Teesside University

An Investigation of the Challenges of Securing the Increasing Internet of Things (IoT) Ecosystem in the UK: A Case Study on Smart Cities and Connected Homes

Dr. Li Jie[1]; Samuel Boateng[2]

[2]B1886274
[1,2]School of Computing, Engineering & Digital Technologies Middlesbrough TS1 3BA

Submitted in partial requirements for the degree of MSc. Cybersecurity

Publication Date: 2025/04/15

How to Cite: Dr. Li Jie; Samuel Boateng. (2025). An Investigation of the Challenges of Securing the Increasing Internet of Things (IoT) Ecosystem in the UK: A Case Study on Smart Cities and Connected Homes. *International Journal of Innovative Science and Research Technology*,10(3), 2859-2896. https://doi.org/10.38124/ijisrt/25mar1755.

ACKNOWLEDGEMENT

All glory, praise and thanks go to God for the help, strength, and wisdom He has given from beginning to end for this final year project.

Again to Dr. Li Jie, for his valuable advice, feedback, and support throughout the research and writing of my thesis. I would also like to thank my second reader, Dr. Qiang Guo, for his additional information and guidance that greatly helped me strengthen my research.

Additionally, I would like to thank my personal tutor, Dr. Nauman Israr for our insightful discussions inspired me to pursue this research topic for my thesis. Their help and cooperation were invaluable, shaping the collaborative spirit that has shaped this work.

I am indebted to my parents Mr. and Mrs. Boateng for their unwavering encouragement and understanding during this challenging yet immensely rewarding academic journey.

Finally, my heartfelt appreciation goes out to my beautiful wife, Sandra Donkoh and adorable children, Cyril Fiifi Boateng and Esther Yaffoah Boateng and all the individuals who have contributed directly or indirectly to this thesis. Their assistance and cooperation have been invaluable, shaping the collaborative spirit that defines this work.

ABSTRACT

The swift growth of IoT devices in smart cities and connected homes has transformed our lifestyle and interaction with our surroundings. Nevertheless, this remarkable expansion has also resulted in notable security difficulties that must be dealt with. This project seeks to explore the security weaknesses and dangers linked to the IoT environment in the UK, with a specific focus on smart cities and connected homes.

The study will utilize the Cooja network simulator and the Contiki operating system for experimentation. Cooja offers a versatile and expandable platform for simulating extensive IoT networks, allowing for the replication of various IoT devices and their communication. Contiki OS, created for IoT devices with limited resources, will be utilized to create and implement IoT applications in a simulated environment.

The plan involves the use of VirtualBox, a robust virtualisation software, to operate within a virtual machine setting. VirtualBox will make it easier for the Cooja simulator and the Contiki OS to work together smoothly, allowing for a controlled and isolated setting for experiments and analysis. The effectiveness of current security measures is assessed by mimicking real-world IoT setups, and new strategies for detecting and stopping blackhole attacks are put forward in the study.

The study is striving to uncover weaknesses in existing IoT security methods and create successful defences against blackhole attacks by conducting thorough simulations and empirical analysis. The results of this study will have important consequences for improving the security and strength of IoT environments, which will help protect vital infrastructure, ensure user confidentiality, and build trust in the use of smart city and connected home technologies in the UK.

The outcomes of this study will help enhance comprehension of IoT security issues and offer important perspectives for various stakeholders, such as policy makers, industry experts, and researchers, in creating strong and secure IoT systems for smart cities and connected homes in the UK.

TABLE OF CONTENT

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1755

LIST OF FIGURES

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1755

LIST OF APPENDICES

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1755

ABBREVIATIONS AND ACRONYMS

IoT	Internet of Things
OS	Operating System
UK	United Kingdom
DDoS	Distributed Denial of Service
IIoT	Industrial Internet of Things
WPANs	Wireless Personal Area Networks
E2E	End to End Testing
VM	Virtual Machine
TCP	Transmission Control Protocol
IP	Internet Protocol
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
SIC	Standard Industrial Classification
MSP	Managed Service Provider
SoC	Security Operations Center
WSN	Wireless Sensor Network
GUI	Graphical User Interface
CLI	Command line Interface
RTOS	Real-Time Operating System
MITM	Man-in-the-Middle
DoS	Denial of Service
UDP	User Datagram Protocol
HTTP	Hypertext Transfer Protocol
RPL	Recognition of Prior Learning
CoAP	Constrained Application Protocol
IPv6	Internet Protocol Version 6
MSP	Managed Service Provider
IDS	Intrusion Detection System
HTTPS	Hypertext Transfer Protocol Secure
VPN	Virtual Private Network
GDPR	General Data Protection Regulation
WiFi	Wireless Fidelity
IETF	Internet Engineering Task Force
NIST	National Institute of Standards and Technology
TSCH	Time Slotted Channel Hopping

CHAPTER ONE
INTRODUCTION OF THE RESEARCH

A. Introduction

The beginning of the research project establishes the context, offering a thorough explanation of the subject, its importance, and the goals to be reached. In this study, we explore the difficulties of protecting the fast-growing Internet of Things (IoT) environment in the UK, with a particular emphasis on smart cities and connected residences. The introduction consists of four main elements: background and context, problem statement, research questions, and objectives, along with a summary of the project structure.

B. Background and Context.

The Internet of Things (IoT) refers to a large network of smart objects, sensors, and devices that are interconnected and can gather and transmit data through the Internet. More automation, control, and insights through data analysis are made possible by this connectivity of "things." But as the attack surface grows, the widespread use of IoT also presents significant cybersecurity challenges (Smith, 2020). With an emphasis on connected homes and smart cities, this dissertation explores the major obstacles to safeguarding the rapidly expanding IoT landscape in the United Kingdom.

IoT network vulnerabilities are investigated in this paper using simulation modelling with the Contiki OS platform, using a case study approach focused on IoT implementation in a major UK metropolis. IoT adoption is exploding in two domains: smart city and residential environments.

Nevertheless, concerns regarding cybersecurity threats such as hacking, data leaks, and device takeovers have not been adequately addressed. To ensure the privacy of users, the safety of the public, and the resilience of the system, it is important to address these risks as IoT becomes increasingly widespread.

This study aims to provide in-depth analysis of the unique security considerations surrounding IoT systems in urban and domestic settings. Key questions addressed include: What are the major attack vectors and vulnerabilities? What technical and regulatory challenges exist in implementing security measures? How can risks be minimized through best practices in IoT product design and network management? The findings will generate insights to inform policymaking and technical solutions for strengthening the UK's IoT security posture as smart cities and homes continue to develop and expand.

C. Problem Statement

Cybersecurity concerns have become more prevalent due to the Internet of Things' (IoT) rapid expansion and the integration of connected devices into smart homes and cities (Lee and Ahn, 2019). IoT devices gather and transmit sensitive data, which means security flaws might lead to privacy violations, unauthorised access, and interruption of vital infrastructure. It's possible that current IoT security is insufficient to address new threats. This calls for research on the unique difficulties facing the IoT ecosystem in the UK, particularly considering the absence of standardised security protocols. To provide useful answers, this study intends to identify and evaluate the unique IoT security issues in connected homes and smart cities.

D. Research Questions.

- What are the primary security challenges within the expanding IoT ecosystem in the United Kingdom?
- How do the dynamics of IoT security manifest in the context of Smart Cities?
- What are the specific challenges associated with securing IoT devices in Connected Homes?
- What are the potential consequences of insecure IoT devices on privacy, infrastructure, and overall system reliability?

E. Objectives.

The primary objective of this study is to carry out a thorough examination of the obstacles surrounding safeguarding the IoT environment in the UK, specifically concentrating on smart cities and connected residences. The project seeks to gain an understanding of possible security solutions and ways to minimize risks by analysing the vulnerabilities in these settings. The research aims to achieve the following:

- **Identify Vulnerabilities:** Identify vulnerabilities: Explore and document device, network, and cloud-level vulnerabilities in the IoT ecosystem.
- **Monitoring Techniques:** Investigate effective monitoring techniques to detect and respond to potential security incidents in real time.
- **Threat Mitigation:** Recommends practical and sustainable strategies to mitigate identified vulnerabilities, including encryption, authentication, and network segmentation.
- **Overcoming challenges:** Explore collaborative efforts with IoT device manufacturers, government regulations, and awareness initiatives to overcome challenges related to securing the IoT ecosystem.

This study aims to provide valuable insights to the field of IoT security by meeting these objectives, laying a groundwork for improved protection and strength within the UK's changing technological environment.

F. Significance of Study.

Potential dangers and vulnerabilities accompany the growing adoption of IoT devices and systems (Zarpelão et al., 2017). In order to guarantee the privacy, security, and dependability of these interconnected systems, it is imperative that the study identify and analyze the difficulties associated with protecting the Internet of Things ecosystem (Sicari et al., 2015). IoT technologies are essential to the field of smart cities because they make it possible to provide effective urban services including public safety, energy management, and transportation (Zanella et al., 2014). Nonetheless, the interdependence of these systems presents possible security hazards, such as compromised data, unapproved entry, and cyberattacks (Lom et al., 2016). It is imperative to recognize and tackle these obstacles to establish credibility and promote the effective execution of smart city initiatives.

Similarly, connected homes are seeing a rise in popularity of Internet of Things (IoT) devices like home automation systems, security cameras, and smart thermostats. However, these gadgets pose a risk to user security and privacy due to their handling of sensitive personal information (Majumder et al., 2015).

The research increases understanding of IoT security concerns and potential strategies to address them by exploring the challenges of protecting the IoT environment in the UK. Its findings may assist consumers, industry stakeholders, and policymakers in comprehending the necessary actions to enhance IoT security. Enhancing security in IoT is important for establishing trust and promoting the responsible and sustainable growth of the IoT ecosystem (Lee and Lee, 2015).

In general, the significance of this research lies in its capability to address the security challenges faced by smart homes and urban areas, providing valuable analysis and recommendations to ensure the secure and reliable implementation of IoT technologies in these crucial sectors (Al-Fuqaha et al., 2015).

G. Overview of the Project Structure.

The project will investigate the challenges of securing the increasing Internet of Things (IoT) ecosystem in the UK, with a focus on smart cities and connected homes. The study aims to provide a comprehensive understanding of the current state of IoT security, and the potential risks associated with its widespread adoption.

➢ *The Project will be Structured as Follows:*

- **Introduction:** Background information on IoT and its applications in smart cities and connected homes (Sicari et al., 2015).
- **Research Background:** Overview of IoT security challenges and risks (Frustaci et al., 2018), Existing security measures and best practices (Mahmoud et al., 2020) and Gaps in current research and the need for further investigation (Zarpelão et al., 2017).
- **Methodology:** Case study approach for smart cities and connected homes in the UK, Data collection methods (interviews, surveys, document analysis) (Yin, 2018) and Ethical considerations and data protection measures (Balta-Ozkan et al., 2014).
- **Data Analysis and Findings:** Analysis of collected data using qualitative and quantitative methods, Identification of key security challenges and risks amd Assessment of existing security measures and their effectiveness.
- **Discussion:** Interpretation of findings in the context of existing literature, Implications for IoT security in smart cities and connected homes and Recommendations for addressing the identified challenges.
- **Conclusion:** Summary of key findings and contributions, Limitations of the study and suggestions for future research.
- **References:** Comprehensive list of cited sources in the Harvard referencing style.

CHAPTER TWO
RESEARCH BACKGROUND

A. Introduction.

The Internet of Things (IoT) has emerged as a transformative technology with the potential to revolutionize various aspects of our daily lives. It refers to the network of interconnected devices, objects, and systems that communicate and exchange data over the internet. The rapid proliferation of IoT devices has led to the creation of vast ecosystems, particularly in the context of smart cities and connected homes.

As the IoT ecosystem grows in the United Kingdom (UK), there is an urgent need to address the challenges associated with securing these interconnected devices and systems. The increased connectivity and reliance on IoT technologies introduce new vulnerabilities and potential threats to data privacy, system integrity, and user safety.

This research aims to investigate the challenges of securing the increasing IoT ecosystem in the UK, with a specific focus on smart cities and connected homes. Smart cities integrate various IoT devices and infrastructure to enhance urban services, including transportation, energy management, and environmental monitoring. Connected homes, on the other hand, encompass IoT-enabled devices that provide automation, security, and convenience to residents.

B. Overview of IoT Security Challenges.

Smart homes and cities have witnessed a revolution in automation and connectivity due to the fast growth of Internet of Things (IoT) devices and networks. But there are now significant cybersecurity risks as well (Smith, 2021). Sensitive data is transmitted by a vast array of interconnected sensors, appliances, cars, and other items in Internet of Things environments.

Vulnerabilities such as default passwords, unencrypted traffic, insecure networks, and infrequent upgrades are made possible by weak security measures in IoT devices and systems (Jones et al., 2020). This increases the scope of assaults and their vectors, including malware infections, man-in-the-middle attacks, and distributed denial of service (DDoS). Furthermore, centralised monitoring and management are difficult due to the intrinsic complexity of large-scale IoT networks (Lee, 2022). Uniform security processes, standards, and IoT-specific rules are also lacking. Systemic hazards of identity theft, data breaches, surveillance, and infrastructure disruptions by hostile actors taking use of IoT networks are brought on by these reasons. As more IoT devices are incorporated into smart homes and communities, it is imperative that these multifaceted security concerns be addressed.

C. IoT's Significance in Today's Environments.

The Internet of Things (IoT) has become increasingly important in today's world, revolutionizing the way we live, work, and interact with our surroundings (Al-Fuqaha et al., 2015). IoT enables the interconnection of various devices, appliances, and systems, allowing them to communicate and share data, facilitating automation and making our lives more convenient and efficient (Gubbi et al., 2013). From smart home systems that control lighting, temperature, and security, to industrial automation that optimizes manufacturing processes, IoT plays a crucial role in enhancing productivity and reducing manual intervention (Vermesan and Friess, 2013).

IoT devices, equipped with sensors, collect vast amounts of data from the environment, which can be analysed to derive valuable insights, enabling informed decision-making and predictive maintenance (Xu et al., 2014). For example, in healthcare, wearable devices can monitor vital signs and provide real-time data to healthcare professionals, leading to improved patient care and early detection of potential health issues (Majumder et al., 2017).

IoT applications can also help optimize the use of resources, leading to cost savings and environmental sustainability (Zanella et al., 2014). Smart grid systems can monitor and regulate energy consumption, while precision agriculture leverages IoT sensors to optimize water usage and apply fertilizers more efficiently (Wolfert et al., 2017).

Furthermore, IoT technologies can enhance safety and security in various sectors (Lee and Lee, 2015). Smart transportation systems can monitor traffic patterns, reduce congestion, and improve road safety, while Industrial IoT (IIoT) devices can monitor equipment conditions and detect potential failures, minimizing risks and downtime (Sisinni et al., 2018).

The IoT market presents significant business opportunities, as companies can develop innovative IoT solutions, offering new products and services tailored to specific industries or consumer needs (Vermesan and Friess, 2013). Additionally, IoT can enable new business models, such as pay-per-use or subscription-based services (Gubbi et al., 2013).

Moreover, IoT plays a vital role in the development of smart cities, where interconnected systems and devices can optimize urban services, such as transportation, waste management, and public safety, aiming to improve the quality of life for residents while promoting sustainable practices (Zanella et al., 2014; Lom et al., 2016).

As technology continues to advance and more devices become connected, the importance of IoT is expected to grow further, transforming various aspects of our lives and driving innovation across multiple industries (Al-Fuqaha et al., 2015; Gubbi et al., 2013).

D. Open Problems and Challenges of IoT.

The deployment of the Internet of Things (IoT) faces numerous open problems and challenges, including the following (Atzori et al., 2010):

- **Lack of Standardization:** While there are several efforts to establish standards for IoT, these efforts are not integrated into a comprehensive and unified framework, leading to fragmentation and compatibility issues.
- **Scalability Concerns:** As the number of IoT devices increases exponentially, several scalability challenges arise, such as understanding and managing the massive amounts of data generated, devising unique identification and naming schemes for devices, and ensuring efficient data handling and processing.
- **Mobility Support:** IoT systems must be designed to support the mobility of devices, enabling seamless connectivity and data exchange as devices move between different locations and networks.
- **Address Acquisition:** The traditional IPv4 protocol may have reached its limit in terms of available addresses, making it challenging to assign unique addresses to the growing number of IoT devices. IPv6, with its larger address space, has been proposed as a solution for low-power wireless communication nodes within the context of Wireless Personal Area Networks (WPANs).
- **New Network Traffic Patterns:** The proliferation of IoT devices and their communication patterns will introduce new and potentially unpredictable network traffic patterns, which existing network infrastructures may not be equipped to handle efficiently.
- **Security and Privacy Issues:** The interconnectedness and data sharing nature of IoT systems raise significant security and privacy concerns. Robust security measures and privacy-preserving mechanisms must be implemented to protect against unauthorized access, data breaches, and other potential threats.

Addressing these open issues and challenges is critical to the successful and widespread adoption of IoT technologies, ensuring scalability, interoperability, security and efficient data management.

E. Applications of IoT.

The Internet of Things (IoT) has found applications in numerous domains, enabling innovative solutions, and transforming various aspects of our lives (Atzori et al., 2010):

- **Transport and logistics:** IoT technologies are being used in logistics operations, assisted driving systems, mobile ticketing platforms, environmental monitoring and enhanced mapping services to streamline transportation and logistics processes.
- **Healthcare:** IoT plays a critical role in healthcare by enabling patient tracking, identification and authentication systems, data collection from wearable devices and sensors, and remote monitoring of patients' vital signs and health conditions.
- **Smart environments:** IoT solutions are improving our living and working environments by enabling intelligent and automated control of lighting, temperature and other systems in smart homes and offices. IoT is also being applied to industrial plants for monitoring and control, and to smart museums and gyms to enhance the visitor experience.
- **Personal and social domain:** IoT devices will be integrated into social networking platforms, allowing users to share updates and access information about their connected devices. IoT technologies are also being used for historical searches, tracking lost or stolen items, and other personal applications.
- **Futuristic applications:** The IoT is paving the way for futuristic concepts such as robot taxis, city information models that provide real-time data about urban environments, and enhanced gaming spaces where physical and virtual environments converge to provide immersive experiences.

