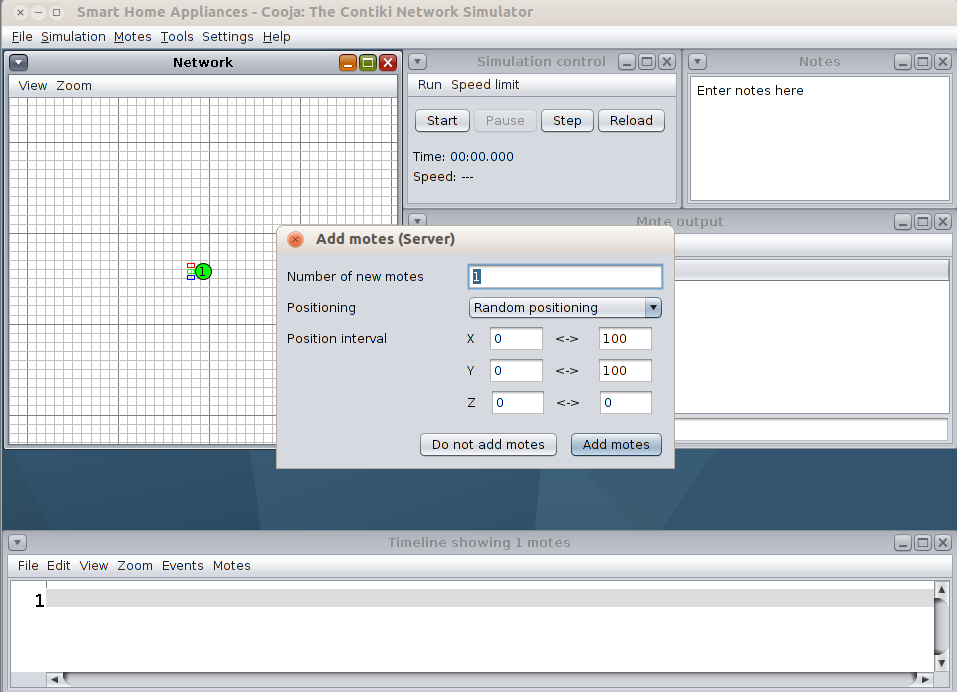


Figure 3‑6. Server - Add Motes

### Smart Lights Sky Mote (Sensing Layer)

Smart Light Sky Mote are created using the udp-client.c of ipv6/rpl-udp in Contiki. The group modified and derived the code from udp-client.c to make the Smart Light Sky Mote as a functional actuator that responds to the click of the button. Once the button is clicked, the lights will turn on and the device will send a message in the server indicating that it is turned on or off. Red, blue, and green LEDs are also used that lights up when the sky mote is turned on and turns off when sky mote is turned off. Figure 3-7 displays the creation of Smart Lights, the group decided to call the sky mote as ‘Lights’ for easier depiction.

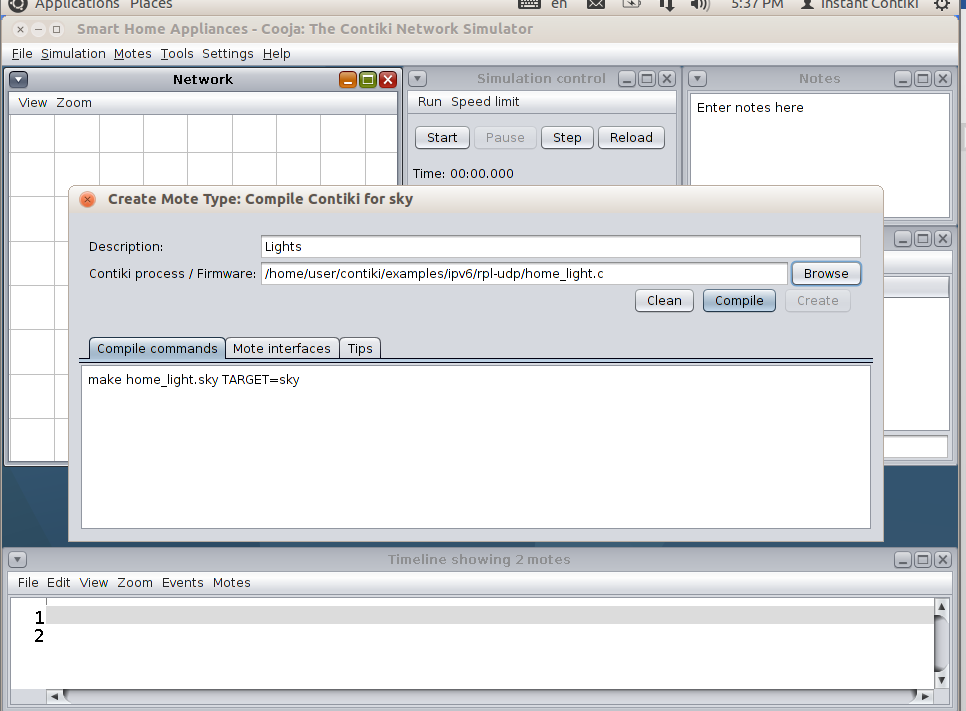


Figure 3‑7. Smart Lights Sky Mote

Two Sky Motes for Smart Lights are employed in this simulation.

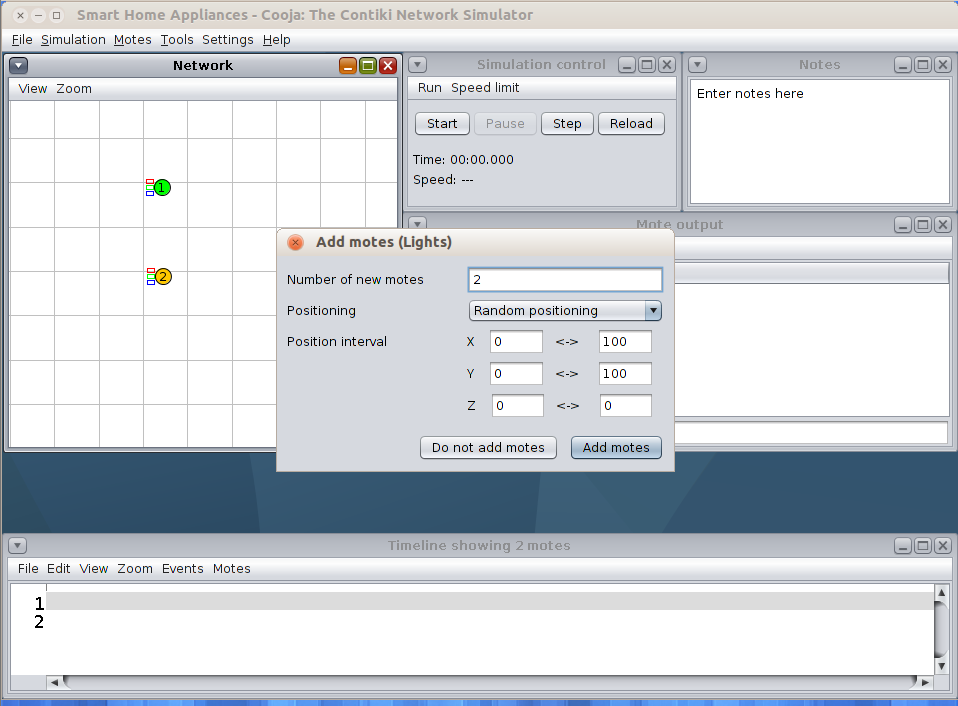


Figure 3‑8. Smart Lights - Add Motes

### Smart Fan Sky Mote (Sensing Layer)

Smart Fan Sky Mote is derived from udp-client.c just like Smart Lights. Smart Fan is programmed to be turned on and off with the click of a button. Red and Green LEDs are applied to indicate whether the Smart Fan is on or off. If Red LED is on, it means that Smart Fan is off. On the other hand, if Green LED is on, it means that Smart Fan is on. Figure 3-9 displays the creation of Smart Fan Sky Mote.