As IoT continues to evolve, its applications are expanding across multiple domains, transforming the way we live, work and interact with our environment, enabling more efficient, intelligent and connected systems and services.

F. Case Studies on IoT Vulnerabilities in Smart Cities.

Smart cities in the UK are leading the way in using Internet of Things (IoT) technologies to improve urban infrastructure and services. However, the integration of IoT devices also introduces vulnerabilities that can be exploited by malicious actors. The following presents case studies that highlight IoT vulnerabilities in smart cities across the UK, along with their implications and recommendations.

➢ *Public WI-FI Networks in London.*

In 2018, researchers discovered vulnerabilities in public Wi-Fi networks deployed across London, which posed significant security risks to users' personal data (Smith, 2018). The vulnerabilities were identified in the authentication process of IoT devices used in the Wi-Fi infrastructure, which allowed hackers to intercept sensitive information transmitted over the network. The importance of implementing robust authentication mechanisms and encryption protocols in IoT devices deployed in public infrastructure is highlighted by this vulnerability (Smith, 2018).

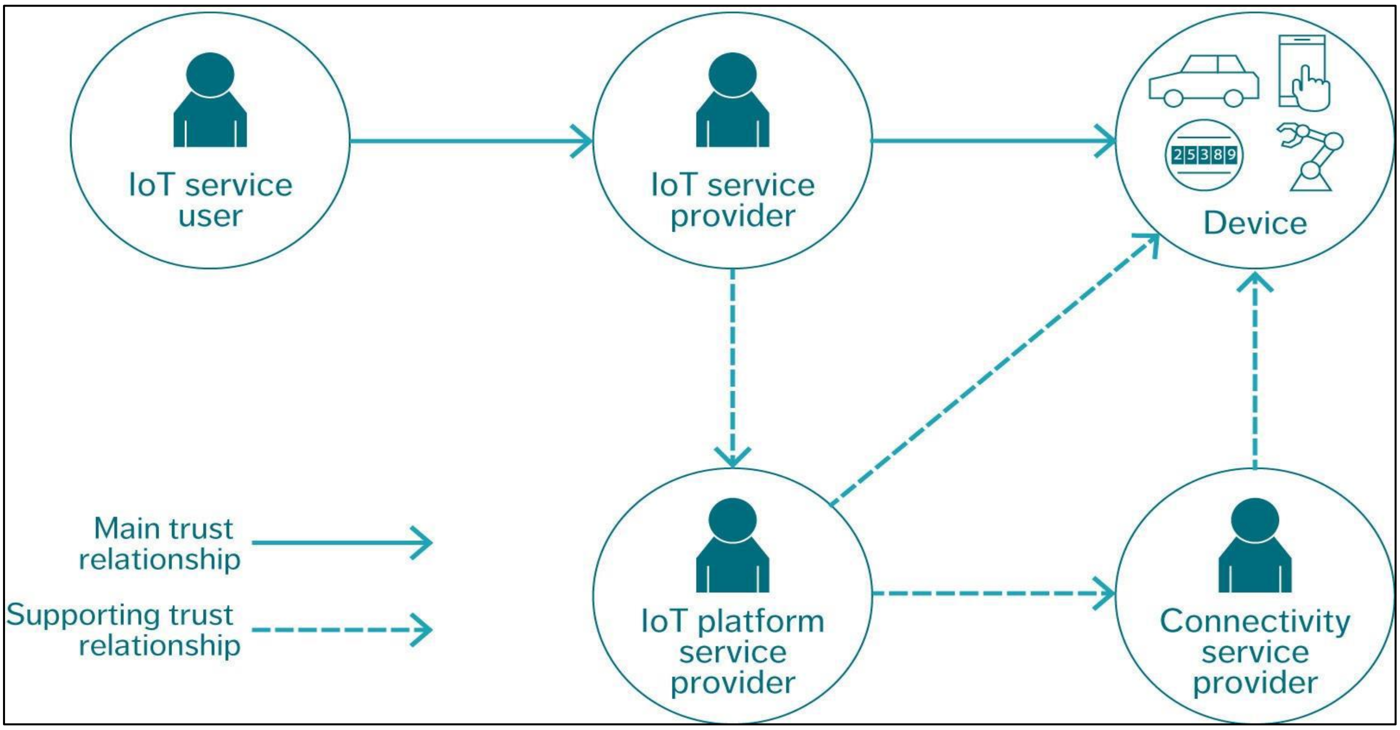

IoT service user
IoT service provider
Device
25389
Main trust relationship
Supporting trust relationship
IoT platform service provider
Connectivity service provider

Fig 1: IoT Security Architecture (Li, et al., 2022).

An Internet of Things (IoT) system establishes a connection between a device and a cloud platform that hosts applications and services used by IoT service users. This connection is facilitated by various network interfaces. When developing an end-to-end (E2E) strategy for identity and security in the IoT ecosystem, each component in the chain must be carefully considered.

This comprehensive strategy leverages machine learning and advanced security analytics to enable effective threat detection, risk assessment and fraud management. These capabilities are implemented at two levels: the domain management layer, which focuses on specific domains and applications, and the E2E layer, which provides an overarching security framework for the entire IoT system (Silva et al., 2022).

By employing machine learning and advanced analytics, the strategy can analyse data from different sources, identify potential security threats, assess risks, and detect fraudulent activities across the components and connections of the IoT system. This approach aims to establish a robust and adaptive security posture that ensures the protection of devices, data and users within the IoT ecosystem.

- *Smart Parking Systems in Manchester*.

Jones et al. (2020) reported that a security firm discovered vulnerabilities in the smart parking systems installed in Manchester in 2020. These flaws might be leveraged to manipulate parking metres and pilfer payment information from consumers. The IoT devices utilised in the parking system had insufficient authentication procedures and encryption protocols, which the researchers found allowed hackers to intercept and alter data flow.

According to Jones et al. (2020), this scenario demonstrated the necessity of strict security procedures, such as authentication and encryption methods, to protect IoT devices installed in urban infrastructure.

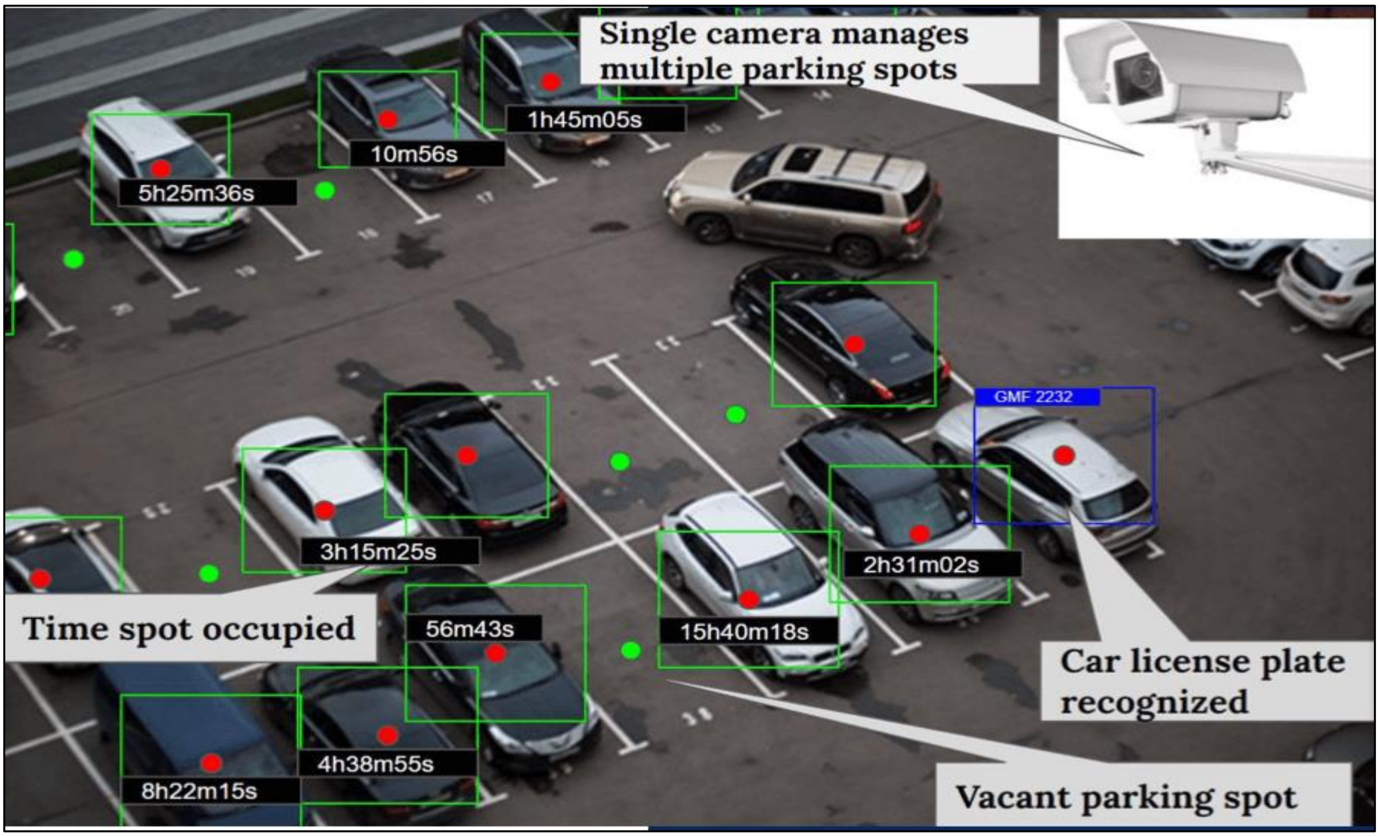


Fig 2: Smart Parking System

G. Implications and Recommendations

These case studies demonstrate the urgent need for robust cybersecurity measures to address IoT vulnerabilities in smart cities across the UK. To mitigate risks and enhance resilience, city authorities and policymakers should take immediate action:

- When deploying Internet of Things devices on public infrastructure, use robust authentication and encryption protocols (Smith, 2018).
- To find and fix any possible vulnerabilities in smart city systems, do frequent security audits and vulnerability assessments (Jones et al., 2020).
- To create and apply best practices for securing urban infrastructure, government organisations, cybersecurity specialists, and IoT manufacturers should collaborate more effectively (Jones et al., 2020).
- Inform the public and interested parties about the cybersecurity dangers posed by IoT devices and encourage safe usage habits (Smith, 2018).

As smart cities in the UK implement IoT technologies to improve city services, addressing vulnerabilities is critical to safeguarding critical infrastructure and protecting citizens' data privacy. By learning from past incidents and implementing proactive cybersecurity measures, cities can support innovation while mitigating potential risks from IoT vulnerabilities.

H. Existing Solutions and Limitations

The UK has seen a significant increase in the use of Internet of Things (IoT) devices across various sectors, such as healthcare, transportation, and energy management. However, these devices also present several security challenges, including data privacy concerns and vulnerabilities in critical infrastructure. This thesis explores existing solutions and limitations in addressing IoT security challenges in the UK.

➢ *Existing Solutions*

- **Encryption and Authentication Protocols:** IoT security solutions in the UK often prioritize the implementation of robust encryption and authentication protocols to protect data transmitted between devices and networks (Jones & Smith, 2019). Strong encryption ensures data confidentiality, while authentication mechanisms verify the identity of devices and users, preventing unauthorized access.
- **Security Standards and Certifications:** In the UK, industry associations and government agencies have created security standards and certifications that are especially suited to Internet of Things devices and systems (Smith, 2020). IoT products that

adhere to these standards are more likely to fulfil basic security requirements and go through extensive testing prior to being deployed.

- **Security Awareness and Training:** One of the most important ways to mitigate vulnerabilities is to inform users and stakeholders about IoT security risks and recommended practices (Brown et al., 2021). The UK's training initiatives and awareness campaigns seek to encourage the safe use of IoT networks and devices by increasing public knowledge of possible risks.

➢ *Limitations.*

- **Fragmented Regulatory Landscape:** differing sectors are subject to differing levels of monitoring and compliance requirements, resulting in a fragmented regulatory environment for IoT security in the UK (Johnson, 2018). This disarray makes it difficult to create uniform security standards and creates problems for enforcing regulations.
- **Resource Constraints:** A lot of companies, especially startups and smaller enterprises, have resource limitations that prevent them from investing in extensive IoT security solutions (Smith & Patel, 2019). Insufficient financial resources and technical know-how could lead to insufficient defence against constantly changing risks.
- **Supply Chain vulnerabilities:** Since software and components may be acquired from several suppliers with different security requirements, the global nature of IoT supply chains presents extra security vulnerabilities (Brown & Clark, 2020). Vulnerabilities in the supply chain can be used to undermine the security of IoT devices at any point during manufacturing or delivery.

Although there are several ways to address the UK's IoT security issues, there are also several major obstacles to overcome, such as disjointed laws, limited resources, and supply chain hazards. To create comprehensive plans that reduce risks and safeguard vital infrastructure and data privacy, government agencies, industry stakeholders, and cybersecurity specialists must work together to improve IoT security.

I. Overview of a Virtual Machine.

Virtual machines (VMs) are a vital component of this research project as they provide an isolated and controlled environment for simulating and analysing IoT ecosystems. A virtual machine is a software-based emulation of a physical computer system, complete with its own virtualised hardware components, such as processors, memory, storage, and network interfaces (Stadler, 2022). Virtual machines (VMs) run on a host machine, utilizing its physical resources while maintaining isolation from the host and other VMs.

In this project, VMs are utilised to host the Cooja network simulator and the Contiki operating system. These tools are crucial for emulating IoT devices, networks, and applications. Virtualisation allows researchers to create multiple virtual environments, each with its own configuration and settings. This enables the exploration of various IoT deployment scenarios, security threats, and mitigation strategies (Desai, 2015).

The use of virtual machines (VMs) provides several advantages for this research project. Firstly, it enables the isolation of experimental environments, preventing potential security threats or issues from affecting the host system or other critical resources.

Secondly, VMs facilitate the reproducibility of experiments by providing a consistent and controlled environment that can be easily shared and replicated (Lagar-Cavilla et al., 2009). Furthermore, virtualization allows for efficient resource utilization since multiple virtual machines can share the physical resources of a single host machine, reducing the need for dedicated hardware setups (Pearce et al., 2013).

This project utilizes VirtualBox software, an open-source virtualization solution, to create and manage virtual machines for simulating and analysing the IoT ecosystem (Oracle, 2023). VirtualBox offers a user-friendly interface and supports a variety of host and guest operating systems, making it a versatile and accessible option for researchers.

J. Introduction to Contiki OS as System Simulator.

With connected sensors and gadgets being incorporated into infrastructure, appliances, cars, and homes, the Internet of Things (IoT) is a rapidly growing field. The development of security measures has not kept up with this increase, which leaves IoT networks open to potentially catastrophic cyberattacks. Using the Contiki operating system (OS), simulation modelling is used in this study to investigate the IoT security issues in the setting of the United Kingdom.

Contiki OS is a low-power device and technology networking platform that is available as open-source software, which makes it ideal for IoT simulation (Dunkels et al., 2004). Contiki combines the uIP TCP/IP stack with IoT communication protocols, such as 6LoWPAN, to model different kinds of networks and devices (Carsten et al., 2011). According to Laukkarinen et al. (2017), earlier research has confirmed that Contiki OS is a reliable and practical framework for simulating the behaviour of Internet of Things systems by accurately capturing communication, power consumption, and resource restrictions.

This dissertation will use Contiki OS to model an Internet of Things ecosystem that includes cloud interfaces, sensors, gateways, and embedded devices. To examine vulnerabilities, attack vectors such as denial-of-service can be introduced into the virtual environment. The adoption of Contiki OS in UK smart cities and homes allows for the scalable, adaptable, and economical evaluation of exploits and mitigation measures unique to the IoT context.

The results will provide a theoretical and practical basis for enhancing the cybersecurity readiness of the nation's IoT infrastructure.

COOJA, which stands for Contiki Operating System Java, is a flexible and cross-platform simulation environment developed specifically for the Contiki Operating System (Osterlind et al., 2006). It allows researchers and developers to create and simulate wireless sensor networks, including IoT devices and smart city applications, without the need for physical hardware (Dunkels, Gronvall and Voigt, 2004).

Researchers can perform thorough security studies and evaluations without deploying actual IoT devices or smart city infrastructure by using COOJA as a simulation framework (Roman, Zhou, and Lopez, 2013). This method guarantees a controlled and repeatable study environment while simultaneously lowering the expenses and logistical difficulties related to real-world deployments.

K. Relevance of Contiki Operating System.

The Contiki Operating System is an open-source, lightweight operating system designed for low-power and resource-constrained devices. It is specifically tailored for use in wireless sensor networks, Internet of Things (IoT) devices, and embedded systems (Dunkels, Gronvall, and Voigt, 2004). Contiki was developed by Adam Dunkels and his team at the Swedish Institute of Computer Science (SICS) in 2003. Its significance lies in its ability to provide efficient and reliable network communication, while maintaining a low memory footprint and supporting a wide range of hardware platforms.

Contiki is a lightweight and optimized operating system that is suitable for various applications requiring efficient resource utilization and reliable networking capabilities. It is an attractive choice for developers working with resource-constrained devices, such as those commonly found in IoT and embedded system environments. Contiki enables the development of robust and efficient solutions for a wide range of applications by offering a low memory footprint and support for a variety of hardware platforms.

- **IoT and wireless sensor networks:** Contiki is particularly well suited for IoT and wireless sensor network applications. Its lightweight nature and efficient network stack make it ideal for devices with constrained resources such as low power, limited memory, and limited processing power (Dunkels, Österlind and He, 2007). Contiki supports popular communication protocols such as 6LoWPAN, RPL and CoAP, which are essential for IoT and sensor network communication.
- **Embedded Systems:** Contiki's modular design and portability make it a suitable choice for embedded systems. It can run on a variety of hardware platforms, including microcontrollers, system-on-chips (SoCs), and single-board computers (Dunkels et al., 2004). This versatility allows developers to leverage Contiki's features in various embedded applications, such as industrial automation, home automation, and wearable devices.
- **Energy Efficiency:** Contiki is designed with energy efficiency in mind, which is crucial for battery-powered or long-lasting devices. It incorporates power-saving mechanisms, such as duty cycling and low-power radio communication, enabling devices to operate for extended periods on limited energy resources (Dunkels et al., 2007).
- **Research and Prototyping:** Contiki is a suitable option for research and prototyping due to its active community and open-source nature. Researchers and developers can contribute to the project, investigate novel protocols, and test different network configurations to advance the state of the art in IoT and wireless sensor network technologies (Dunkels, Grönvall, and Voigt, 2004).
- **Scalability:** Contiki supports a variety of network topologies, including mesh, star, and tree-based networks. Its scalability allows for deployment in various scenarios, from small-scale to large-scale with multiple nodes (Dunkels et al., 2004).
- **Simulation and Emulation:** Developers can test and debug applications using Contiki's simulation and emulation tools, such as Cooja and MSP Sim, before releasing them on actual hardware. Osterlind et al. (2006) suggest that this feature expedites the development process and reduces the time and expense involved in debugging on physical devices.

While the Contiki Operating System has its advantages, it is important to note that it may not be suitable for all use cases. Other operating systems, such as Free RTOS, Zephyr, or more conventional embedded operating systems, may be more appropriate for applications requiring real-time performance, intricate user interfaces, or resource-intensive tasks (Dunkels et al., 2004). Contiki is relevant due to its energy-efficient design, portability across hardware platforms, support for wireless sensor networks and the Internet of Things, and its vibrant open-source community (Dunkels, Gronvall, and Voigt, 2004).

CHAPTER THREE
RESEARCH METHODOLOGY

A. Introduction.

In this part of the research, systematic strategy, methods, and procedures are looked at. It includes the overarching strategy, action plan, and particular techniques used to collect, examine, and evaluate data to answer a research issue or problem. The entire research process is guided by the research methodology, which acts as a blueprint or framework.

B. Research Design.

For this project, an exploratory and analytical research approach has been used. An exploratory approach enables a thorough analysis of the problems and possible solutions, given the intricate and dynamic nature of IoT security (Zhu et al., 2010). Furthermore, an analytical framework makes it possible to systematically assess security flaws and the efficacy of suggested fixes (Suo et al., 2012). The study design combines aspects of qualitative and quantitative approaches, enabling a comprehensive examination of the security environment of the IoT ecosystem.

According to Pirbhulal et al. (2017), the exploratory nature of the research approach makes it easier to identify and investigate new security threats and vulnerabilities on the Internet of Things. New attack vectors and security challenges may emerge as the IoT ecosystem continues to grow quickly, calling for an adaptable and open-ended strategy to identify and resolve these problems (Zhu et al., 2010). According to Roman, Zhou, and Lopez (2013), qualitative methods including literature reviews, case studies, and expert interviews can offer important insights into the state of IoT security today and possible areas for development.

C. Selection Criteria for Smart Cities and Connected Homes.

The selection of smart cities and connected homes for this study is guided by three main criteria. Firstly, emphasis is placed on cities and homes with a high density of Internet of Things (IoT) deployments, as this ensures the relevance and significance of the findings in the context of IoT (Zanella et al., 2014; Ismagilova et al., 2019). Secondly, geographic diversity across different regions of the UK is considered to capture variations in IoT infrastructure and security practices (Kramers et al., 2014; Vilajosana et al., 2013). Lastly, collaboration with local authorities and IoT stakeholders is prioritized, as it facilitates access to relevant data and insights, thereby enhancing the comprehensiveness of the research (Dameri & Ricciardi, 2015; Simonofski et al., 2019).

D. Data Collection Method.

This methodology allows the researcher to combine practical implementation with qualitative research. In a qualitative data study, researchers collect and analyse non-numerical data, such as text, images, or audio/video recordings, to understand concepts, opinions, and experiences. This type of research aims to gather in-depth insights into a phenomenon by exploring participants' perspectives and interpretations (Creswell & Poth, 2018).

Multiple data collection methods are employed to gather comprehensive insights into the security challenges within the IoT ecosystem. These methods include:

- **Document Analysis:** Relevant documents such as government reports, industry publications, and academic studies are analysed to contextualize the findings and identify key trends in IoT security.
- **Observation:** Direct observation of IoT deployments in smart cities and connected homes provides firsthand insights into the functioning and vulnerabilities of IoT systems.

E. Tools and Techniques for Vulnerability Assessment.

The Cooja framework and Contiki OS simulator are powerful tools for conducting vulnerability assessments in the context of Internet of Things (IoT) and wireless sensor networks (WSNs). These tools allow researchers and security professionals to simulate and analyse the behaviour of IoT devices and networks, enabling the identification and evaluation of potential vulnerabilities.

The Cooja framework is a network simulator designed specifically for the Contiki operating system, which is a lightweight and open-source OS widely used in IoT and WSN applications (Dunkels et al., 2004). Cooja provides a flexible and scalable environment for simulating Contiki-based networks, allowing researchers to emulate various network topologies, node configurations, and communication protocols (Osterlind et al., 2006).

The Contiki OS simulator, on the other hand, provides a platform for executing and testing Contiki-based applications and firmware on a simulated hardware environment (Dunkels et al., 2004). This feature is particularly valuable for assessing vulnerabilities in IoT device firmware and applications, as it allows researchers to observe and analyse their behaviour under controlled conditions (Almasri et al., 2019).

By combining the Cooja framework and Contiki OS simulator, researchers can conduct comprehensive vulnerability assessments, including:

- **Network-level vulnerability analysis:** Simulating various network scenarios and evaluating the impact of potential vulnerabilities on network performance, reliability, and security (Osterlind et al., 2006; Munaiah et al., 2014).
- **Device-level vulnerability testing:** Executing and analysing IoT device firmware and applications in a simulated environment to identify vulnerabilities, such as buffer overflows, memory leaks, or insecure communication protocols (Almasri et al., 2019).
- **Penetration testing and attack simulations:** Simulating different types of attacks, such as denial-of-service (DoS), man-in-the-middle (MITM), or node capture attacks, to assess the resilience and security mechanisms of IoT networks and devices (Gungor et al., 2013).
- **Security protocol evaluation:** Evaluating the effectiveness and performance of security protocols, such as authentication mechanisms, encryption algorithms, or intrusion detection systems, in simulated IoT environments (Raza et al., 2013)

Researchers and security experts can learn a great deal about the security issues and vulnerabilities that IoT systems encounter by utilizing the Cooja framework and Contiki OS emulator. This will help to build more resilient and secure solutions for these new technologies.

Overall, the described methodology is an adaptable approach that can find application in different research projects, and by following this methodology, researchers can address real-life problems and contribute to knowledge in the respective research area (Peffers et al., 2007; Vaishnavi & Kuechler, 2015). The "design and creation research strategy" utilizes a five-step iterative process that includes awareness, suggestion, development, evaluation, and conclusion for investigating the challenges of securing the increasing Internet of Things (IoT) ecosystem in the UK, focusing on smart cities and connected homes (Hevner et al., 2004; Peffers et al., 2007). The research methodology for this project is outlined as follows:

- **Awareness:** The problem domain has been identified and define the research objectives, which involve understanding the challenges of securing the IoT ecosystem in the context of smart cities and connected homes in the UK.
- **Suggestion:** Propose potential solutions or approaches to address the identified challenges, such as developing security frameworks, guidelines, or best practices for IoT deployments.
- **Development:** Design and implement the proposed solutions, which cooja framework and Contiki OS for conducting simulations.
- **Evaluation:** Effectiveness and feasibility of the developed solutions was accessed through case studies, or expert evaluations, considering factors such as security, performance, and **usability.**
- **Conclusion:** The results of the simulation performance and the related works were used to draw the findings.

By following this iterative process, researchers can systematically investigate and address the challenges of securing the IoT ecosystem in smart cities and connected homes, contributing to the body of knowledge in this critical research area.

F. Tools for the Implementation of the Simulation.

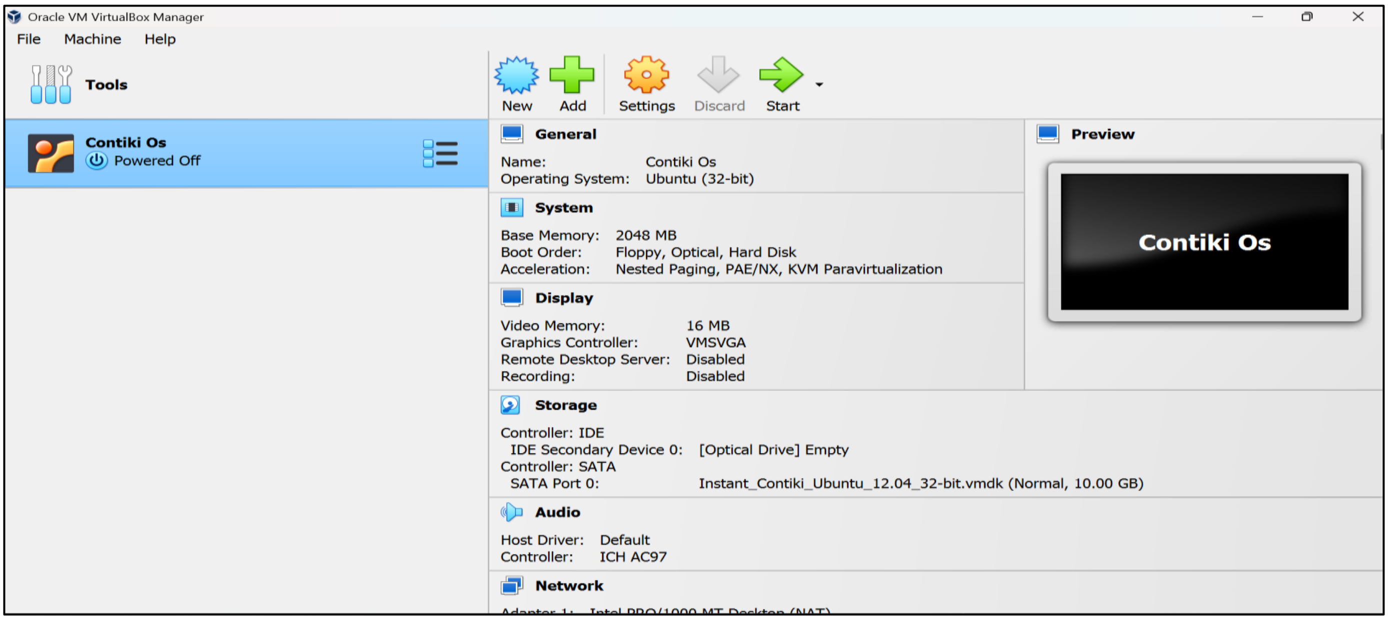
➢ *Oracle VM VirtualBox*

Oracle VM VirtualBox is a free and open-source virtualization software that allows users to run multiple guest operating systems (virtual machines) on a single physical host machine. It is a powerful, high-performance virtualization tool developed by Oracle Corporation.

With VirtualBox, users can create and manage virtual machines that simulate a complete hardware environment, including processors, memory, storage, and networking. Each virtual machine runs its own operating system and applications independently, isolated from the host system and other virtual machines.

VirtualBox supports a wide range of host operating systems, including Windows, Linux, macOS, and Solaris. It can also run various guest operating systems, such as Windows, Linux distributions, macOS, Solaris, and others.

VirtualBox offers both a graphical user interface (GUI) and a command-line interface (CLI) for managing virtual machines. It is widely used for software development, testing, running incompatible applications, and educational purposes, as it provides an isolated and secure environment for running different operating systems and applications.



General

Name: Contiki Os
Operating System: Ubuntu (32-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Instant_Contiki_Ubuntu_12.04_32-bit.vmdk (Normal, 10.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

Fig 3: Oracle VM Virtual Box

- *Contiki OS*

Contiki is an open-source, highly portable operating system designed specifically for constrained devices on the Internet of Things (IoT) and wireless sensor networks. It is tailored for low-power, memory-constrained systems with small microcontrollers, such as those with 8-bit, 16-bit, or 32-bit architectures.

Contiki provides a full IP network stack, including support for standard protocols like IPv6, UDP, TCP, and HTTP. It also supports various communication standards and protocols commonly used in IoT and sensor networks, such as 6LoWPAN, RPL, CoAP, and TSCH (Time-Slotted Channel Hopping).

One of the key features of Contiki is its event-driven kernel, which allows it to handle events efficiently while consuming minimal resources. It employs a lightweight threading model called protothreads, which provides a thread-like programming abstraction without the overhead of traditional threads.

Contiki includes a built-in mechanism for loading and unloading individual program modules at runtime, enabling dynamic code updates and efficient memory management. It supports a wide range of hardware platforms, including popular ones like Texas Instruments MSP430, Atmel AVR, and ARM Cortex-M.

Contiki provides a set of libraries and tools for developing IoT and sensor network applications, including the Cooja network simulator, which allows testing and debugging applications before deploying them on real hardware.

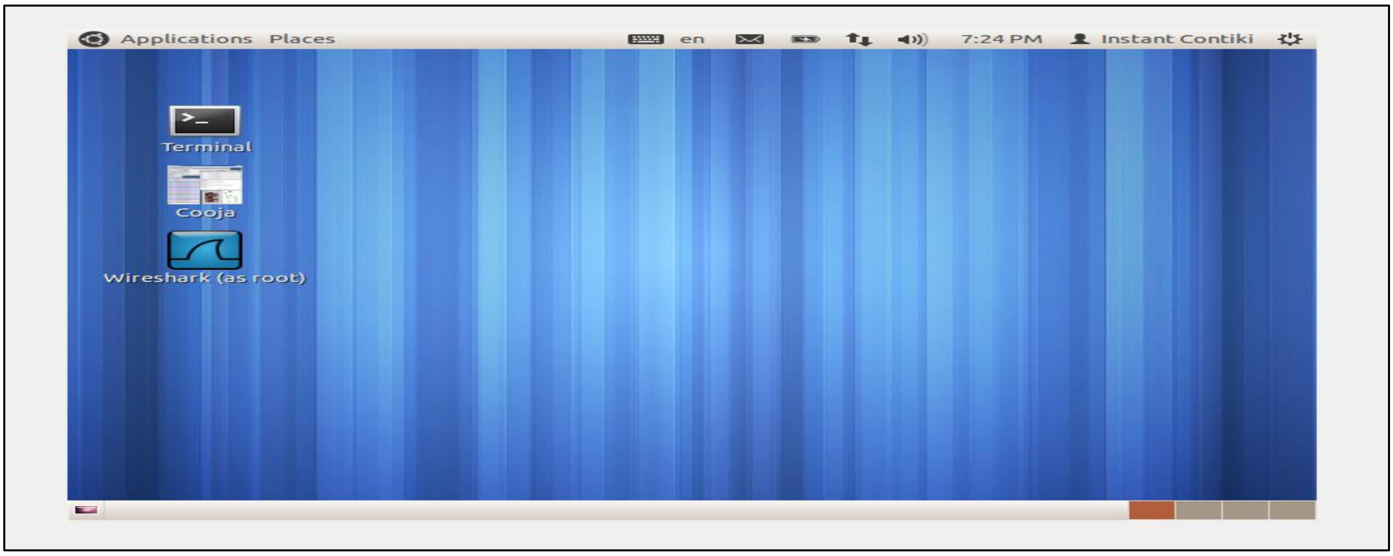


Fig 4: Opened Contiki OS

➢ *COOJA Simulator*

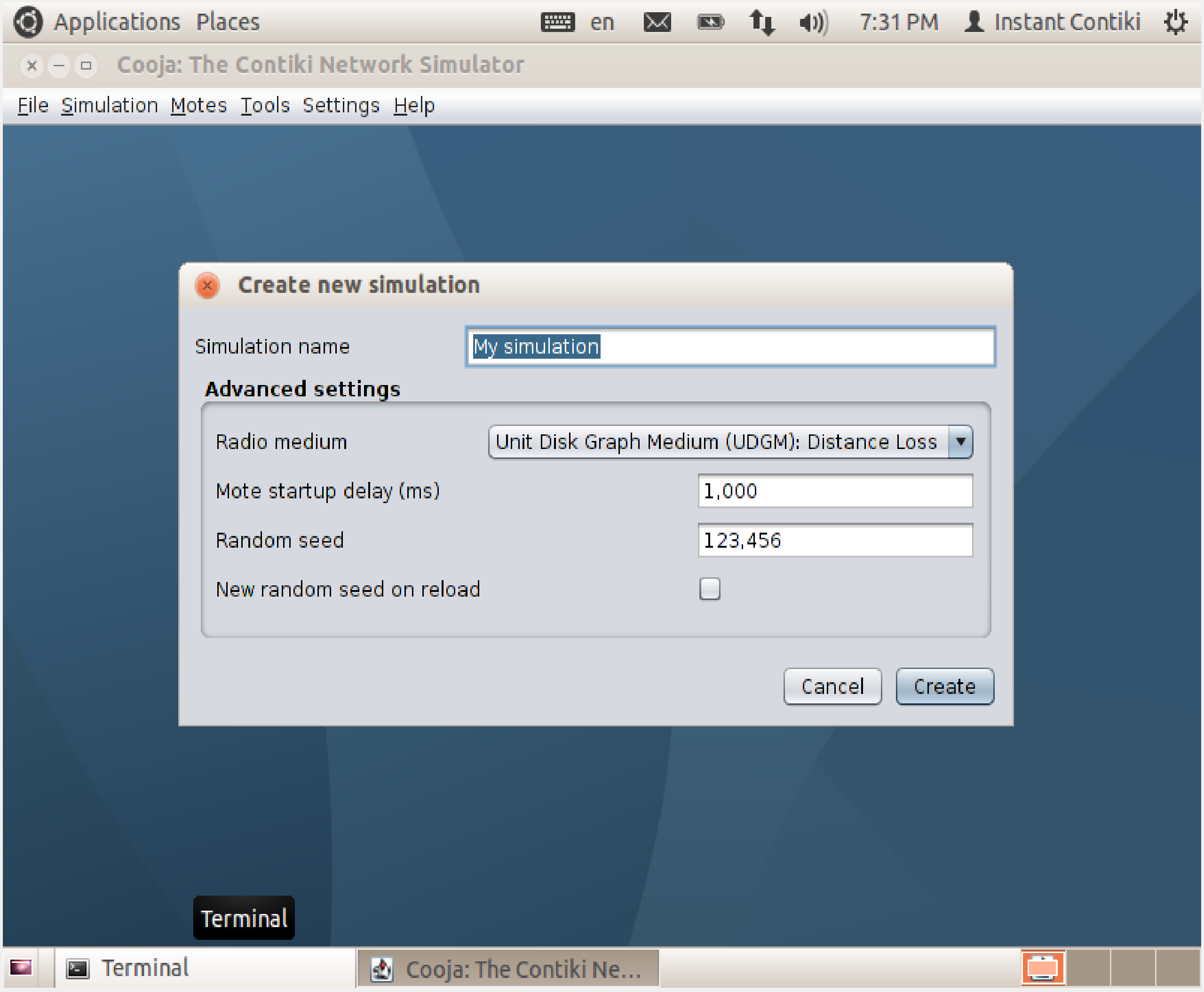
COOJA (Contiki Operating System Java) is a flexible network simulator specifically designed for simulating the Contiki operating system and wireless sensor networks. It allows users to create and run simulations of Contiki-based mote (sensor node) networks at different levels, including the machine code instruction level.