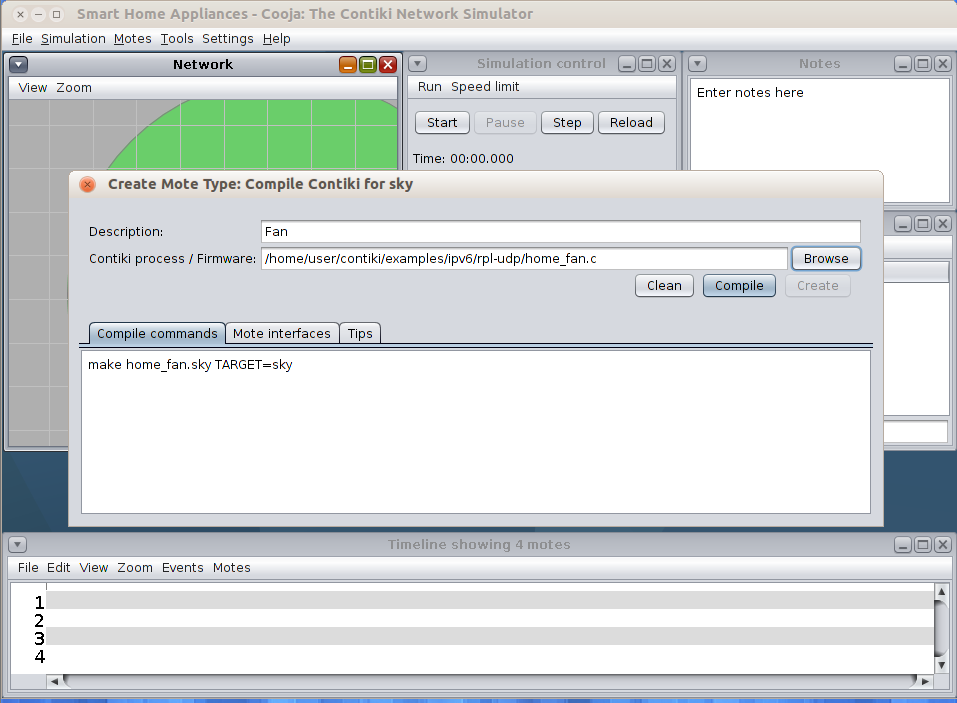


Figure 3‑9. Smart Fan Sky Mote

Only 1 Sky Mote for Smart Fan is used in the simulation.

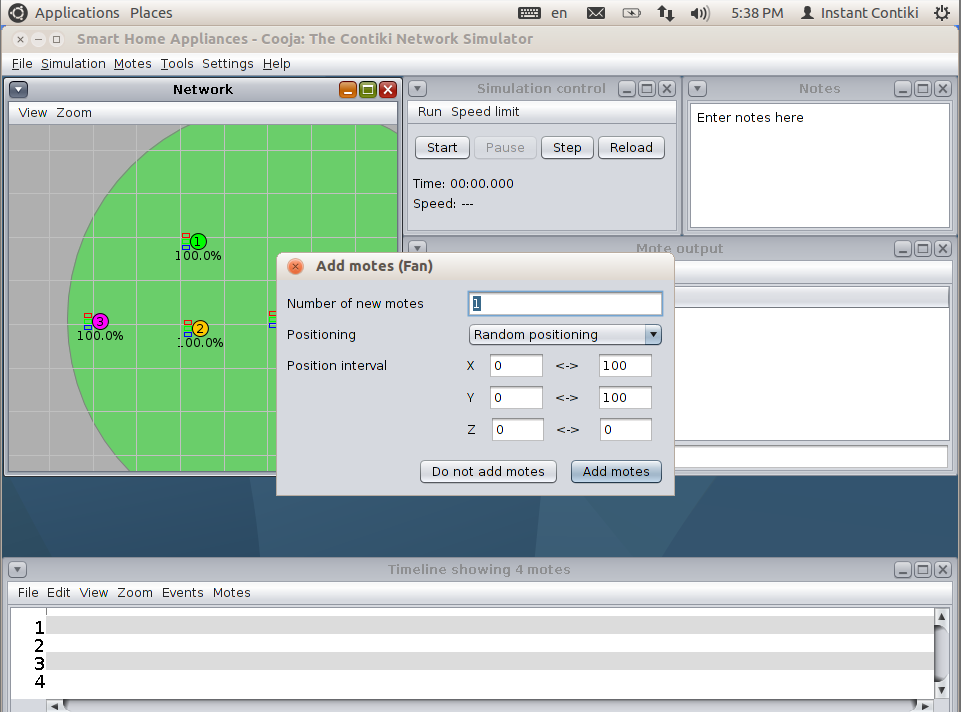


Figure 3‑10. Smart Fan - Add Motes

### Smart Air Conditioning (AC) Sky Mote (Sensing Layer)

Smart Air Conditioning (AC) Sky Mote is also derived from udp-client.c just like Smart Lights. Smart AC just like Smart Fan and Smart Lights is programmed to be turned on and off with the click of a button. Red and Green LEDs are applied to imply if the AC is currently turned on or off. Figure 1-11 shows the creation of Smart AC Sky Mote.

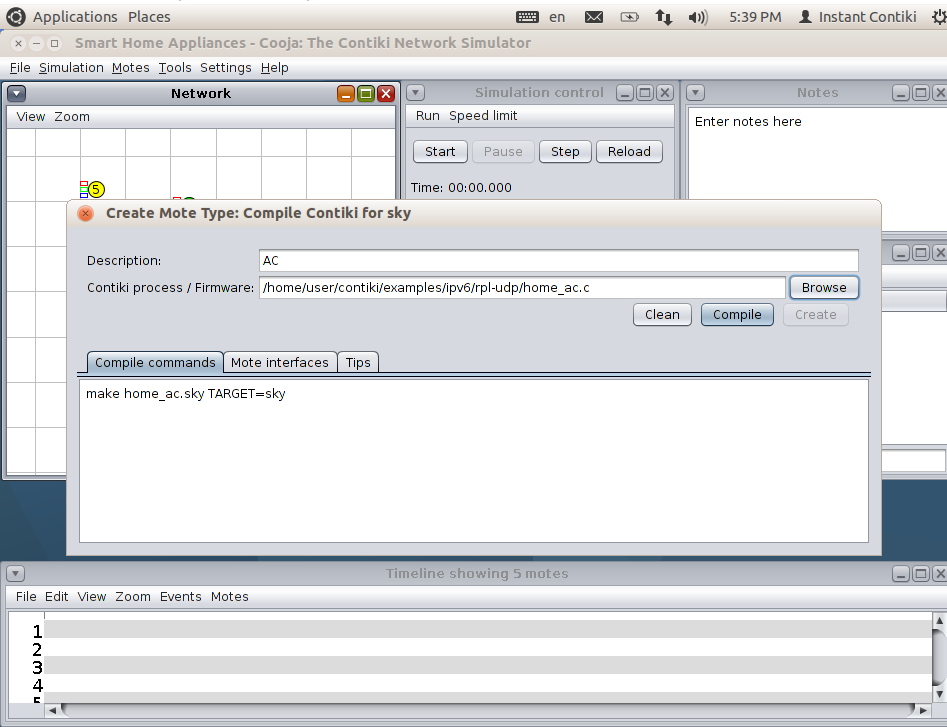


Figure 3‑11. Smart Air Conditioning (AC) Sky Mote

For the simulation, 1 Sky Mote of Smart AC is utilized.