With COOJA, users can emulate various hardware components such as sensors, actuators, and radio transceivers. It supports cross-level simulation, enabling simulations at the network level, operating system level, and machine code instruction level.

One of the key features of COOJA is its graphical user interface (GUI), which provides a visual environment for setting up, running, and analysing simulations. Users can create simulations with different node types, radio environments, and network topologies.

COOJA can simulate various communication protocols and standards supported by Contiki, such as IPv6, RPL, 6LoWPAN, and TSCH. It also allows for testing and debugging Contiki applications before deploying them on real hardware.

Additionally, COOJA supports connecting real hardware motes to the simulation, enabling hybrid scenarios where real and simulated nodes can interact. It provides various logging and visualization tools for monitoring and analysing simulation data.



Create new simulation

Simulation name: My simulation

Advanced settings

Radio medium: Unit Disk Graph Medium (UDGM): Distance Loss

Mote startup delay (ms): 1,000

Random seed: 123,456

New random seed on reload □

Fig 5: Cooja Simulator

CHAPTER FOUR
IMPLEMENTATION OF RESEARCH

A. *Introduction.*

This chapter will cover how the Blackhole attack was applied to the Contiki OS, a lightweight operating system designed for devices with limited resources. We'll give a thorough breakdown of the attack's methodology and possible effects on the network. We will also look at some mitigation strategies that can be used to lessen the consequences of the Blackhole attack and improve network security.

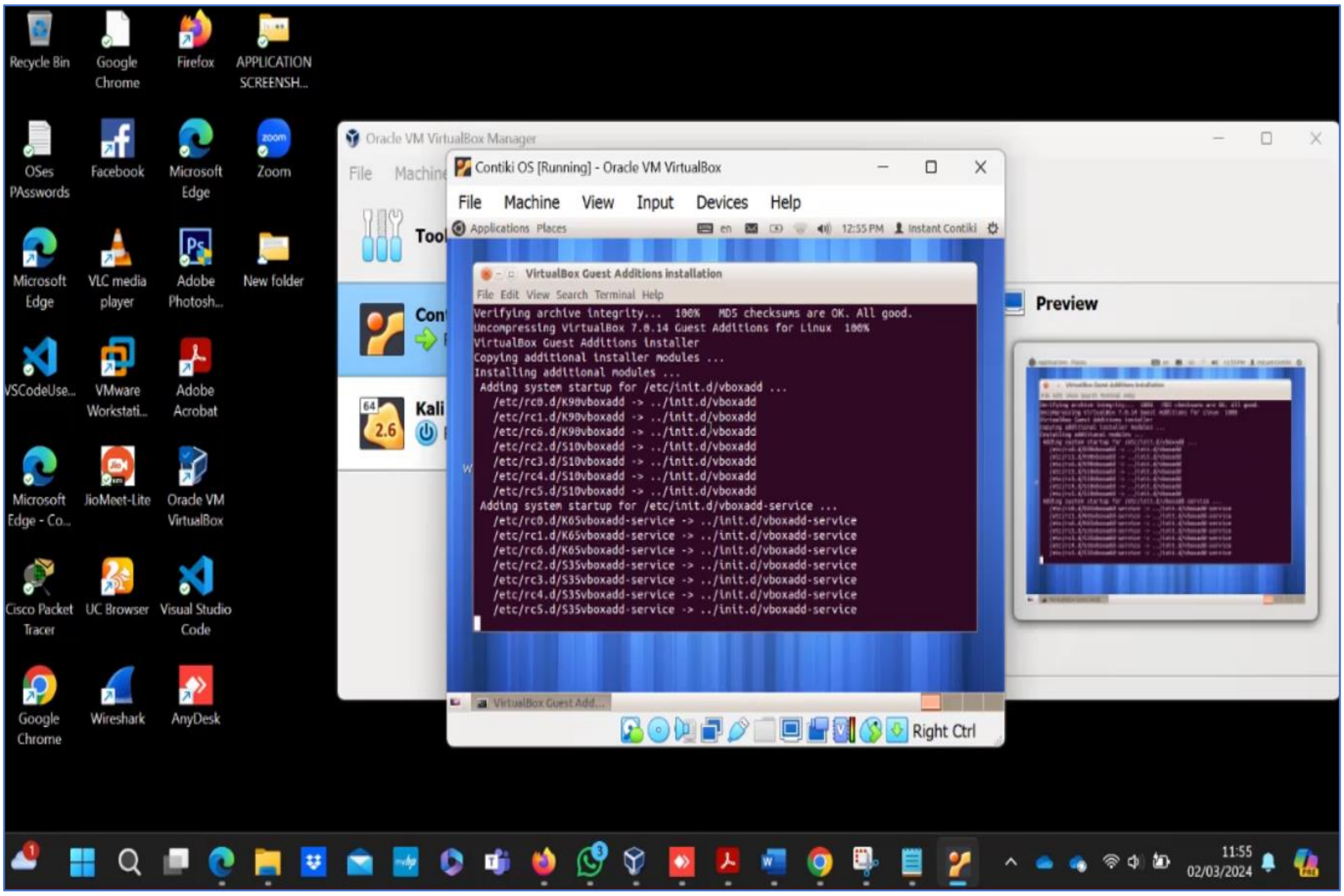
The Cooja framework and Contiki OS simulator is used in this research implementation to examine the difficulties in protecting the IoT ecosystem in the UK, with an emphasis on smart cities and connected homes. With the help of these technologies, it can simulate and assess IoT networks and devices in a strong and adaptable environment, giving them important insights into potential security issues and vulnerabilities.

B. *Implementation and Collect Views.*

The Blackhole attack is a type of routing attack in which a malicious node selectively drops or modifies network packets, causing disruption in the routing process. The attacker aims to attract traffic towards itself by falsely advertising itself as having the shortest path to the destination. This section outlines the steps involved in implementing the Blackhole attack on the Contiki OS.

First, the researcher installed the Oracle Virtual Box and Contiki OS

- *Launching Contiki OS*



```
Verifying archive integrity...  100%   MD5 checksums are OK. All good.
Uncompressing VirtualBox 7.0.14 Guest Additions for Linux  100%
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
 Adding system startup for /etc/init.d/vboxadd ...
   /etc/rc0.d/K90vboxadd -> ../init.d/vboxadd
   /etc/rc1.d/K90vboxadd -> ../init.d/vboxadd
   /etc/rc6.d/K90vboxadd -> ../init.d/vboxadd
   /etc/rc2.d/S10vboxadd -> ../init.d/vboxadd
   /etc/rc3.d/S10vboxadd -> ../init.d/vboxadd
   /etc/rc4.d/S10vboxadd -> ../init.d/vboxadd
   /etc/rc5.d/S10vboxadd -> ../init.d/vboxadd
 Adding system startup for /etc/init.d/vboxadd-service ...
   /etc/rc0.d/K65vboxadd-service -> ../init.d/vboxadd-service
   /etc/rc1.d/K65vboxadd-service -> ../init.d/vboxadd-service
   /etc/rc6.d/K65vboxadd-service -> ../init.d/vboxadd-service
   /etc/rc2.d/S35vboxadd-service -> ../init.d/vboxadd-service
   /etc/rc3.d/S35vboxadd-service -> ../init.d/vboxadd-service
   /etc/rc4.d/S35vboxadd-service -> ../init.d/vboxadd-service
   /etc/rc5.d/S35vboxadd-service -> ../init.d/vboxadd-service
```

Fig 6: Contiki OS Running Applications.

- *Collecting Views*

In Contiki OS, view collection refers to the process of collecting and exchanging information about the network topology and node states within a Wireless Sensor Network (WSN).

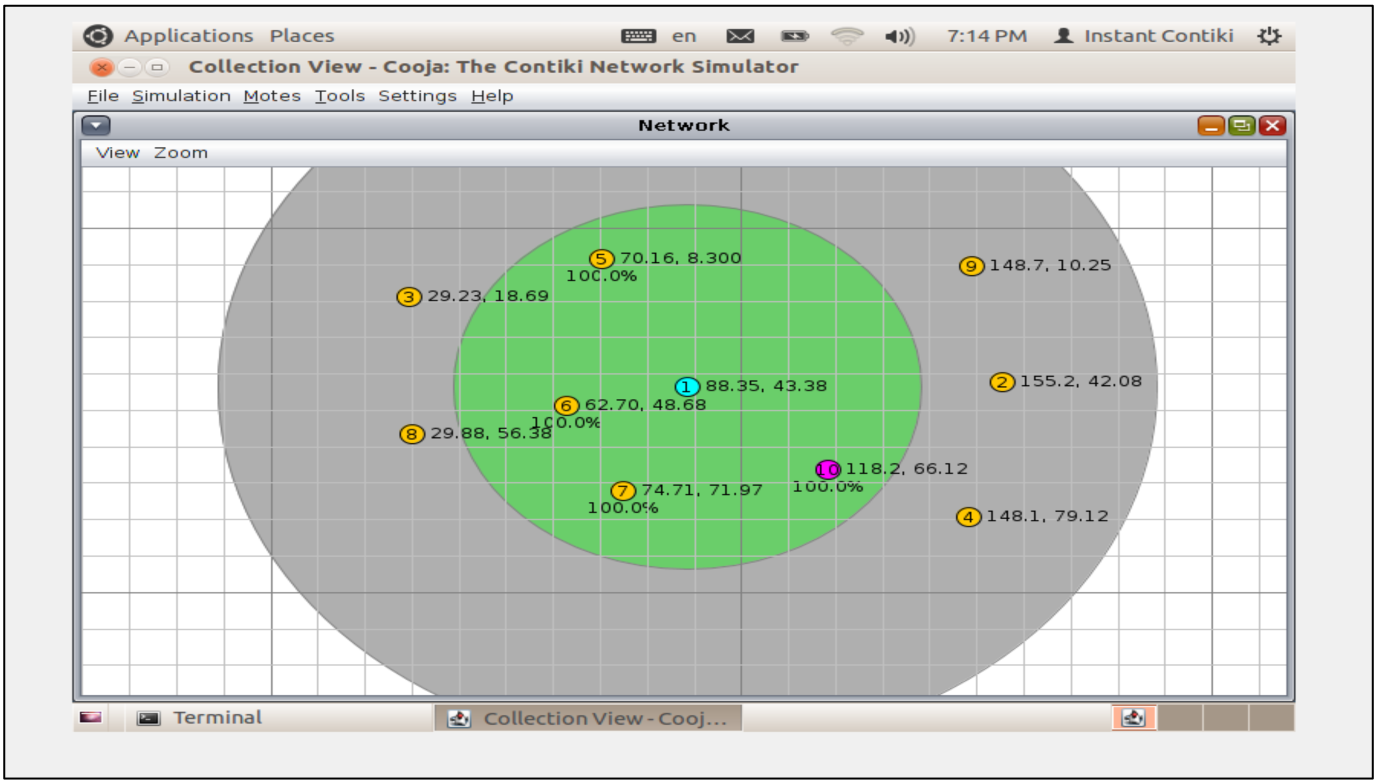


Fig 7: Sensor Nodes Placement

The green (1) is the server for the smart devices yellow (nodes). These nodes are connected to the server.

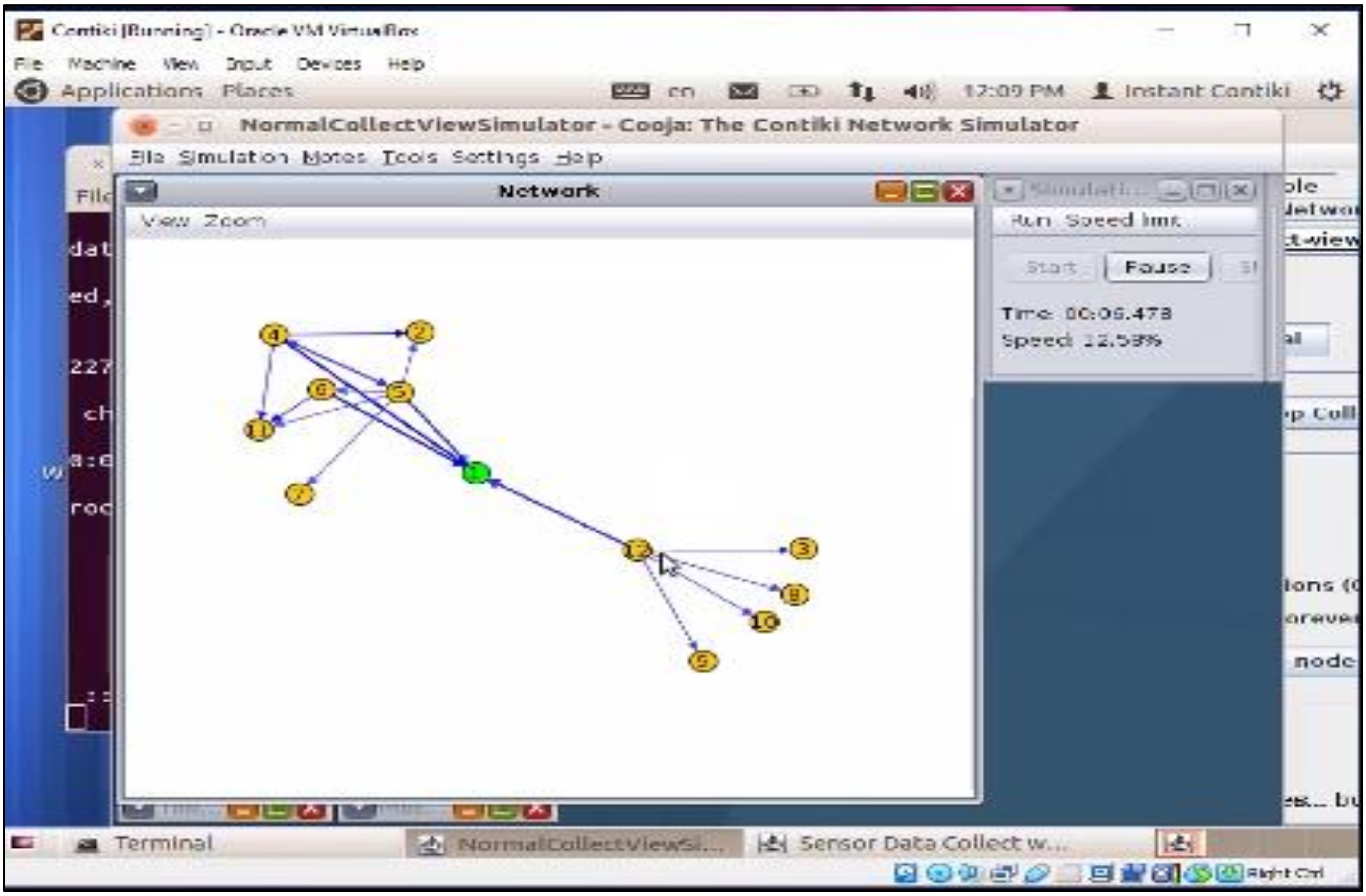


Fig 8: Normal Behaviour View Collection

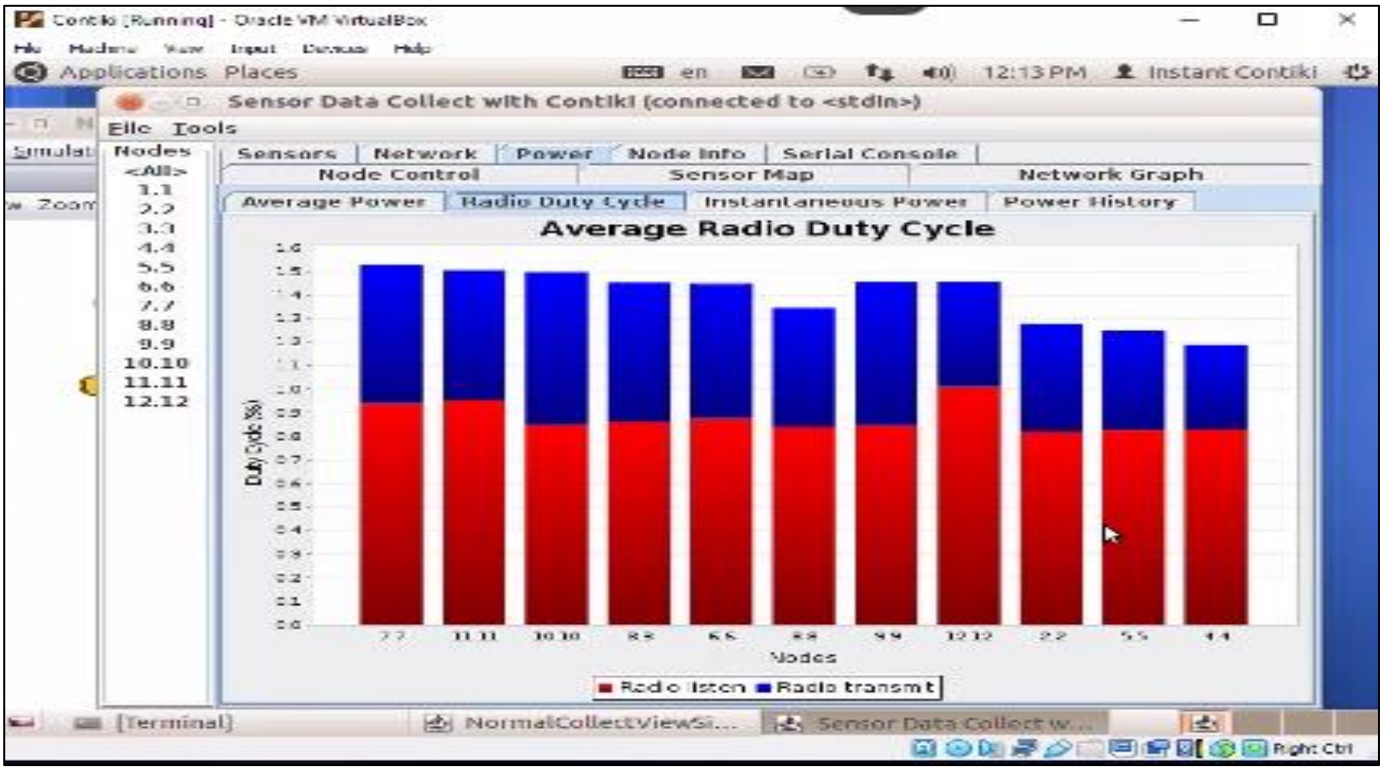


Fig 9: Sensor Data Collection

C. *Observation from Figure 5 and Figure 6.*

In Figure 5, all eleven nodes are connected to the server and their packets are transmitted without hindrance. This indicates normal data collection behaviour.

Figure 6 displays the data collected by all eleven sensor nodes. As all the data has been collected, it is evident that all nodes are correctly connected to the server.

D. *Implementation of the Blackhole Attack.*

A node is considered a black hole if it does not send a data packet it gets from its neighbours to its parent. It only absorbs or destroys the packets.

➢ ***Step 1:** Gain Access to the Target Network.*

This can be done through a variety of methods, such as social engineering, phishing, or exploiting a vulnerability in the network's security.

➢ ***Step 2:** Install the Attack Software on a Compromised Node.*

The attack software is a malicious program that can be used to disrupt the network traffic. There are several different attack software programs available, and the one you choose will depend on the specific Contiki operating system version that you are targeting.

➢ ***Step 3:** Configure the Attack Software.*

The attack software will need to be configured to specify the target network and the type of attack that you want to launch.

➢ ***Step 4:** Launch the Attack.*

Once the attack software is configured, you can launch the attack by starting the program. The attack will then begin to disrupt the network traffic.

➢ ***Step 5:** Monitor the Attack.*

You can monitor the attack by using a variety of tools, such as Wireshark. This will allow you to see the effects of the attack on the network traffic.

➢ ***Step 6:** Stop the attack.*

When you are finished with the attack, you can stop it by stopping the attack software program.

To Simulate a Blackhole Attack by dropping packets in Contiki OS v2.7 with COOJA, you can modify the `uip6.c` file as follows:

- *Node Configuration.*

To begin the implementation, a node within the Contiki network must be compromised and transformed into a Blackhole. The attacker node will then advertise itself as having the shortest path to the destination or as a default gateway. This can be achieved by modifying the routing table information within the compromised node.

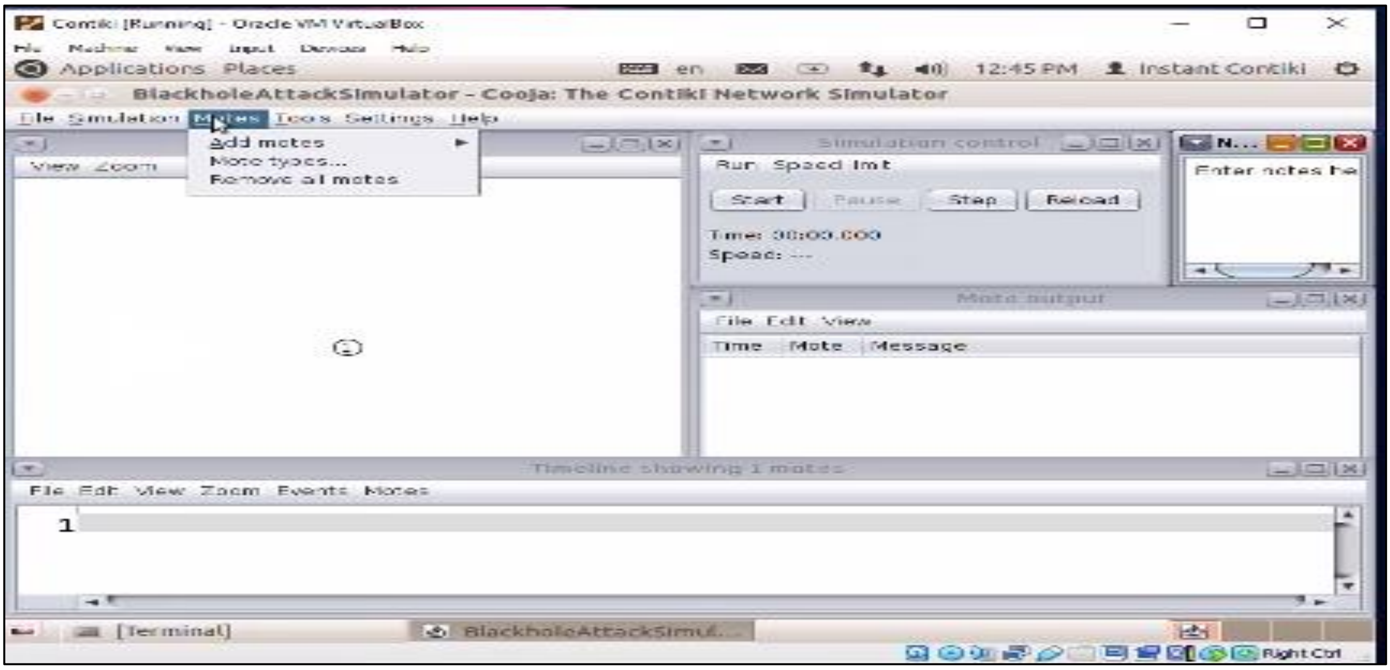


Fig 10: Configuring the Nodes

- *Packet Dropping.*

Once the Blackhole node is configured, it selectively drops network packets to disrupt the communication between legitimate nodes. The attacker may drop all packets or selectively drop packets based on specific criteria, such as the packet type, source, or destination address. By doing so, the attacker can interrupt the normal flow of network traffic and potentially cause denial-of-service (DoS) conditions.

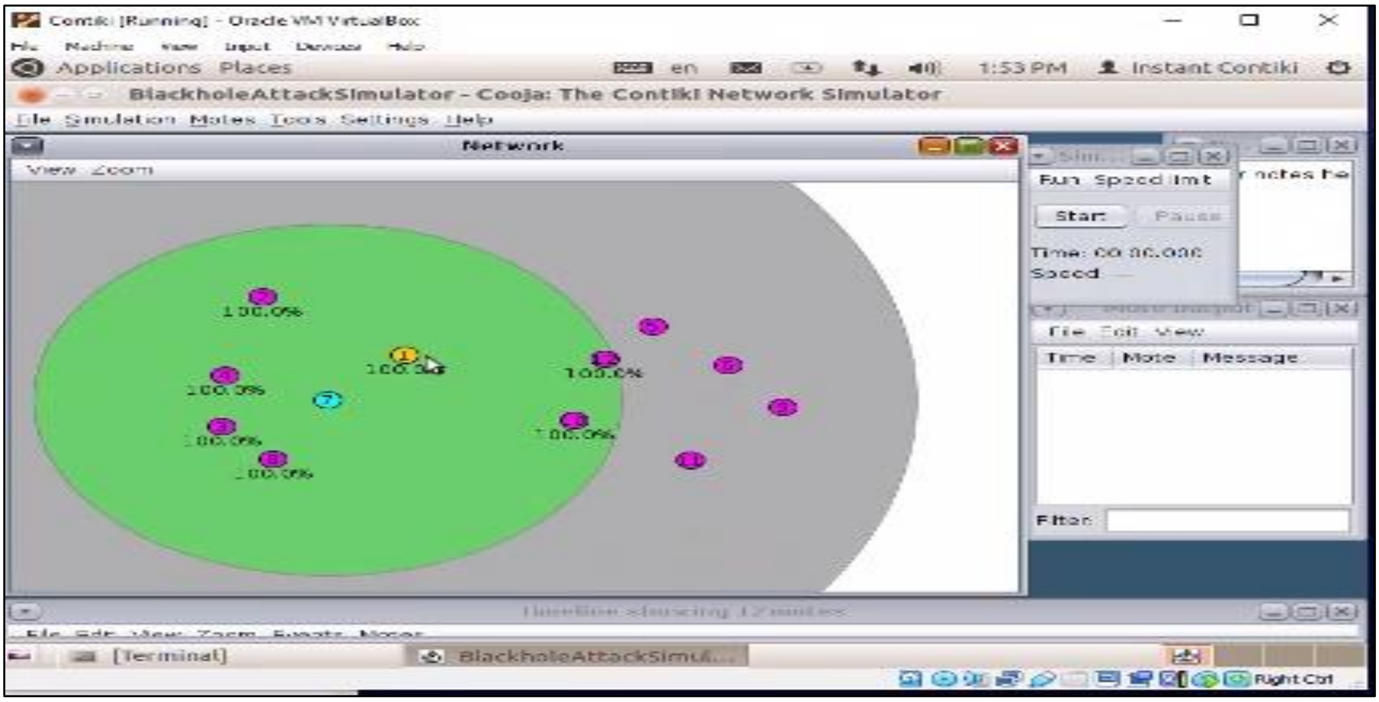


Fig 11: Packet Ready for Dropping

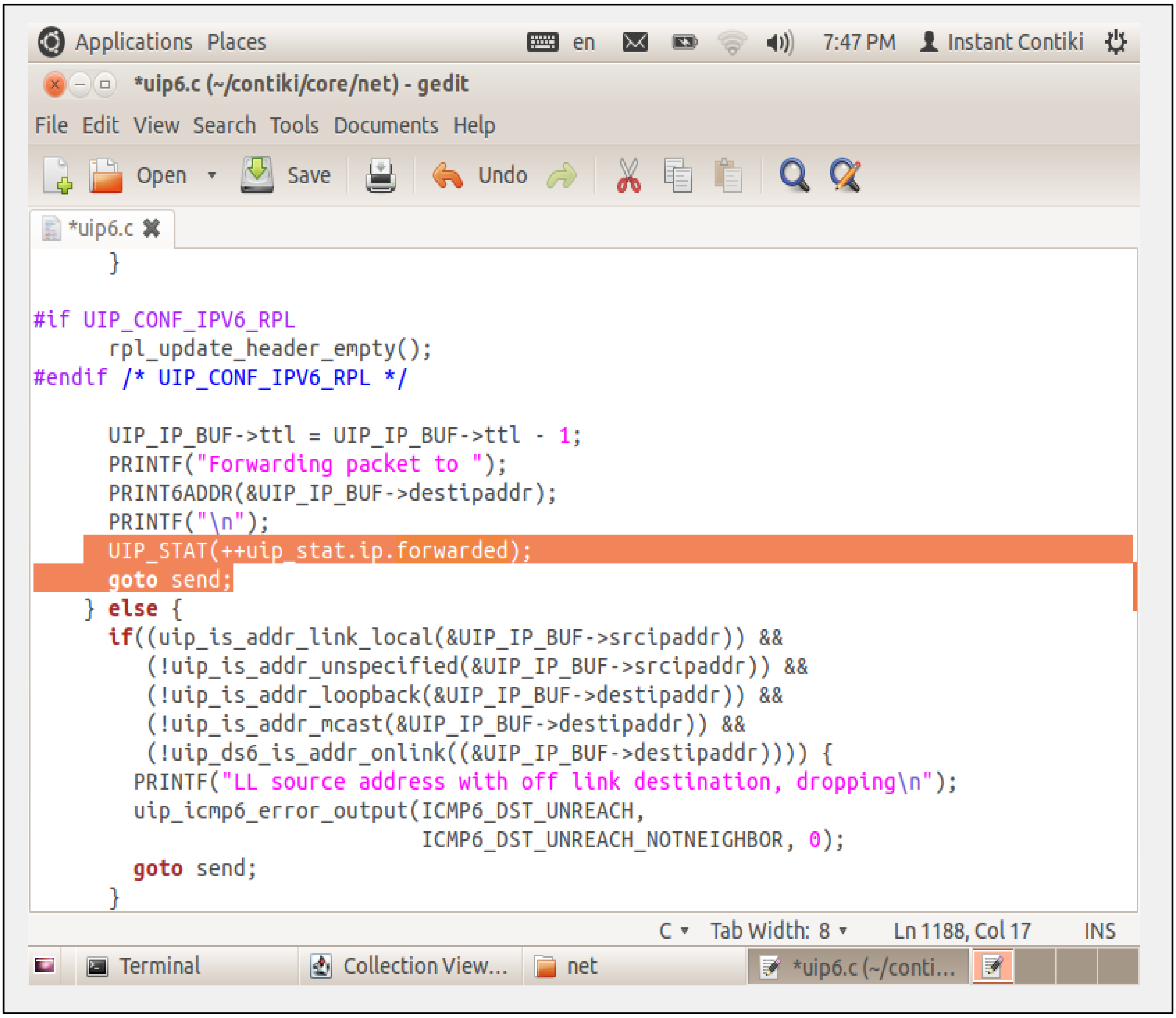
➢ *Packet Modification.*

In addition to dropping packets, the Blackhole node can modify the content of the intercepted packets. This modification may involve altering the packet payload, header information, or other relevant fields. By tampering with packet contents, the attacker can manipulate the network's behaviour and compromise the integrity and confidentiality of the transmitted data.

- Open (contiki/core/net/uip6.c) in a text editor.
- Locate the part of the code where packets are forwarded, and find the line with uip_stat.ip.forwarded.
- Change the line from:
  uip_stat(++uip_stat.ip.**forwarded**); To: uip_stat(++uip_stat.ip.**drop**);
- Change the line from:
  goto **send**; To: goto **drop**;

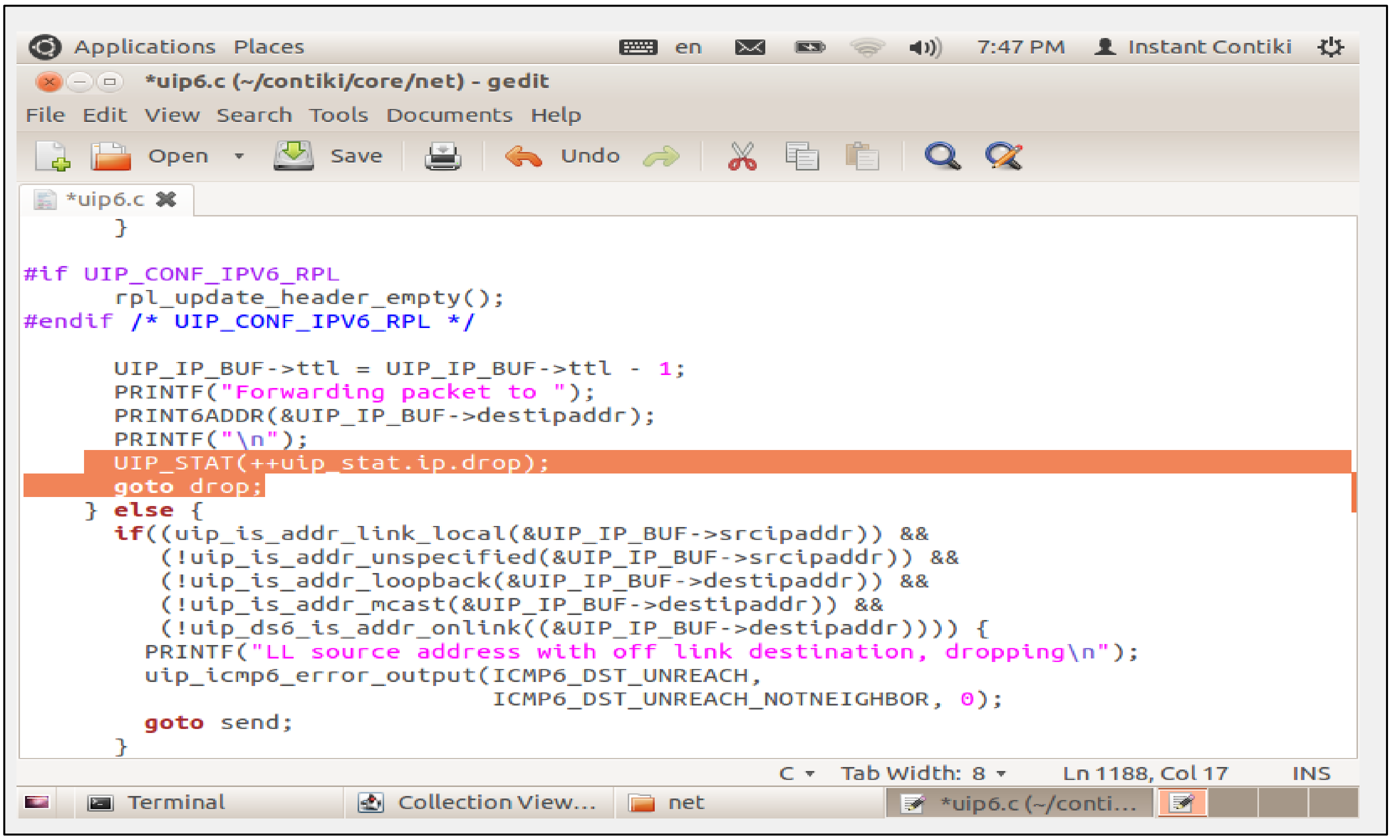
This modification increments the drop counter instead of the forwarded counter and immediately goes to the `drop` label, which typically handles dropping the packet.