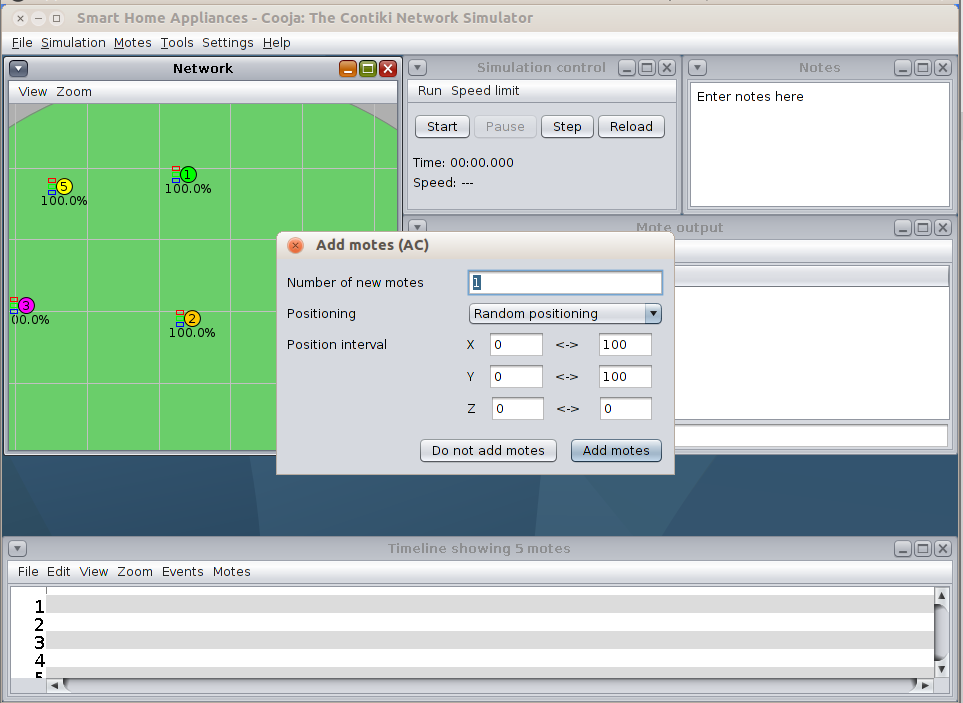


Figure 3‑12. Smart AC - Add Motes

### Smart Washing Machine Sky Mote (Sensing Layer)

Smart Washing Machine just like the other smart devices are derived from udp-client.c. Smart Washing Machine also uses the Red and Green LEDs to indicate if the smart device is currently turned on or off. Figure 3-13 displays the creation of Smart Washing Machine Sky Mote.

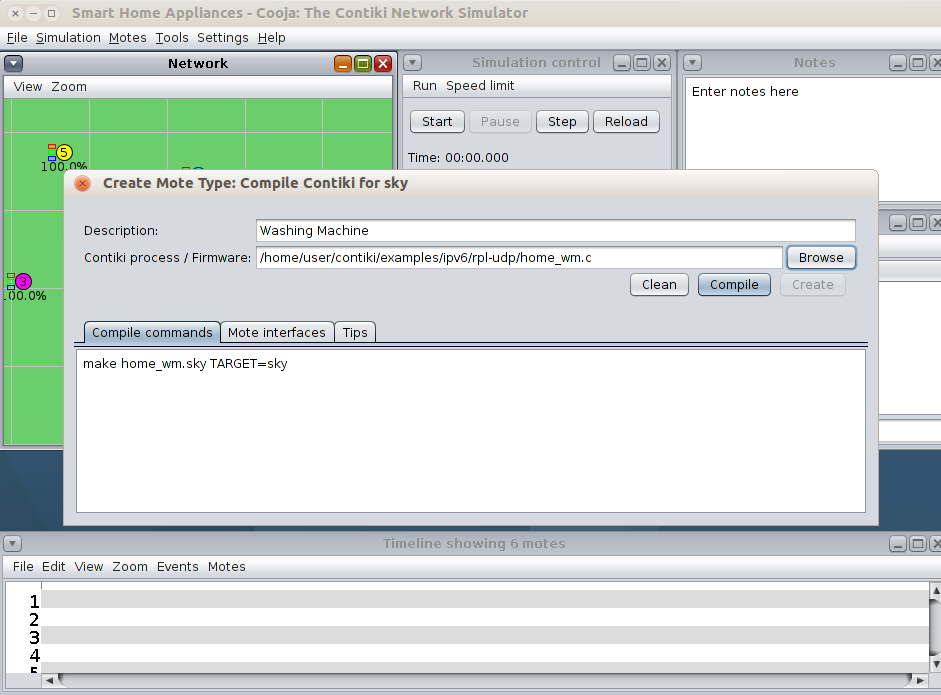


Figure 3‑13. Smart Washing Machine Sky Mote

In this simulation, only 1 Smart Washing Machine will be employed.

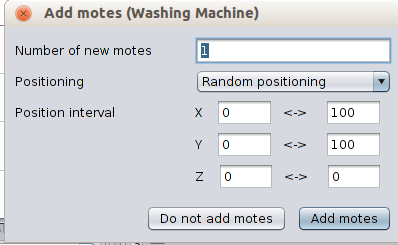


Figure 3‑14. Smart Washing Machine - Add Motes

## Results

Before the simulation is started, we had to use the tool, Serial Socket (SERVER) for sky mote 1 (Router). Enabling this tool for the Router will make it connect to the terminal and get packets. Figure 3-15 shows how the serial socket is enabled for sky mote 1.

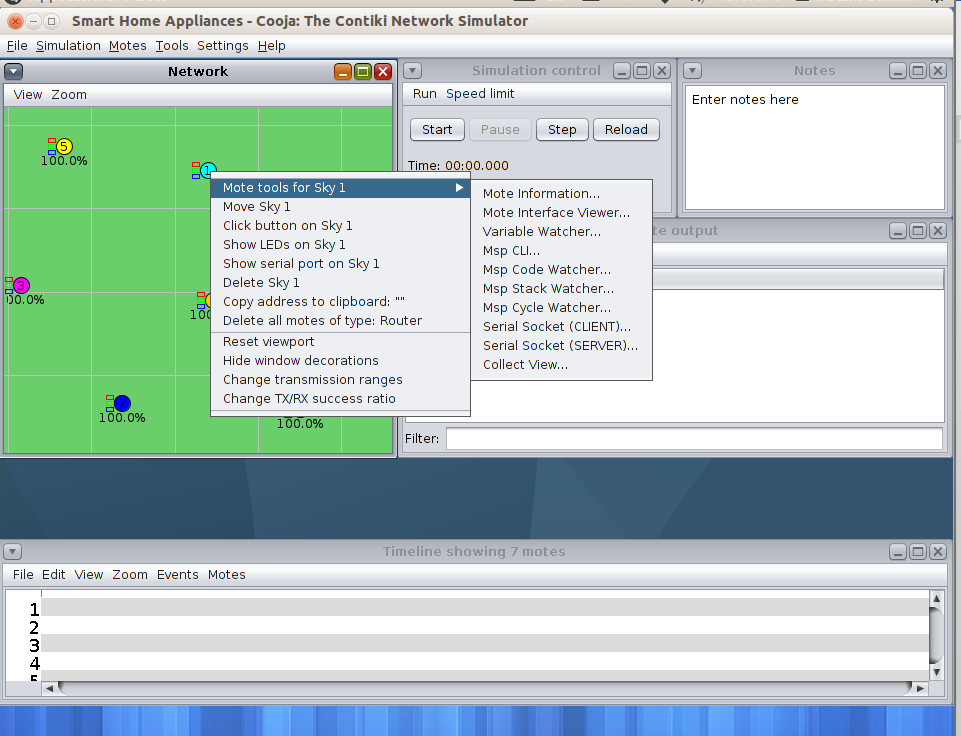


Figure 3‑15. Serial Socket (SERVER) for Sky Mote 1

Figure 3-16 shows how to enable the Radio Messages to see the packets that is happening within the network.