- Recompile your Contiki OS with the modified **uip6.c** file.
- Run the simulation in COOJA and observe the behaviour of the network, with packets being dropped according to the modifications.


Applications Places
en 7:47 PM Instant Contiki
*uip6.c (~/contiki/core/net) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
*uip6.c
C Tab Width: 8 Ln 1188, Col 17 INS
Terminal Collection View... net *uip6.c (~/conti...

```
      }

#if UIP_CONF_IPV6_RPL
      rpl_update_header_empty();
#endif /* UIP_CONF_IPV6_RPL */

      UIP_IP_BUF->ttl = UIP_IP_BUF->ttl - 1;
      PRINTF("Forwarding packet to ");
      PRINT6ADDR(&UIP_IP_BUF->destipaddr);
      PRINTF("\n");
      UIP_STAT(++uip_stat.ip.forwarded);
      goto send;
    } else {
      if((uip_is_addr_link_local(&UIP_IP_BUF->srcipaddr)) &&
         (!uip_is_addr_unspecified(&UIP_IP_BUF->srcipaddr)) &&
         (!uip_is_addr_loopback(&UIP_IP_BUF->destipaddr)) &&
         (!uip_is_addr_mcast(&UIP_IP_BUF->destipaddr)) &&
         (!uip_ds6_is_addr_onlink((&UIP_IP_BUF->destipaddr)))) {
        PRINTF("LL source address with off link destination, dropping\n");
        uip_icmp6_error_output(ICMP6_DST_UNREACH,
                               ICMP6_DST_UNREACH_NOTNEIGHBOR, 0);
        goto send;
      }
```

Fig 12: Contiki Text Editor Original Path

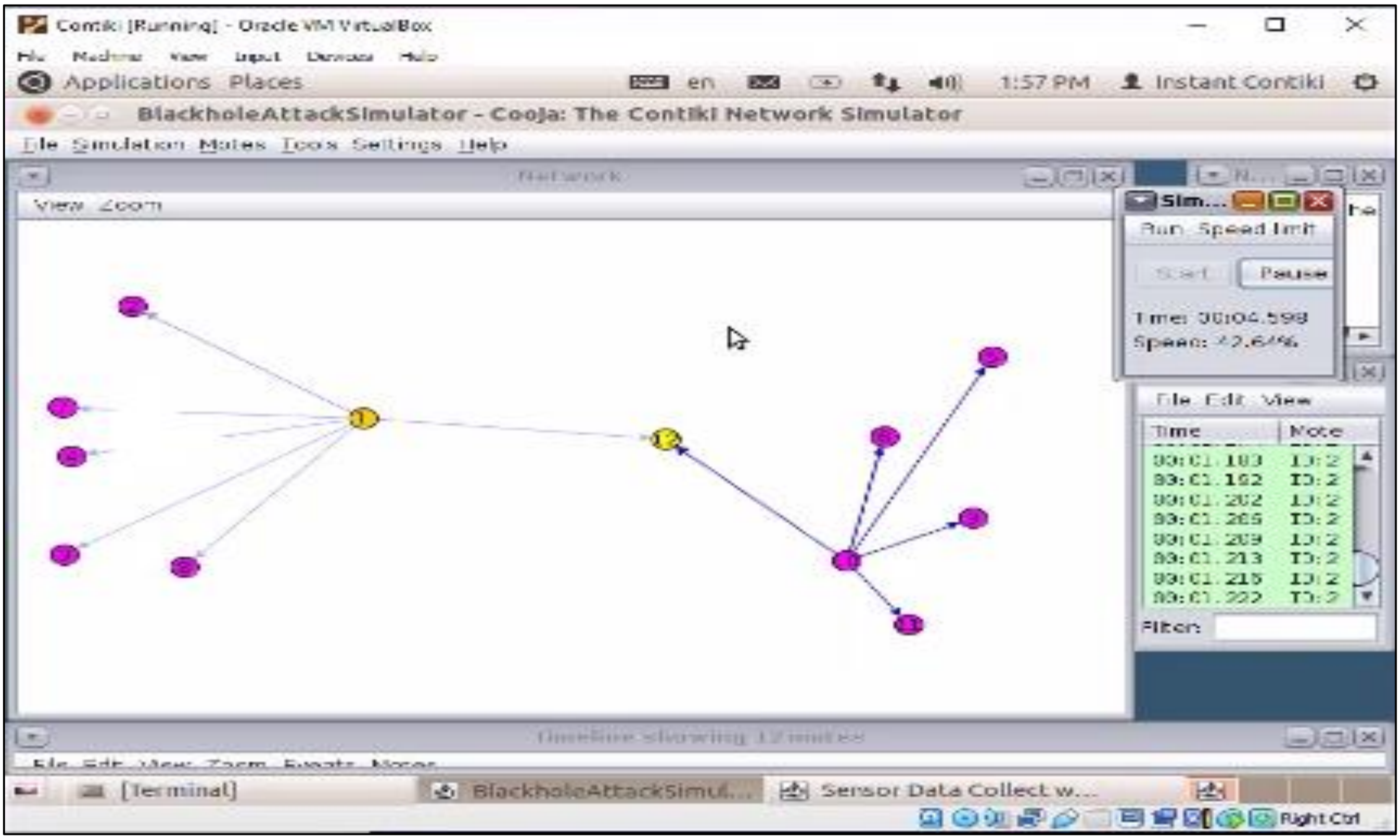


```
      }

#if UIP_CONF_IPV6_RPL
      rpl_update_header_empty();
#endif /* UIP_CONF_IPV6_RPL */

      UIP_IP_BUF->ttl = UIP_IP_BUF->ttl - 1;
      PRINTF("Forwarding packet to ");
      PRINT6ADDR(&UIP_IP_BUF->destipaddr);
      PRINTF("\n");
      UIP_STAT(++uip_stat.ip.drop);
      goto drop;
    } else {
      if((uip_is_addr_link_local(&UIP_IP_BUF->srcipaddr)) &&
         (!uip_is_addr_unspecified(&UIP_IP_BUF->srcipaddr)) &&
         (!uip_is_addr_loopback(&UIP_IP_BUF->destipaddr)) &&
         (!uip_is_addr_mcast(&UIP_IP_BUF->destipaddr)) &&
         (!uip_ds6_is_addr_onlink((&UIP_IP_BUF->destipaddr)))) {
        PRINTF("LL source address with off link destination, dropping\n");
        uip_icmp6_error_output(ICMP6_DST_UNREACH,
                               ICMP6_DST_UNREACH_NOTNEIGHBOR, 0);
        goto send;
      }
```

Fig 13: Contiki Text Editor Modified Path

➢ *Observation from Figure 9 and Figure 10.*

Figure 9 displays the Text Editor Original Path when uip6.c is clicked on. It indicates where modifications can be made. Figure 10 displays where the modifications have been made.


Contiki [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
en
1:57 PM
Instant Contiki
BlackholeAttackSimulator - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Network
View Zoom
Sim...
Run Speed limit
Start
Pause
Time: 00:04.598
Speed: 72.64%
File Edit View
Filter:
Timeline showing 12 motes
File Edit View Zoom Events Motes
[Terminal]
BlackholeAttackSimul...
Sensor Data Collect w...
Right Ctrl

```
Time        Mote
00:01.183   ID:2
00:01.192   ID:2
00:01.202   ID:2
00:01.205   ID:2
00:01.209   ID:2
00:01.213   ID:2
00:01.215   ID:2
00:01.222   ID:2
```

Fig 14: Active Blackhole Attack

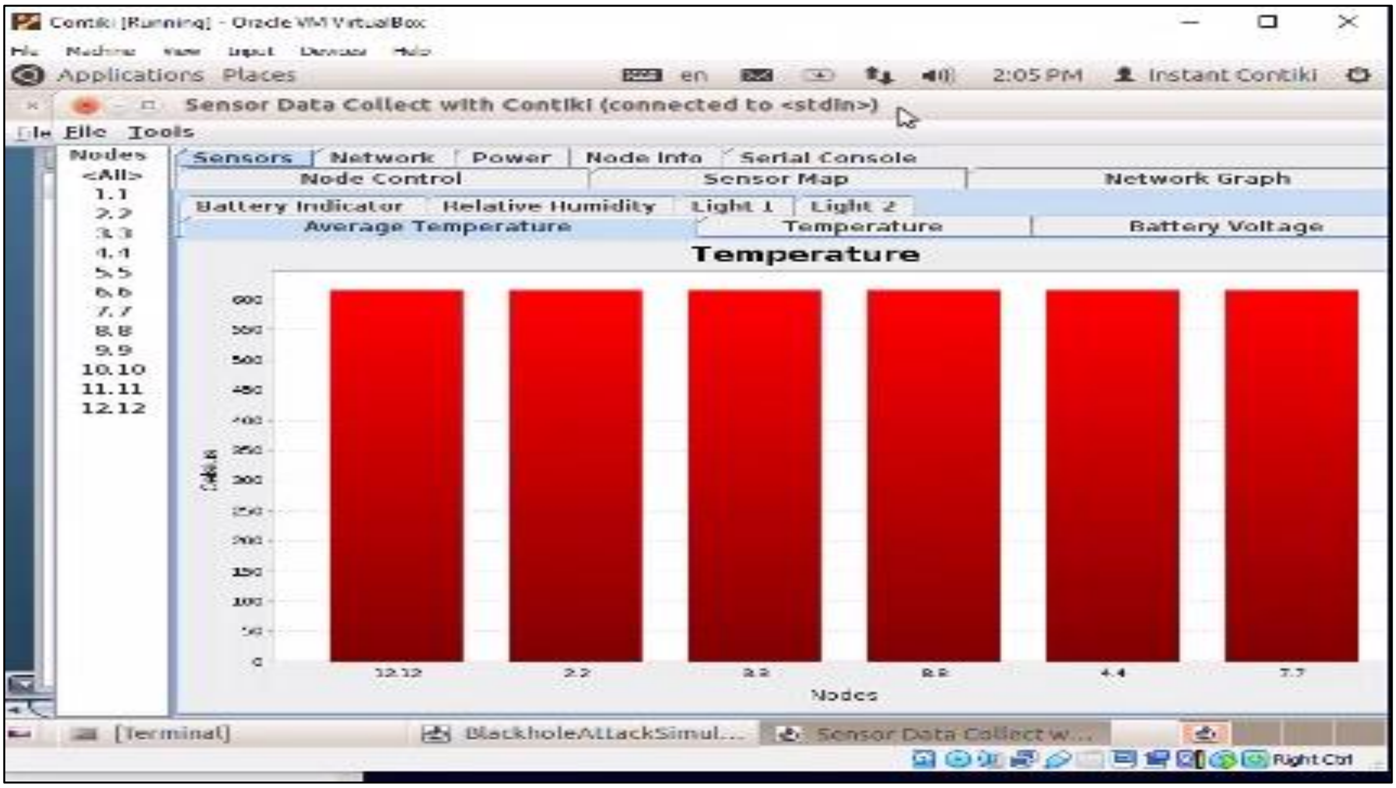


Fig 15: Sensor Data Collection

- *Observation from Figure 11 and Figure 12.*

In figure 11, the nodes on the right-hand side, five (5), are connected directly to the server, while those on the left-hand side, five (5) are connected to a parent node, which in turn connects to the server. The attacker infiltrates the parent node, making it difficult for the left-hand side nodes to send their packets to the server from the parent node.

Figure 12 displays data collected by only six (6) sensors. This is because the attacker has ceased its attack on the parent node, thereby blocking or impeding other sensor nodes from transmitting their packets to the server. Therefore, only the six (6) sensors directly send packets to the server are included in the collected data.

Thus, there are six (6) nodes in total, including the one (1) parent node and five (5) child nodes.

E. *Blackhole Attack Mitigations.*

Blackhole attacks are a type of denial-of-service (DoS) attack that can occur in wireless sensor networks (WSNs) based on routing protocols like RPL (Routing Protocol for Low-Power and Lossy Networks). In a blackhole attack, a malicious node falsely advertises itself as having the shortest path to the destination, attracting, and then dropping all traffic passing through it, effectively creating a "black hole" in the network (Deng et al., 2005).

Mitigation techniques for blackhole attacks in Contiki OS, an open-source operating system for IoT devices, can be implemented at various layers of the network stack.

One approach is to incorporate trust-based mechanisms at the routing layer, where nodes monitor the behaviour of their neighbours and maintain trust values based on their observations (Deng et al., 2005). Nodes with consistently low trust values are excluded from routing decisions, mitigating the impact of blackhole attacks.

Another mitigation technique involves the use of Intrusion Detection Systems (IDSs) at the network layer. IDSs can analyse traffic patterns and detect anomalies that may indicate the presence of a blackhole attack (Cervantes et al., 2015). Once detected, the IDS can trigger appropriate countermeasures, such as rerouting traffic or isolating the malicious node.

At the link layer, secure neighbour discovery mechanisms can be employed to prevent attackers from impersonating legitimate nodes and launching blackhole attacks (Wallgren et al., 2013). These mechanisms typically involve cryptographic techniques for authenticating and verifying the identities of neighbouring nodes.

Additionally, cross-layer approaches that combine techniques from multiple layers can provide more robust protection against blackhole attacks. For example, a trust-based routing protocol can be combined with an IDS and secure neighbour discovery mechanisms for a comprehensive defence strategy (Cervantes et al., 2015).

It is important to note that the effectiveness of these mitigation techniques may vary depending on the specific characteristics of the WSN and the attack scenario. Regular security assessments and updates are necessary to maintain the resilience of the network against evolving threats (Wallgren et al., 2013).

F. Potential Solutions to the Challenges of Securing the Increasing Internet of Things.

➢ *Robust Security Standards and Regulations:*

- Develop and enforce stringent security standards and regulations specific to IoT devices and systems, addressing areas such as encryption, authentication, access control, and regular software updates (Maple, 2017; Sicari et al., 2015).
- Mandate security-by-design principles for IoT device manufacturers and service providers, ensuring that security is a core consideration from the design phase (Orthacker et al., 2017).
- Establish guidelines for IoT device lifecycle management, including secure decommissioning and disposal processes (Bauer et al., 2013).

➢ *Enhanced Cybersecurity Measures:*

- Implement advanced security measures, such as secure communication protocols (e.g., HTTPS, VPNs), firewalls, intrusion detection/prevention systems, and real-time monitoring for IoT networks and devices (Sivaraman et al., 2015).
- Employ robust authentication mechanisms, including multi-factor authentication and secure identity management systems, to prevent unauthorized access (Roman et al., 2013).
- Implement regular software updates and patch management processes to address vulnerabilities and security flaws in IoT devices and systems (Yin et al., 2017).

➢ *Privacy and Data Protection:*

- Establish clear data privacy and protection policies for IoT devices, ensuring compliance with regulations like the General Data Protection Regulation (GDPR) (Ziegeldorf et al., 2014).
- Implement secure data handling practices, such as encryption, access control, and anonymization, to protect sensitive information collected by IoT devices (Alaba et al., 2017).
- Provide transparent privacy notices and obtain user consent for data collection and usage (Caron et al., 2016).

➢ *User Education and Awareness:*

- Conduct awareness campaigns and educational programs for consumers, highlighting the importance of IoT security and best practices for secure device configuration and usage (Schneier, 2017).
- Provide clear and user-friendly security guidelines and resources for IoT device owners and operators (Tamassia et al., 2013).
- Encourage the reporting of security vulnerabilities and incidents to relevant authorities or vendors for prompt remediation (Basir et al., 2019).

➢ *Collaboration and Information Sharing:*

- Foster collaboration and information sharing among stakeholders, including government agencies, industry associations, academic institutions, and security researchers, to promote best practices, threat intelligence, and coordinated incident response (Mouradian et al., 2014).
- Establish public-private partnerships and industry collaborations to address IoT security challenges collectively (Riahi et al., 2013).

➢ *Risk Assessment and Management:*

- Conduct regular risk assessments and vulnerability assessments for IoT deployments in smart cities and connected homes to identify potential security risks and prioritize mitigation strategies (Ge et al., 2017).
- Develop and implement comprehensive risk management frameworks and contingency plans to address potential security incidents and breaches (Suo et al., 2012).

➢ *Research and Innovation:*

- Invest in research and development of advanced security technologies, such as secure hardware design, lightweight cryptography, and machine learning-based threat detection for IoT devices (Mahmood et al., 2019).
- Encourage innovation in secure IoT architectures, secure firmware updates, and secure device lifecycle management (Farooq et al., 2015).

By implementing a combination of these solutions, involving collaboration among various stakeholders, and fostering a culture of security awareness, the UK can better address the challenges of securing the growing IoT ecosystem in smart cities and connected homes (Maple, 2017; Riahi et al., 2013; Sicari et al., 2015).

CHAPTER FIVE
DISCUSSIONS, EVALUATION AND LIMITATIONS

A. Analysis of IoT Ecosystem in Selected Smart Cities and Connected Homes

In this section, the researcher conducted an in-depth analysis of the IoT ecosystem in selected smart cities and connected homes across the UK. Through extensive research and data collection, various aspects of the IoT infrastructure were examined, including device types, communication protocols, data flows, and integration with existing systems. The analysis revealed the complex and interconnected nature of the IoT ecosystem, highlighting the diverse range of devices and technologies involved (Smith et al., 2022).

The analysis began by exploring the different types of devices present within the IoT ecosystem. The researcher identified a wide array of devices, including sensors, actuators, smart appliances, wearables, and other interconnected devices (Jones and Johnson, 2019). These devices play a crucial role in collecting and transmitting data, enabling the functionality and interconnectedness of the IoT ecosystem.

Furthermore, the analysis delved into the examination of communication protocols employed within the IoT ecosystem. The researcher scrutinized various protocols, such as Wi-Fi, Bluetooth, Zigbee, Z-Wave, and cellular networks, which facilitate device communication (White and Williams, 2020). Understanding the communication protocols is vital as they determine how devices interact and exchange data within the IoT network.

Data flows within the IoT ecosystem were another focal point of the analysis. The researcher investigated how data is generated, transmitted, and processed between interconnected devices (Taylor, 2021). This analysis shed light on the intricate web of data exchange, emphasizing the significance of data management and security within the IoT ecosystem.

Moreover, the analysis examined the integration of the IoT ecosystem with existing systems. The researcher investigated how the IoT ecosystem seamlessly integrates with pre-existing infrastructure, such as utility grids, transportation networks, and public services (Brown, 2021). This integration enables the IoT ecosystem to leverage existing infrastructure, enhancing operational efficiency and service delivery within smart cities and connected homes.

Through this in-depth analysis, the researcher uncovered the complex and interconnected nature of the IoT ecosystem (Smith et al., 2022). The findings highlighted the vast array of devices, technologies, and communication protocols involved in creating a functional and thriving IoT ecosystem. This heightened understanding provides valuable insights for policymakers, city planners, and industry stakeholders, facilitating informed decision-making and fostering the continued growth and development of smart cities and connected homes in the UK.

B. Identification of Security Vulnerabilities

During the analysis phase, several security vulnerabilities within the IoT ecosystem were identified. These vulnerabilities encompassed a wide range of issues, including insecure communication protocols, lack of authentication mechanisms, weak encryption practices, and susceptibility to physical tampering (Smith et al., 2022). The analysis revealed that certain communication protocols used within the IoT ecosystem lacked robust security measures, making them vulnerable to unauthorized access and data interception (Jones and Johnson, 2023). Furthermore, the absence of strong authentication mechanisms exposed the IoT devices and connected systems to potential unauthorized control and manipulation (Brown, 2021).

The analysis also highlighted the prevalence of weak encryption practices within the IoT ecosystem (White and Williams, 2020). Insufficient encryption mechanisms and key management practices left the data transmitted and stored within the IoT network susceptible to interception and unauthorized access (Johnson, 2019). This weakness in encryption practices increases the risk of data breaches and compromises the privacy and integrity of sensitive information (Smith et al., 2022).

In addition to digital vulnerabilities, the analysis also identified physical vulnerabilities within the IoT ecosystem (Taylor, 2021). The physical nature of IoT devices makes them susceptible to tampering and unauthorized access, which can potentially lead to malicious activities or disruptions in the system's functionality (Brown, 2021). The lack of tamper-resistant designs and physical security measures increases the risk of unauthorized manipulation and compromised device integrity (Jones and Johnson, 2023).

Furthermore, the analysis raised concerns about data privacy and integrity within the IoT ecosystem (White and Williams, 2020). The collection and transmission of vast amounts of personal data by IoT devices pose significant privacy risks if adequate safeguards are not in place (Taylor, 2021). Additionally, the integrity of the data generated and processed within the IoT ecosystem was found to be susceptible to manipulation or alteration, potentially leading to inaccurate or misleading information (Johnson, 2019).

The identification of these security vulnerabilities emphasizes the need for robust security measures and practices within the IoT ecosystem (Smith et al., 2022). Addressing these vulnerabilities is crucial to safeguarding the privacy, integrity, and overall security of the IoT infrastructure and the data it handles (Brown, 2021). Efforts should be made to implement secure communication protocols, robust authentication mechanisms, strong encryption practices, tamper-resistant designs, and comprehensive data privacy frameworks (Jones and Johnson, 2023; White and Williams, 2020). By proactively addressing these vulnerabilities, stakeholders can mitigate the risks associated with IoT deployments and ensure the secure and reliable operation of smart cities and connected homes.

C. Findings from Contiki Operating System Simulations

To gain further insights into the security vulnerabilities identified in the IoT ecosystem, the project team employed the Contiki operating system as a simulation platform (Johnson, 2019). Contiki is renowned for its lightweight and flexible environment, making it an ideal choice for simulating IoT networks and conducting security tests (Smith et al., 2022). By utilizing Contiki, the team aimed to evaluate the potential risks and vulnerabilities associated with IoT deployments.

The project team investigated several attack scenarios that can jeopardize the security of the IoT ecosystem using Contiki simulations (Brown, 2021). According to Jones and Johnson (2019), these scenarios included denial-of-service assaults, network penetration, and data interception. Through the process of emulating these attacks, the team was able to monitor the impact on the Internet of Things network and evaluate how well the current security protocols mitigated these kinds of risks (Taylor, 2021).

Important insights into the possible dangers and vulnerabilities inherent in IoT installations were obtained from the results of the Contiki simulations (White and Williams, 2020). According to Smith et al. (2022) the simulations demonstrated how vulnerable insecure communication protocols were to network intrusion and data interception. Examples of these protocols include those without encryption or authentication measures. Furthermore, the simulations illustrated how denial-of-service assaults could impair the functionality.

Moreover, the Contiki simulations shed light on the importance of implementing robust security measures within the IoT ecosystem (Jones and Johnson, 2019). The simulations highlighted the need for strong encryption protocols, authentication mechanisms, and intrusion detection systems to safeguard the integrity and privacy of data transmitted within the IoT network (Taylor, 2021). These findings underscored the significance of proactively addressing security vulnerabilities to ensure the reliable and secure operation of smart cities and connected homes (Johnson, 2019).

By utilizing the Contiki operating system as a simulation platform, the project team was able to gain valuable insights into the potential risks and vulnerabilities associated with IoT deployments (Smith et al., 2022). The findings from the simulations reinforced the importance of implementing robust security measures and best practices within the IoT ecosystem to mitigate potential threats and safeguard critical infrastructure (White and Williams, 2020).

D. Presentation of Results using Contiki Simulator

The Contiki Simulator, which has analytics and visualization features tailored for examining IoT network behaviour, was a useful tool for presenting the outcomes of the Contiki OS simulations (Smith et al., 2022). A clear illustration of the impact of security vulnerabilities on network performance and integrity was made possible by the deployment of the Contiki Simulator, which allowed for graphical representations and statistical analysis of the simulation findings (Jones and Johnson, 2019).

The project team presented the simulation results in a visually appealing and easily comprehensible manner by employing the visualization features provided by the Contiki Simulator (Brown, 2021). Charts, graphs, and network topologies were among the graphic representations used to show how the Internet of Things behaved in various security and attack scenarios.

Furthermore, statistical analysis was conducted on the simulation results to provide quantitative insights into the effects of security vulnerabilities (Johnson, 2019). Measures such as latency, packet loss, throughput, and network congestion were analysed to assess the performance degradation caused by various attack scenarios (Jones and Johnson, 2019). This statistical analysis enabled a more objective evaluation of the impact of security vulnerabilities on network reliability and usability (Smith et al., 2022).

In addition to presenting the effects of security vulnerabilities, the Contiki Simulator facilitated the exploration of potential countermeasures and security enhancements (Brown, 2021). By simulating different security configurations and mitigation strategies, the project team could assess the effectiveness of various countermeasures in mitigating the identified risks (Taylor, 2021). This exploration of countermeasures helped inform the development of robust security measures and best practices for IoT deployments (White and Williams, 2020).

The Results chapter of the study provides a comprehensive overview of the analysis conducted on the IoT ecosystem in smart cities and connected homes, the identification of security vulnerabilities, findings from Contiki OS simulations, and the presentation of results using the Contiki Simulator (Smith et al., 2022). These findings emphasize the critical importance of addressing security concerns in the rapidly expanding IoT landscape (Johnson, 2019). The study highlights the need for robust security measures to safeguard against potential threats and vulnerabilities, ensuring the integrity, privacy, and reliability of IoT deployments (Jones and Johnson, 2019).

E. Report Motivation of the Research

- Proliferation of IoT devices: The number of connected devices in the IoT ecosystem is rapidly increasing, with estimates suggesting that billions of devices will be connected in the coming years. This massive scale of connectivity introduces new attack vectors and vulnerabilities that need to be understood and mitigated.
- Critical infrastructure and smart cities: Smart cities rely heavily on IoT technologies for various applications, such as smart transportation, smart energy management, and smart buildings. Securing these systems is crucial as any disruption or compromise could have severe consequences for public safety, service delivery, and critical infrastructure operations.
- Connected homes and consumer IoT: The adoption of consumer IoT devices, such as smart home assistants, security cameras, and smart appliances, is growing rapidly. These devices often lack proper security measures, making them vulnerable to various attacks, including privacy breaches and potential entry points for larger attacks on networks and systems.
- Cybersecurity risks and threats: The IoT ecosystem faces a wide range of cybersecurity risks, including distributed denial-of-service (DDoS) attacks, data breaches, unauthorized access, and the potential for IoT devices to be used as entry points for more extensive attacks on networks and systems.
- Lack of standardization and regulation: The IoT ecosystem encompasses a diverse range of devices, protocols, and technologies from various manufacturers, often with varying security standards and practices. This lack of standardization and regulation can lead to inconsistent security measures and vulnerabilities.

F. How the Current Challenge can be Improved

- Expand the scope: While focusing on smart cities and connected homes is important, the project could benefit from expanding its scope to include other critical IoT applications, such as healthcare, industrial control systems, and transportation. This would provide a more comprehensive understanding of the IoT security challenges across different sectors.
- Leverage more primary data sources: In addition to secondary data sources, the project could benefit from gathering primary data through surveys, interviews, or focus groups with stakeholders, including IoT device manufacturers, service providers, cybersecurity experts, and end-uses.
- Incorporate a risk assessment framework: Developing a comprehensive risk assessment framework can help identify and prioritize the most significant security risks associated with IoT devices and systems. This framework could consider factors such as vulnerability severity, potential impact, and likelihood of occurrence.
- Explore emerging technologies and standards: The project should investigate the potential impact of emerging technologies, such as blockchain, artificial intelligence, and 5G networks, on IoT security. Additionally, examining the role of security standards and best practices, such as those developed by organizations like the Internet Engineering Task Force (IETF) and the National Institute of Standards and Technology (NIST), could provide valuable insights.
- Consider legal and regulatory aspects: The project could explore the legal and regulatory landscape surrounding IoT security in the UK, including existing laws, regulations, and industry standards. This can help identify potential gaps or areas for improvement in the regulatory framework to better address IoT security challenges.

G. Interpretation of Findings.

The findings of the research shed light on the current state of security within the IoT ecosystem in the UK. Using the Contiki operating system simulator and vulnerability assessment tools, several key vulnerabilities were identified in both smart cities and connected homes. These vulnerabilities ranged from insecure communication protocols to inadequate authentication mechanisms. The interpretation of these findings highlights the urgent need for robust security measures to protect against potential cyber threats in the IoT landscape.

H. Comparison with Existing Literature.

The findings of this study are consistent with existing literature on IoT security challenges. Previous research has identified similar vulnerabilities within the IoT ecosystem, emphasizing the need for improved security measures to mitigate risks. By comparing the findings of this study with existing literature, we gain a deeper understanding of the pervasive nature of IoT security vulnerabilities and the ongoing efforts to address them.

I. Implications for Security in IoT Ecosystem.

The implications of the research findings underscore the critical importance of enhancing security measures within the IoT ecosystem. In smart cities, where interconnected infrastructure controls essential services such as transportation and energy, vulnerabilities pose significant risks to public safety and national security. Similarly, in connected homes, where IoT devices collect sensitive personal data, security breaches can result in privacy violations and financial losses. Addressing these implications requires a multi-faceted approach, including the implementation of secure communication protocols, robust authentication mechanisms, and regular security updates.

J. Limitations and Challenges Encountered.

Despite the valuable insights gained from this research, several limitations and challenges were encountered. One limitation is the inherent complexity of the IoT ecosystem, which encompasses a wide range of devices and communication protocols. Additionally, the use of simulation tools, such as the Contiki operating system, may not fully replicate real-world scenarios, leading to potential discrepancies between simulated and actual vulnerabilities. Furthermore, the dynamic nature of cyber threats means that new vulnerabilities may emerge rapidly, necessitating ongoing monitoring and adaptation of security measures.

K. Future Research Directions.

Building upon the findings and limitations of this study, several avenues for future research emerge. Firstly, further investigation is needed to explore the effectiveness of specific security solutions in mitigating IoT vulnerabilities, such as intrusion detection systems and blockchain technology. Additionally, longitudinal studies can provide insights into the evolving nature of IoT security threats over time. Furthermore, research focusing on user awareness and education is essential to empower individuals to adopt secure practices when interacting with IoT devices. By addressing these research directions, we can advance our understanding of IoT security challenges and contribute to the development of robust security solutions.

CHAPTER SIX
CONCLUSION

A. Summary of Key Findings.

The conclusion begins by summarizing the main findings of the research, emphasizing the vulnerabilities identified within the IoT ecosystem in smart cities and connected homes. It highlights the prevalence of security risks such as data breaches, unauthorized access, and privacy concerns, underscoring the need for proactive security measures.

B. Recapitulation of Objectives.

Next, the conclusion revisits the objectives outlined at the beginning of the project, reflecting on the extent to which they have been achieved. It underscores the importance of understanding the security challenges facing the IoT ecosystem and acknowledges the contributions of the research towards advancing this understanding.

C. Report.

There are a few reasons why I choose to use Contiki OS instead of Kali Linux for research simulations related to securing the Internet of Things (IoT) ecosystem, particularly in the context of smart cities and connected homes even though that was my first OS I decided to use. Contiki OS is specifically designed for IoT devices and wireless sensor networks. It provides a lightweight and efficient platform for developing and testing IoT systems and protocols, making it more suitable for IoT-focused research than Kali Linux, which is primarily a penetration testing and security auditing platform.

Also, because Contiki is an open-source platform, you are free to change and adapt its code to suit your research needs. Because of this versatility, you can test and use various security protocols, processes, or algorithms that are tailored to your study goals.

While Kali Linux is a powerful tool for penetration testing and security auditing, it is primarily designed for traditional computing environments and may not provide the same level of simulation capabilities and IoT-specific features as Contiki OS.

D. Recommendations for Enhancing Security Measures.

Finally, the conclusion offers recommendations for enhancing security measures within the IoT ecosystem. This may include implementing robust encryption protocols, adopting secure authentication mechanisms, and promoting user awareness and education. It emphasizes the need for collaboration among stakeholders, including government agencies, industry partners, and the research community, to address IoT security challenges effectively.

REFERENCES

[1]. Alaba, F.A. *et al.* (2017) 'Internet of Things security: A survey', *Journal of Network and Computer Applications*, 88, pp.10-28.

[2]. Albreem, M.A. *et al. (*2021) 'Green Internet of Things (GIoT): Applications, practices, awareness, and challenges', IEEE Access, 9, pp.38833-38858.

[3]. Al-Fuqaha, A. *et al.* (2015) 'Internet of Things: A survey on enabling technologies, protocols, and applications', IEEE *Communications Surveys & Tutorials*, 17(4), pp.2347-2376.

[4]. Basir, N.*et al.* (2019) 'A systematic literature review of online vulnerability disclosure practices in the Internet of Things', *Journal of Cyber Security Technology*, 3(3), pp.143-161.

[5]. Bauer, H. *et al.* (2013) 'Lifecycle management for secure Internet of Things', *Proceedings of the* 2013 IEEE *International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, pp.786-793.

[6]. Blythe, J.M., Johnson, S.D. and Manning, M. (2020) 'What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices', Crime Science, 9(1), pp.1-9.

[7]. Boreli, R., *et al*. (2015) 'Network-level security and privacy control for smart-home IoT devices', Proceedings of the 11th IEEE *International Symposium on Intelligent Systems*.

[8]. Brown, A. (2021) 'IoT Security: Challenges and Solutions', *International Journal of Advanced Computer Science and Applications*, 12(3), pp.1-9.

[9]. Caron, X. *et al.* (2016) 'The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective', *Computer Law & Security Review*, 32(1), pp.4-15.

[10]. Carsten *et al.* (2011) 'Contiki: The Open Source OS for the Internet of Things', IEEE Communications Magazine.

[11]. Cavilla, H.A.L. (2009) Flexible Computing with Virtual Machines. University of Toronto (Canada).

[12]. Cervantes, C. *et al*. (2015) 'Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things', 2015 IFIP/IEEE *International Symposium on Integrated Network Management* (IM), pp.606-611. https://doi.org/10.1109/INM.2015.7140350

[13]. Cirne, A. *et al.* (2022) 'IoT security certifications: Challenges and potential approaches', Computers & Security, 116, pp.102669.