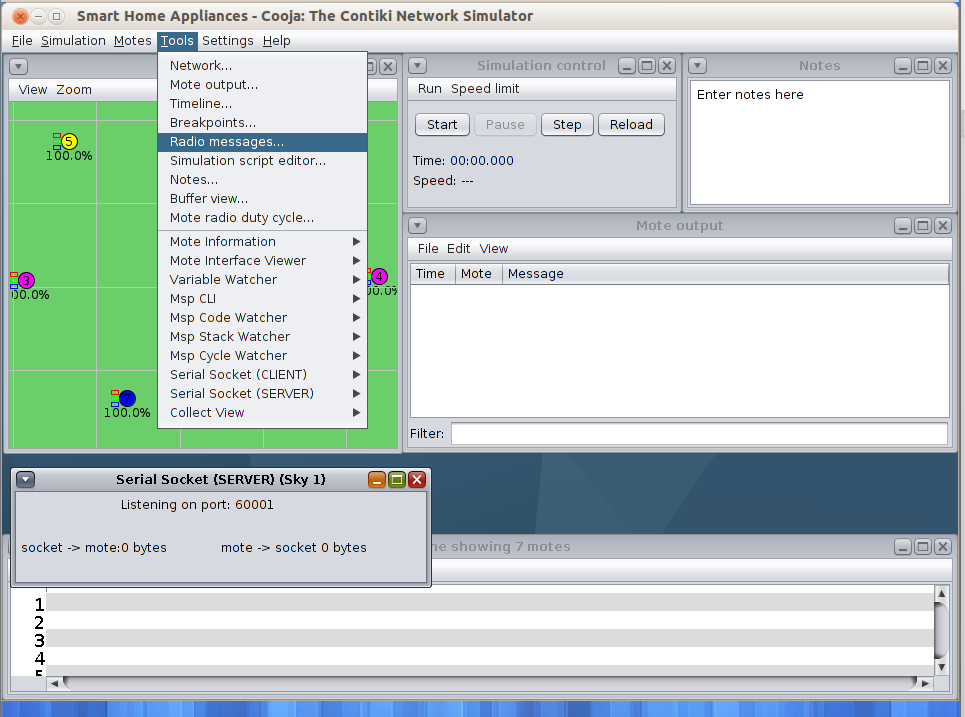
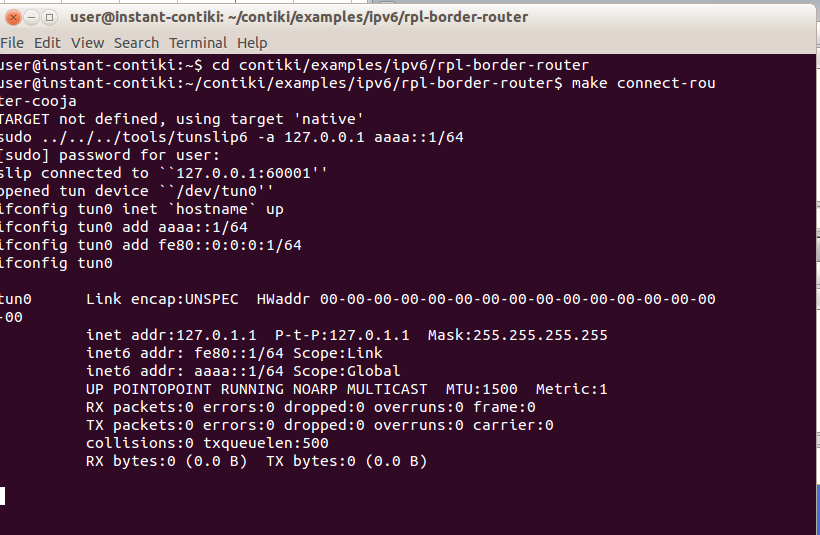


Figure 3‑16. Radio Messages

### Router (Platform Layer)

After enabling the serial socket and radio messages for Router Sky Mote, it is now time to connect the router in the internet. From the terminal, we typed ‘cd contiki/examples/ipv6/rpl-border-router’ to go to the directory of the router file then we entered ‘make connect-router-cooja’. Figure 3-17 shows that the connection is successful in the terminal.



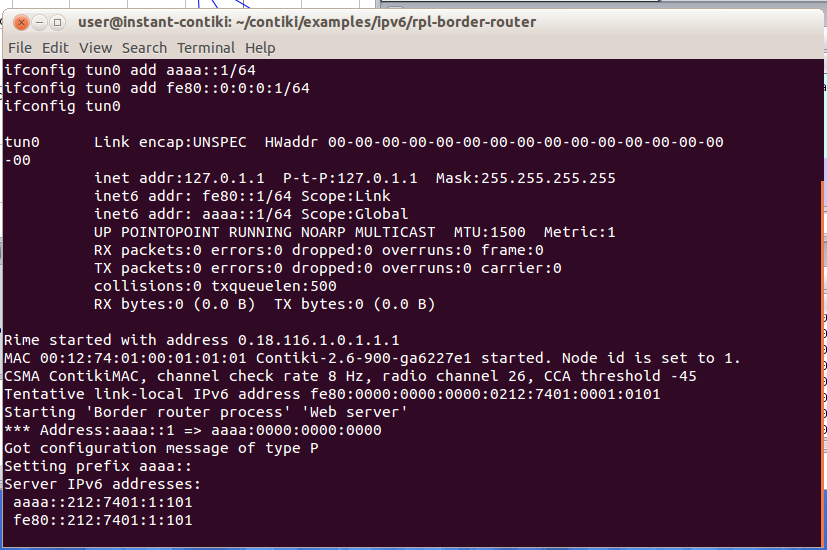


Figure 3‑17. Terminal Router Connection

Once we pressed ‘Start’ in the simulation control, the Serial Socket shows that the client is connected in the network /127.0.0.1. Packets also started to appear immediately in the Radio Messages.

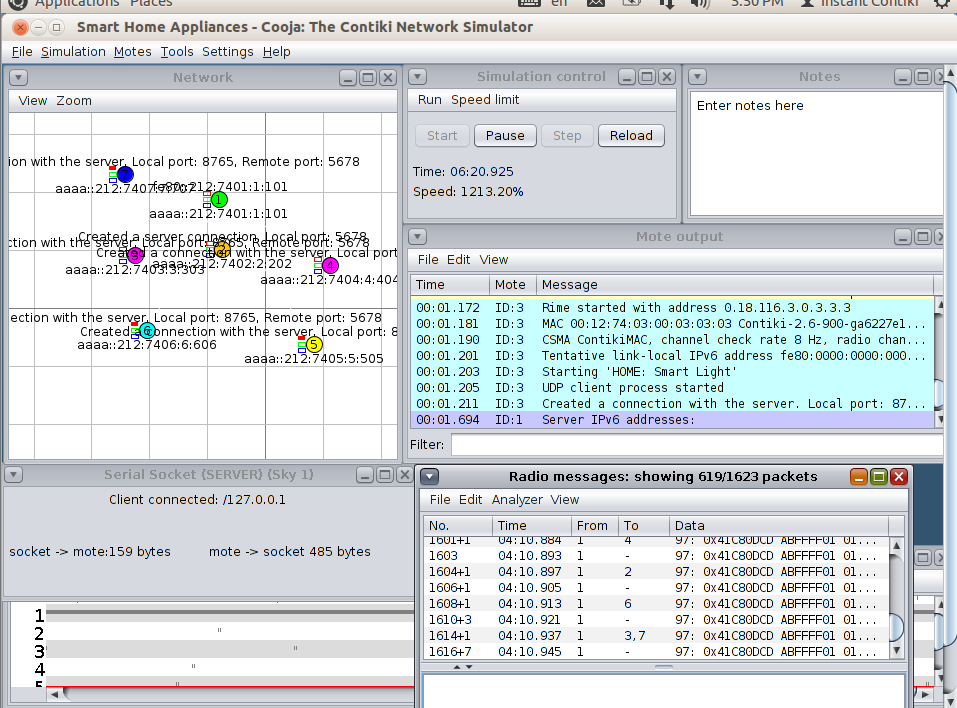


Figure 3‑18. Serial Socket and Radio Messages of Router Sky Mote

A great indication that the router working well is also seen in the mote output. Figure 3-19 shows the successful start of the Router.









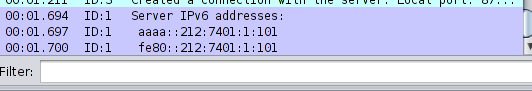


Figure 3‑19. Router Mote Output

### Server (Network Layer)

The server is characterized by Sky Mote 2. Figure 3-20 shows the successful boot up of the server. The Sky Mote 2 indicates the message ‘UDP server process’ meaning that the initiation of the server started without any issues. It created a server connection from the local port, 5678, which is defined in the program.

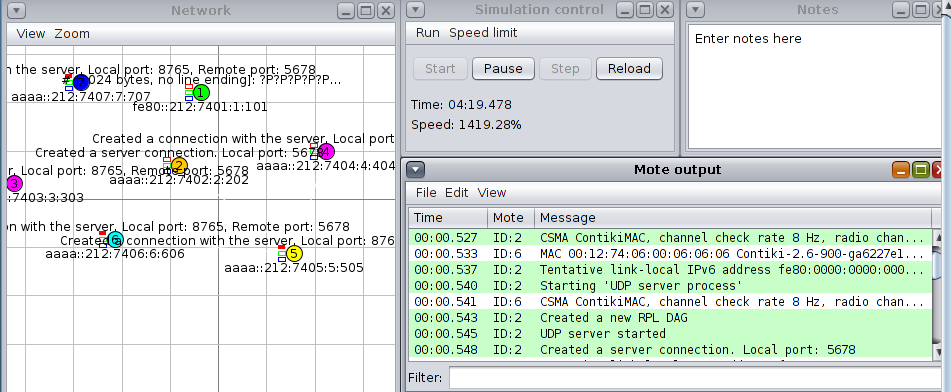


Figure 3‑20. Server Boot Up

The main role of the server is to display the latest message that came from the smart devices. The last device that made a turning on or off process will be displayed by Sky Mote 2. Nevertheless, all transactions between the server and smart devices are saved in the Mote output.

### Smart Lights (Sensing Layer)

Smart Lights, Sky Mote #3 and #4 booted up successfully. Figure 3-21 indicates that the UDP client has started indicating that it is connected to the server.

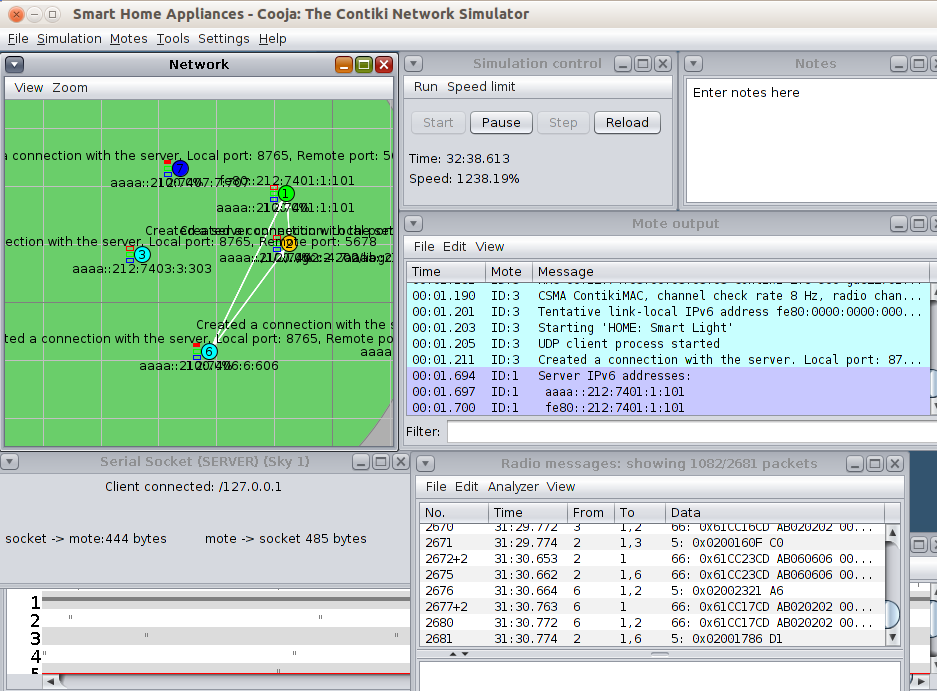


Figure 3‑21. Smart Lights Boot Up

In testing, once the Button of Sky Mote 3 is clicked, the LEDs turned on. Sky Mote 3 also displays the message ‘HOME: Smart Light ON’ and sends the message to the server. The server replies with ‘Data recv’ and displays the message ‘HOME: Smart Light Turning On’.

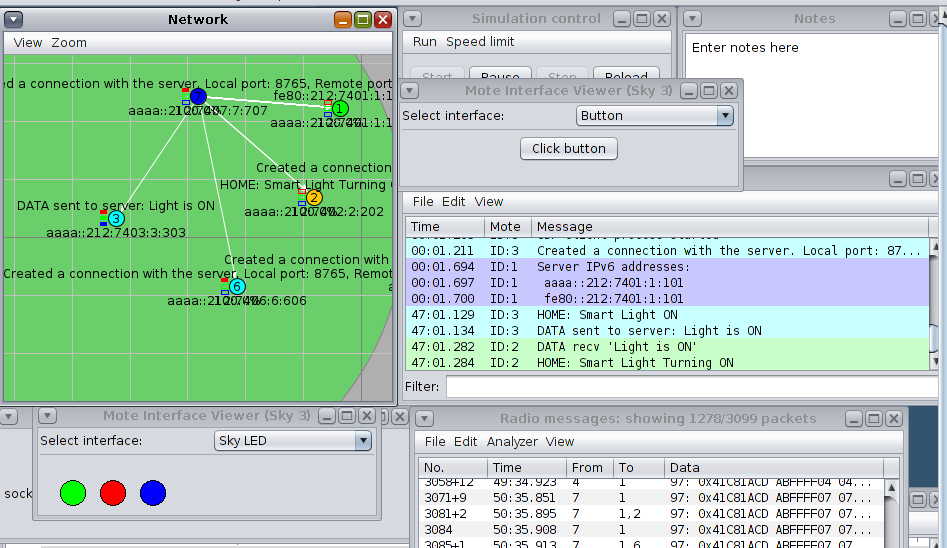


Figure 3‑22. Smart Lights Turning On

If we want to turn it off, just click the button again. All LEDs will turn off, then Sky Mote #3 will display the message ‘HOME: Smart Light OFF’, the data is also sent to the server. The server receives the message and displays the message, ‘HOME: Smart Light Turning OFF”.

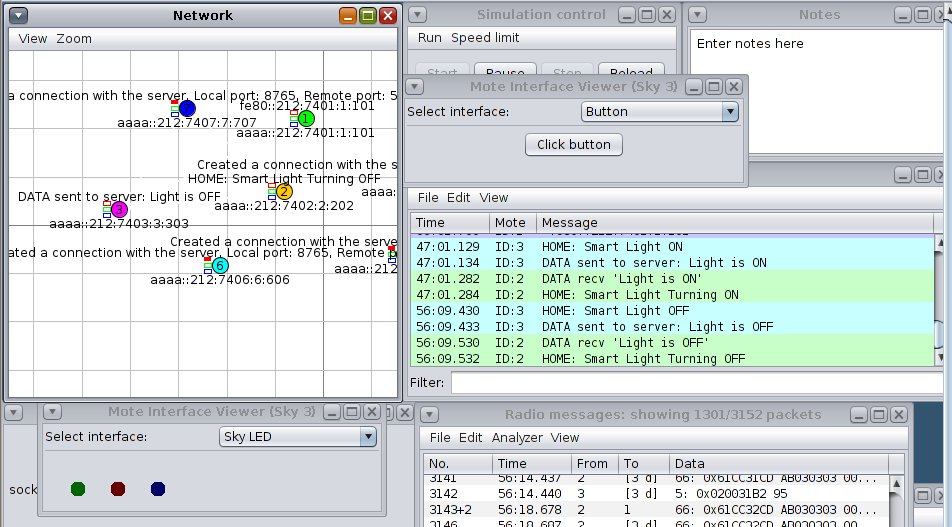


Figure 3‑23. Smart Lights Turning Off

### Smart Fan (Sensing Layer)

Smart Fan is the Sky Mote #5 of the simulation. Figure 3-24 shows the successful boot up of Smart Fan. Just like Smart Lights, it has successfully connected to the server.

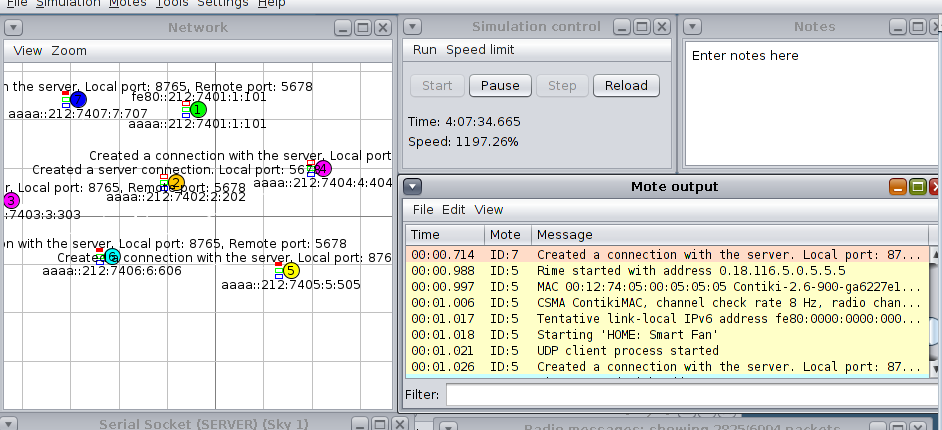


Figure 3‑24. Smart Fan Boot Up

Initially, Smart Fan is turned off. Once we click the button of Sky Mote 5, Green LED turned on, and Sky Mote #5 displays the message ‘HOME: Smart Fan On’. The data is sent to the server, then the server replies with ‘HOME: Smart Fan Turning On’ as an indication that the Smart Fan is on.

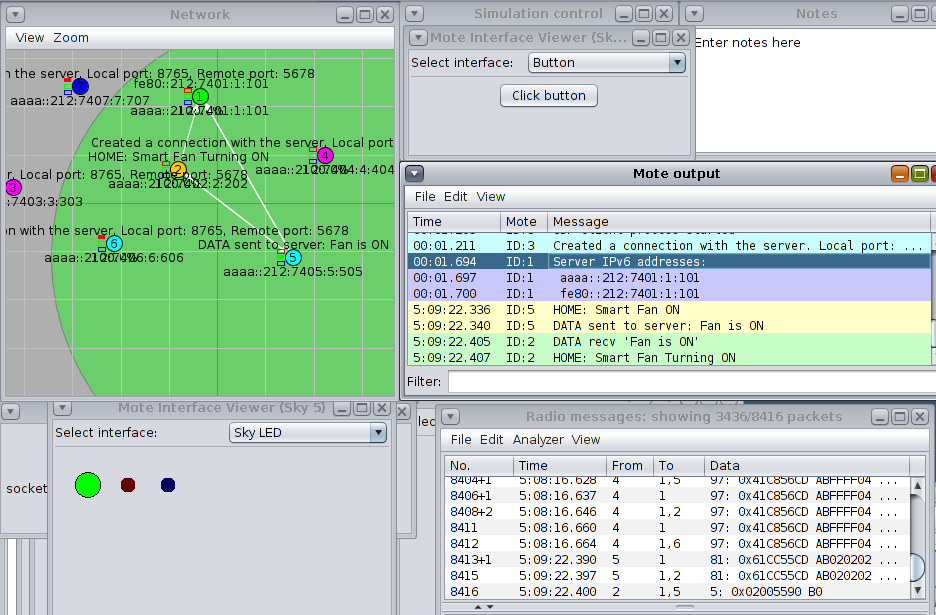


Figure 3‑25. Smart Fan Turning On

Turning off the Fan is done through a click of a button. After the button is clicked, Red LED is turned on and Green LED is off. Sky Mote 5 also displays the message ‘HOME: Smart Fan OFF’. The server receives the data and replies with ‘HOME: Smart Fan Turning OFF’.

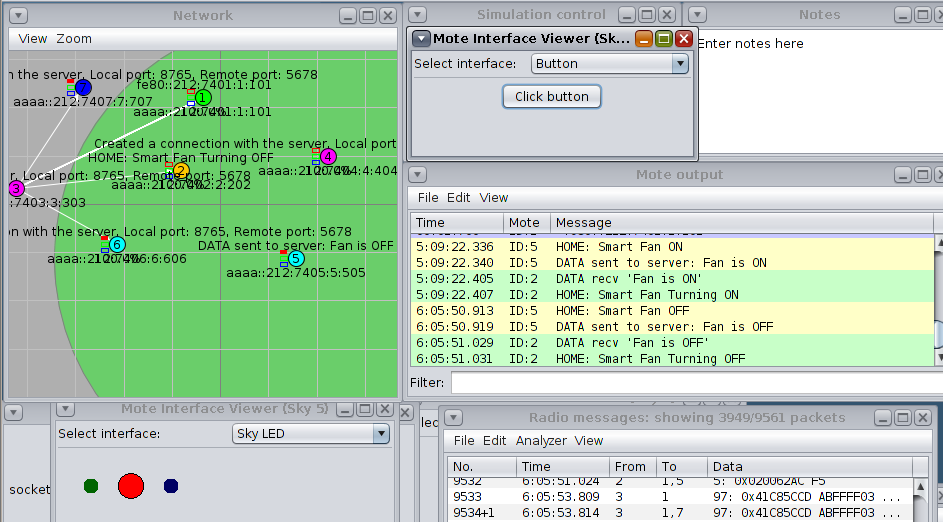


Figure 3‑26. Smart Fan Turning Off

### Smart Air Conditioning (AC) (Sensing Layer)

Smart AC is characterized by Sky Mote #6 in the simulation. From Figure 3-27, it indicates the successful boot up of Smart AC. It has established a connection with the server.

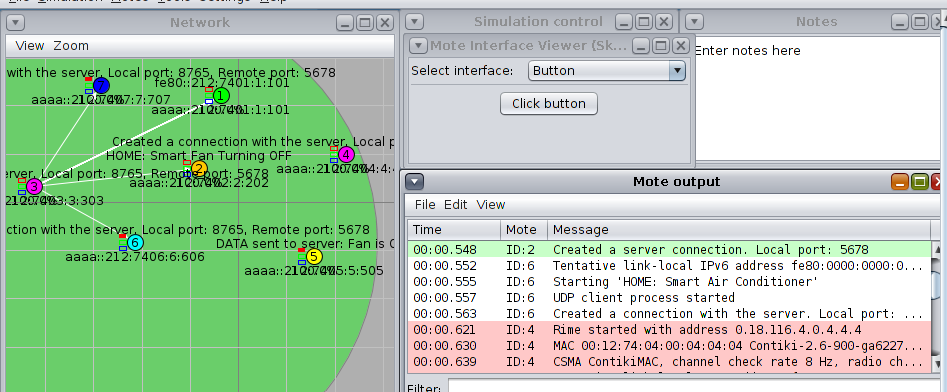


Figure 3‑27. Smart AC Boot Up

Smart AC also works like Smart Fan. It turns on using a button. Once we clicked the button, Green LED of Sky Mote #6 turns on and Sky Mote #6 displays the message ‘HOME: Smart AC ON’. The data is sent to the server and the server responds with ‘HOME: Smart AC Turning ON’.

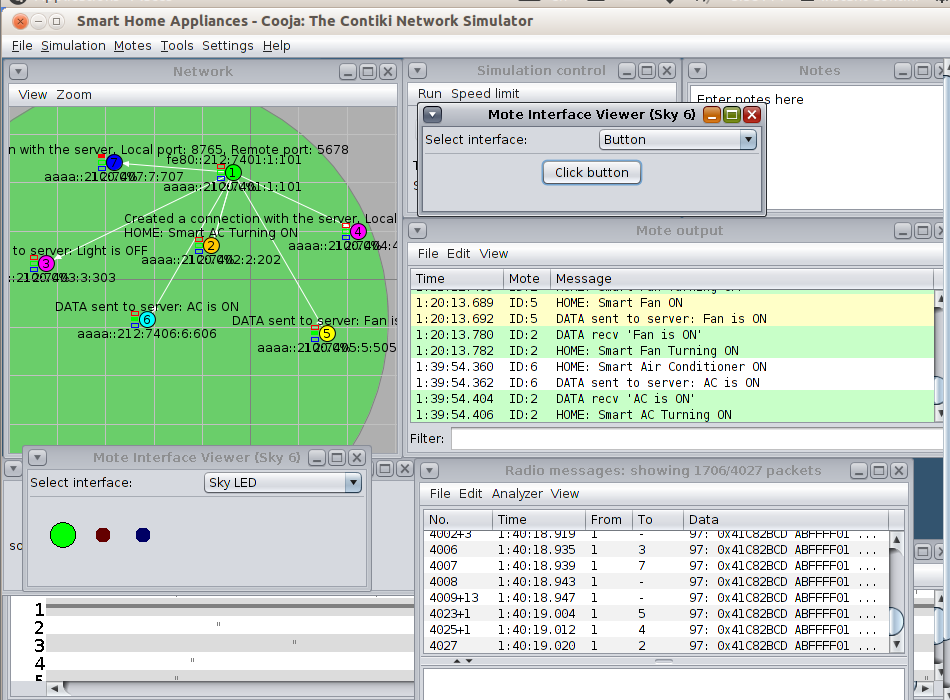


Figure 3‑28. Smart AC Turning On

Turning off the AC is also done by clicking the button again. Once clicked, the RED Led turns on and Green LED turns off. Sky Mote 6 unveils the message ‘HOME: Smart AC OFF’. The server returns the message ‘HOME: Smart AC Turning OFF.”

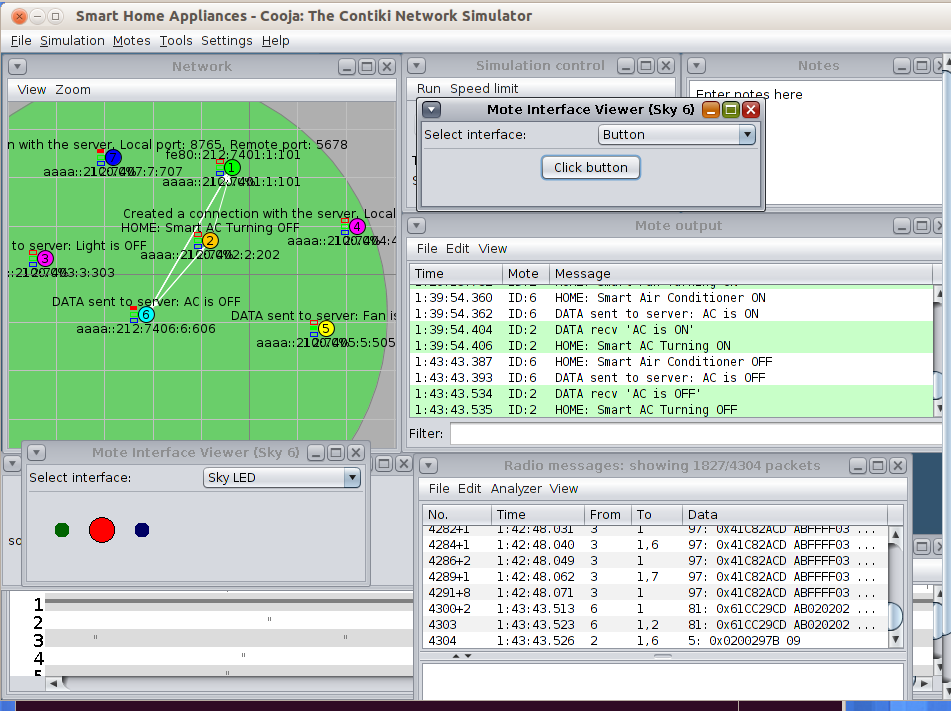


Figure 3‑29. Smart AC Turning OFF

### Smart Washing Machine (Sensing Layer)

Smart Washing Machine is expressed in Sky Mote #7. Figure 3-30 shows the successful boot up of Smart Washing Machine. The Sky Mote #7 created a UDP Client Process that started the connection with the server.

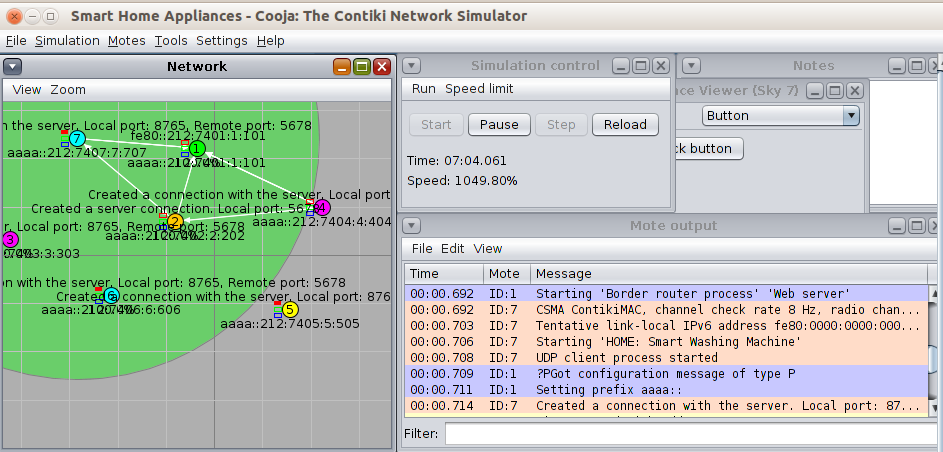


Figure 3‑30. Smart Washing Machine Boot Up

Turning on the Washing Machine is done through the click of a button just like the other smart devices. Once turned on, Green LED brightens up and Sky Mote 7 will display the message ‘HOME: Smart Washing Machine ON’. The data is sent to the server and the server confirms the message by replying ‘HOME: Smart Washing Machine Turning ON.”

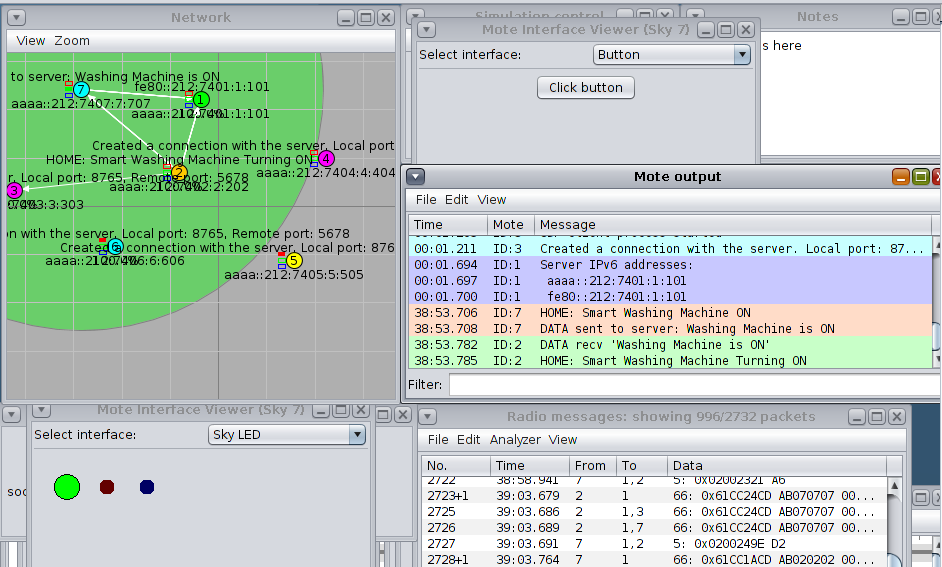


Figure 3‑31. Smart Washing Machine Turning On

If we want to turn off the washing machine, it is also done by clicking the button once more. Once turned off, Red LED turns on, while Green LED turns off. Sky Mote 7 displays the message, ‘HOME: Smart Washing Machine OFF’. The server replies with ‘HOME: Smart Washing Machine Turning OFF.’

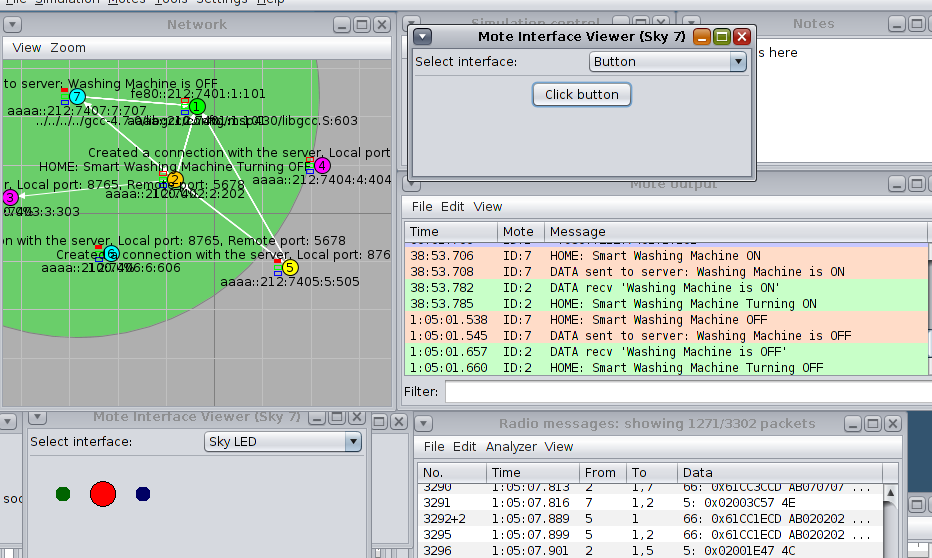


Figure 3‑32. Smart Washing Machine Turning Off

# SECURITY ISSUES OF PROPOSED APPLICATION AND SYSTEM

## Introduction of Threads Modelling Techniques

Threat modelling is a technique in identifying potential threats or risks in a network security and the vulnerabilities that could possibly be imposed by the identified threats or risks.

Threat modelling techniques consists of four steps which are, identifying assets, identifying threats, analysing vulnerabilities and creating countermeasures or mitigation techniques to block the identified threats

## System Architecture

The dashed red lines of Figure 4-1 are where an attacker could possibly impose risk in the smart home system

A person with a computer and a diagram of information

Description automatically generated with medium confidence

Figure 4‑1. System Architecture Threat Modelling

## Analysis Security Issues Using Threats Model

### Identifying Assets

In security analysis, asset is a valuable resource or component within a system that needs protection.



Table 4‑1. Identifying Assets

### Identifying Threats

In security analysis, threat are the potential risks that could impose vulnerabilities in a system causing damage.



Table 4‑2. Identifying Threats

### Analysing Vulnerabilities

In security analysis, vulnerabilities are the weakness or flaws in the system that can be exploited by threats causing damage.



Table 4‑3. Analysing Vulnerabilities

# SECURITY SOLUTIONS

In this section, the team considers these security solutions to mitigate the risk and threats of STRIDE.

## Spoofing

According to the research (*Anti-Spoofing for IoT — Antispoofing Wiki*, 2022), a few countermeasures to mitigate spoofing attacks:

**Encryption** – used to protect ingoing and outgoing traffic of  IoT devices. It minimizes the attackers to gain access to the devices. Advanced Encryption Standard (AES) is an example of encryption algorithm used to protect network layers.

**Anti-jamming** – this can mitigate the attack by switching its frequency to another channel. An inference framework can be used to detect the source of disturbance and take appropriate action to stop the attack.

**Authorization** – using the cryptographic “handshake” between smart gizmos via Bluetooth can prevent unauthorized device access. Also, using authentication and access control can ensure strong gadget-level verification.

**Voice anti-spoofing** – acceleration method is commonly used to detect the vibration of skin of user to help filter out a synthetic vocal request. Another method is two-factor authentication where it implies monitoring the movement of the lips by speaker thru Channel State Information (CSI), which is based on device-free sensing method.

## Tampering

The research ‘*Learn How to Secure Your IoT Devices from Unauthorized Access, Modification, or Destruction with These Six Strategies and Best Practices, (2024)’* indicates the following strategies that can prevent the IoT devices from tampering and protect data and assets.

**Location** – IoT devices must be in a secured place to avoid physical tampering. Also, must not be exposed to environmental hazards. Regular monitoring and checking the location of devices to see if there are any signs of tampering, such as loose wire or missing parts.

**Tamper resistant and detection** – having a tamper resistant and detection to the IoT device can resist hardware and software attacks. Examples are metal enclosures, security screws, and software that can check the device identity or device performance that can lockdown the device if tampering happens.

**Physical security policies** – are rules and procedures to use and maintain the device and network components. For instance, applying authorization and verification for the user to access the device, also define roles and responsibilities of the user.

**Update and Audit** – the user should update its device regularly to have better security and protection. Furthermore, should audit to review and analyze the device to identify and resolve any issues that may occur.

**Train users** – users need to be trained to understand the importance of IoT security and privacy since users are often the weakest link in the security chain. They must know how to properly use the devices, therefore, regular training and giving clear and updated guidelines can help them.

* 1. **Repudiation**

**Audits** – Reviewing and analyzing the logs obtained from the devices serve as a detective tool. With this, preventive measures can be created to be prepared for incoming threats.

**Non-repudiation** – use of digital signatures, cryptography algorithms, and any other authentication methods that can provide proof of its legitimacy can mitigate the risk of unauthorized access or threats.

## Information Disclosure

**Data Encryption** - Implement end-to-end encryption to protect the communication between the devices and the application. This will protect confidential information from unauthorized access.

**Data Minimization**- limiting the gathering of information to important details can reduce the risk of exposure in case of breach. Only the information between the application and devices are necessary, in short, avoid personal information since it is not related to the functionality of the device and application.

## Denial of Service

According to the research (*What Is a Denial of Service (DoS) Attack?* 2015), here are few countermeasures to prevent and mitigate DoS attack:

**Traffic filtering and Rate limiting** – implementing traffic filtering and rate limiting can prevent incoming requests to overload the server and distinguish malicious traffic and legitimate traffic. This helps the users to mitigate potential DoS attacks and maintain access while blocking harmful traffic.

**Intrusion Detection System  -**  to detect network traffic and find security issues.

**Intrusion Prevention System**  – finds intrusions and takes action to stop the threats that were found.

**Incident response and Recovery plans** – developing an incident response and recovery plan that include data backups and system redundancies can minimize the downtime and protect assets despite persistent DoS attacks.

## Elevation of Privilege

**Role-Based Access Control (RBAC)** – identify and assign appropriate permissions to the user roles such as admin, resident, and guest. This is important for the user roles since the needs and responsibilities evolve. Furthermore, verification of the identity through biometrics or any verification process enhances security.

**Least Privilege Principle** – assigning user roles to control the devices can limit the access based on their roles. This approach can restrict the users to change something on the devices and only allows users to make necessary changes.

# CONCLUSION

This paper demonstrated how Smart Home Appliances work. The design of system architecture help defines the structure of the network within the smart home. The system architecture is divided into four layers which are the sensing layer, network layer, platform layer and application layer. In the simulation, only three of the four layers are simulated as the application layer is already assumed to be the mobile application of the smart home. The simulation showed how the smart devices interact within one another and every transaction is received by the server and it is reported in the router. The router saved the packets from the transactions and is directly send in the application layer. The smart devices are controlled using the button and LEDs are used to indicate whether a smart device is currently turned on or off.

The security issues are easily defined in the system architecture. The utilization of threat modelling allowed the group to determine which type of security issues the system is and will face on. STRIDE is used to identify which type of threats exist in the system. The assets used in the system are a viable source of threats that needs updated protection.

After identifying the security issues, the security solutions are defined to mitigate and reduce the risk of STRIDE. The solutions provided indicates how the problem is directly addressed. The solution mostly declares authorization, encryption, IDS and IPS to tackle the threats.

# REFERENCES

*Anti-Spoofing for IoT — Antispoofing Wiki*. (2022, February 18). Antispoofing Wiki. https://antispoofing.org/anti-spoofing-for-iot/

Bashir, M. & Gill, S.S., 2016. IoT enabled smart appliances: An empirical study. Journal of Electrical and Computer Engineering, [online] Available at: https://www.hindawi.com/journals/jece/2016/1234567/ [Accessed 22 July 2024].

Darianian, M. & Michael, M.P., 2008. Smart home mobile RFID-based Internet-of-Things systems and services. International Journal of Computer Applications in Technology, 31(1), pp.94-108.

Gungor, V.C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C. & Hancke, G.P., 2013. Smart grid technologies: Communication technologies and standards. IEEE Transactions on Industrial Informatics, 7(4), pp.529-539.

Learn how to secure your IoT devices from unauthorized access, modification, or destruction with these six strategies and best practices. (2024, February 8). Linkedin.com. https://www.linkedin.com/advice/3/how-can-you-prevent-physical-tampering-your-iot-9tm3c#:~:text=Show%20translation-

Ne3 Simulations (2021). *Contiki Cooja Simulator : Specially Designed Wireless Sensor Networks*. [online] Ns3 Projects. Available at: https://ns3simulation.com/contiki-cooja-simulator/ [Accessed 15 Sep. 2024].

Network Simulation Tools (2021). *Cooja Simulation Tutorials | What is Contiki OS and Cooja simulation*. [online] Network Simulation Tools. Available at: https://networksimulationtools.com/what-is-contiki-os-and-cooja-simulation/ [Accessed 15 Sep. 2024].

What Is a Denial of Service (DoS) Attack? (2015). Palo Alto Networks. https://www.paloaltonetworks.com.au/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=Rate%20Limiting%20and%20Traffic%20Filtering