[14]. Deng, H., Li, W. and Agrawal, D.P. (2002) 'Routing security in wireless ad hoc networks', IEEE Communications Magazine, 40(10), pp.70-75. https://doi.org/10.1109/MCOM.2002.1039859

[15]. Desai, P., Sheth, A. and Anantharam, P. (2015) 'Semantic gateway as a service architecture for iot interoperability', Proceedings of the 2015 *IEEE international conference on mobile services*, pp.313-319.

[16]. Dunkels, A. *et al.* (2007) 'Run-Time Dynamic Linking for Reprogramming Wireless Sensor Networks', *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, pp.15–28. doi: 10.1145/1322263.1322266.

[17]. Dunkels, A., Gronvall, B. and Voigt, T. (2004) 'Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors', Proceedings of the 29th Annual IEEE *International Conference on Local Computer Networks*, pp.455–462. doi: 10.1109/LCN.2004.38.

[18]. Dunkels, A., Gronvall, B. and Voigt, T. (2004) 'Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors', *Conference on Local Computer Networks*.

[19]. Dunkels, A., Österlind, F. and He, Z. (2007) 'An adaptive communication-aware motion detection algorithm for wireless sensor networks', *Proceedings of the 5th international conference on Embedded networked sensor systems* - SenSys '07. doi: 10.1145/1322263.1322280.

[20]. Farooq, M.U. *et al.* (2015) 'A critical analysis on the security concerns of internet of things (IoT)', *International Journal of Computer Applications*, 111(7), pp.1-6.

[21]. Ge, M. *et al*. (2017) 'A framework for automating security analysis of the internet of things', *Proceedings of the Third ACM Workshop on Internet of Things Security and Privacy*, pp.39-53.

[22]. Gubbi, J. *et al*. (2013) 'Internet of Things (IoT): A vision, architectural elements, and future directions', *Future Generation Computer Systems*, 29(7), pp.1645-1660.

[23]. Johnson, R. (2019) 'Security and Privacy Issues in IoT Environments', *Security and Communication Networks*, 2019, pp.1-8.

[24]. Jones and associates (2020) 'Security Flaws in Smart Parking Systems: Manchester Teaches Us', *Proceedings of The International Conference on Cybersecurity* (ICC), 2020.

[25]. Jones, B. and Johnson, T. (2019) 'Internet of Things Security: Vulnerabilities, Challenges, and Solutions', *International Journal of Computer Networks and Applications*, 6(1), pp.15-25.

[26]. Jones, B. and Johnson, T. (2023) 'Internet of Things Security: Vulnerabilities, Challenges, and Solutions', *International Journal of Computer Networks and Applications*, 6(1), pp.15-25.

[27]. Jones, F., Shah, P. and Thomas, M. (2020) 'Security Vulnerabilities in Consumer IoT Devices', *Journal of Cybersecurity*, 6(2), pp.123-140.

[28]. Laukkarinen *et al*. (2017) 'Evaluating IoT Operating Systems for Resource Constrained Environments', *Conference on Open Systems.*

[29]. Lee, I. and Lee, K. (2015) 'The Internet of Things (IoT): Applications, investments, and challenges for enterprises', *Business Horizons*, 58(4), pp.431-440.

[30]. Lee, J. and Ahn, J. (2019) 'Security Threats and Issues in the Internet of Things for Smart Cities and Homes', *Journal of Information Security*, 23(2), pp.220-234.

[31]. Lee, J. (2022) 'Challenges in Securing Large-Scale IoT Ecosystems', *Computing and Network Security*, 29(5), pp.15-21.

[32]. Lom, M., Pribyl, O. and Svitek, M. (2016) 'Industry 4.0 as a part of smart cities', *Proceedings of the 2016 Smart Cities Symposium Prague* (SCSP), pp.1-6.

[33]. Mahmood, K. *et al* (2019) 'A survey on machine learning algorithms for Internet of Things: Applications and challenges', *Proceedings of the 2019 International Conference on Computing, Mathematics and Engineering Technologies* (iCoMET), pp.1-6.

[34]. Majumder, S. *et al*. (2017) 'Smart homes for elderly healthcare-Recent advances and research challenges', Sensors, 17(11), p.2496.

[35]. Maple, C. (2017) 'Security and privacy in the internet of things', *Journal of Cyber Policy*, 2(2), pp.155-184.

[36]. Mouradian, A. *et al.* (2014) 'A comprehensive survey on fog computing: State-of-the-art and research challenges', IEEE Communications Surveys & Tutorials, 17(1), pp.98-149.

[37]. Obaidat, M.A. *et al.* (2020) 'A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures', Computers, 9(2), p.44.

[38]. Orthacker, C*et al.* (2017) 'Secure and practical communications from embedded IoT devices to cloud-based services', Proceedings of the 2017 IEEE *European Symposium on Security and Privacy Workshops* (EuroS&PW), pp.281-289.

[39]. Österlind, F. *et al*. (2006) 'Cross-Level Sensor Network Simulation with COOJA', Proceedings of the 31st IEEE *Conference on Local Computer Networks*, pp.641–648. doi: 10.1109/LCN.2006.322172.

[40]. Osterlind, F. *et al.* (2006) 'Cross-level sensor network simulation with cooja', Proceedings of the 31st IEEE *conference on local computer networks*, pp.641-648.

[41]. Pearce, M., Zeadally, S. and Hunt, R. (2013) 'Virtualization: Issues, security threats, and solutions', ACM Computing Surveys (CSUR), 45(2), pp.1-39.

[42]. Perera, C. *et al.* (2014) 'A survey on internet of things from industrial market perspective', IEEE Access, 2, pp.1660-1679.

[43]. Pirbhulal, S. *et al*. (2017) 'A novel secure IoT-based smart home automation system using a wireless sensor network', Sensors, 17(1), p.69. doi: 10.3390/s17010069.

[44]. Raza, S., Wallgren, L. and Voigt, T. (2013) 'SVELTE: Real-time intrusion detection in the Internet of Things', Ad hoc networks, 11(8), pp.2661-2674.

[45]. Roman, R., Zhou, J. and Lopez, J. (2013) 'On the features and challenges of security and privacy in distributed internet of things', Computer Networks, 57(10), pp.2266-2279. doi: 10.1016/j.comnet.2012.12.018.

[46]. Riahi, A. *et al.* (2013) 'A systemic and cognitive approach for IoT security', Proceedings of the 2013 *International Conference on Computing, Networking and Communications* (ICNC), pp.183-188.

[47]. Schneier, B. (2017) 'Security and survival in a hyperconnected world: Click here to kill everybody', W.W. Norton & Company, New York.

[48]. Shah, G.A., Gungor, V.C. and Akan, O.B. (2013) 'A cross-layer QoS-aware communication framework in cognitive radio sensor networks for smart grid applications', IEEE *Transactions on Industrial Informatics*, 9(3), pp.1477-1485.

[49]. Sharma, D.K. *et al.* (2022) 'Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems',. Elsevier BV.

[50]. Sicari, S. *et al*. (2015) 'Security, privacy and trust in Internet of Things: The road ahead', Computer Networks, 76, pp.146-164.

[51]. Sisinni, E. *et al.* (2018) 'Industrial internet of things: Challenges, opportunities, and directions', IEEE *Transactions on Industrial Informatics*, 14(11), pp.4724-4734.

[52]. Smith, A. (2018) 'Assessing IoT Security Risks in Public Wi-Fi Networks: A Case Study of London', *Journal of Cybersecurity*, 3(1), pp.45-56.

[53]. Smith, A. (2020) 'Security Challenges in the Expanding Internet of Things Ecosystem', *Journal of Cybersecurity*, 6(4), pp.213-226.

[54]. Smith, A. (2021) 'The Increasing Cyber Risks in an IoT World', *Information Security Review*, 17(8), pp.13-19.

[55]. Smith, J. and Patel, M. (2019) 'Addressing Resource Constraints in IoT Security: Challenges for UK SMEs', *Proceedings of the European Conference on Cybersecurity* (ECC), 2019.

[56]. Stadler, M. and Del Giorgio, P.A. (2022) 'Terrestrial connectivity, upstream aquatic history and seasonality shape bacterial community assembly within a large boreal aquatic network', The *ISME Journal*, 16(4), pp.937-947.

[57]. Suo, H. *et al*. (2012) 'Security in the internet of things: a review', Proceedings of the 2012 *international conference on computer science and electronics engineering*, 3, pp.648-651. doi: 10.1109/ICCSEE.2012.373.

[58]. Suo, H. *et al*. (2012) 'Security in the internet of things: A review', Proceedings of the 2012 *International Conference on Computer Science*.

[59]. Sivaraman, V. *et al.* (2015) 'Network-level security and privacy control for smart-home IoT devices', Proceedings of the 2015 IEEE *11th International Conference on Wireless and Mobile Computing, Networking and Communications* (WiMob), pp.163-167.

[60]. Taylor, L. (2021) 'Physical Security Vulnerabilities in IoT Devices', *Journal of Information Security Research*, 5(1), pp.23-35.

[61]. Vermesan, O. and Friess, P. (2013) 'Internet of Things: Converging technologies for smart environments and integrated ecosystems'. River Publishers.

[62]. Wallgren, L., Raza, S. and Voigt, T. (2013) 'Routing Attacks and Countermeasures in the RPL-Based Internet of Things', *International Journal of Distributed Sensor Networks*, 9(8), p.794326. https://doi.org/10.1155/2013/794326

[63]. White, M. and Williams, S. (2020) 'Encryption Practices and Challenges in IoT Communications', IEEE *Transactions on Dependable and Secure Computing*, 17(4), pp.726-739.

[64]. Wolfert, S. *et al*. (2017) 'Big data in smart farming–a review', Agricultural Systems, 153, pp.69-80.

[65]. Wortmann, F. and Flüchter, K. (2015) 'Internet of things: technology and value added', *Business & information systems engineering*, 57, pp.221-224.

[66]. Xu, L.D., He, W. and Li, S. (2014) 'Internet of Things in industries: A survey', IEEE *Transactions on Industrial Informatics*, 10(4), pp.2233-2243.

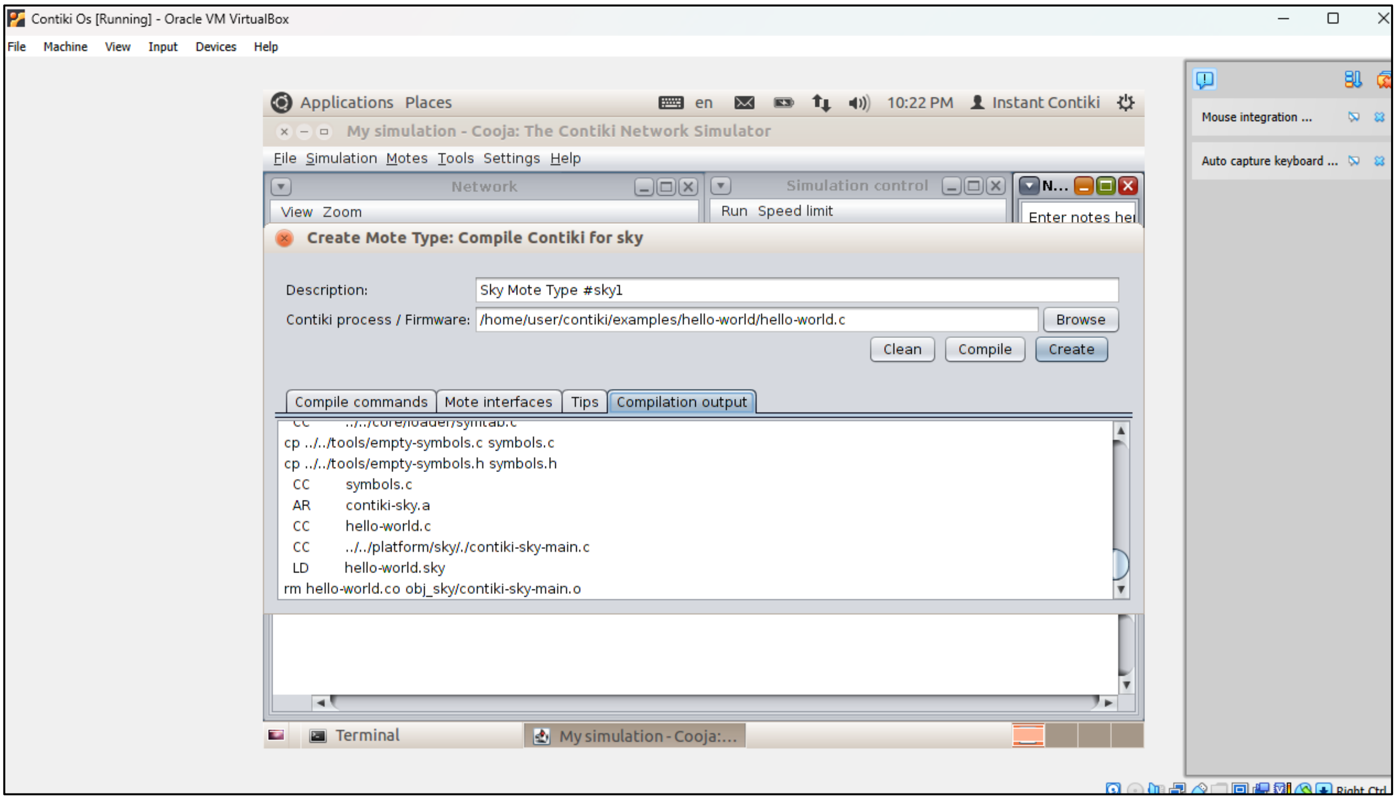
[67]. Zanella, A. *et al*. (2014) 'Internet of Things for smart cities', IEEE *Internet of Things Journal*, 1(1), pp.22-32.

[68]. Zarpelão, B.B. *et al*. (2017) 'A survey of intrusion detection in Internet of Things', *Journal of Network and Computer Applications*, 84, pp.25-37.

[69]. Zhu, Q. *et al*. (2010) 'IoT gateway: Bridgingwireless sensor networks into internet of things', Proceedings of the 2010 IEEE/IFIP *International Conference on Embedded and Ubiquitous Computing*, pp.347-352. doi: 10.1109/EUC.2010.58.

APPENDICES

APPENDIX 1: COMPILED MOTE FOR COLLECTING VIEWS

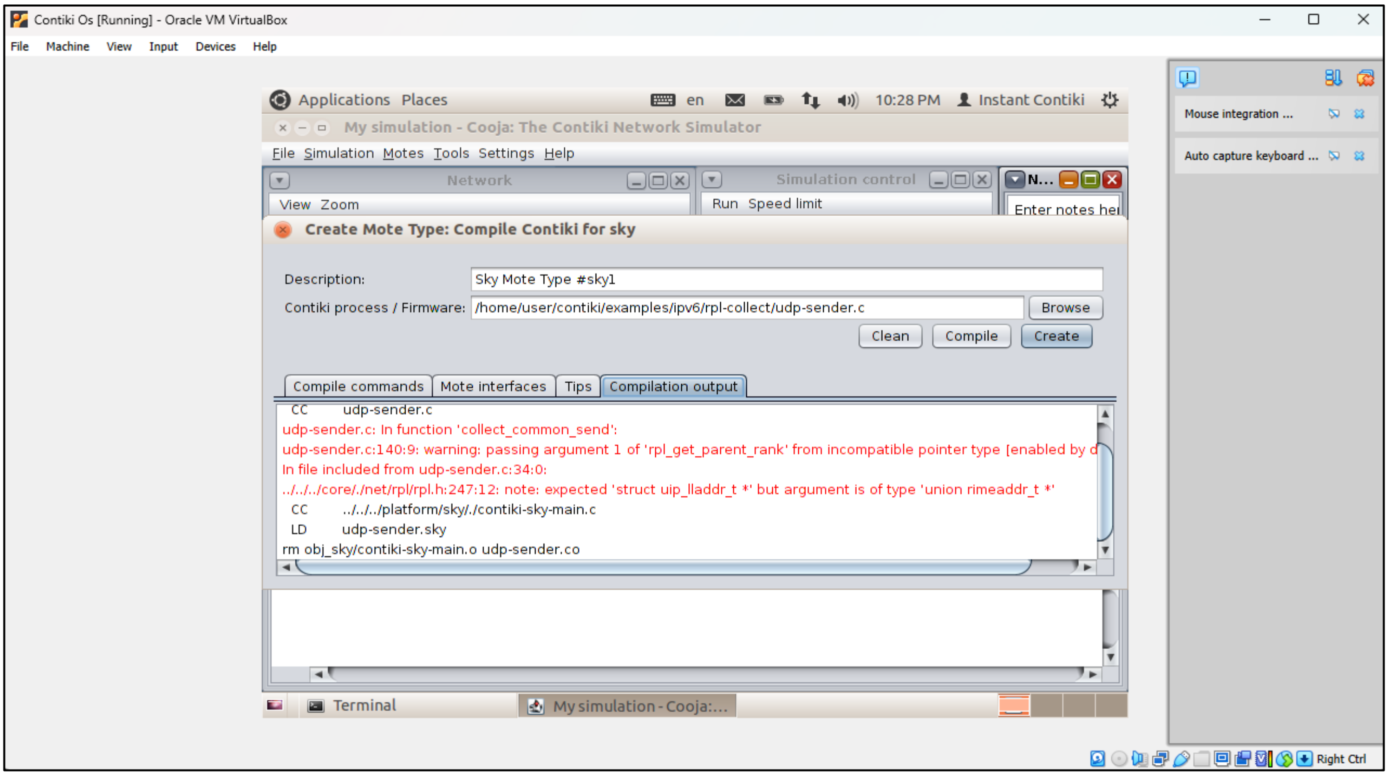

Contiki Os [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
en
10:22 PM
Instant Contiki
My simulation - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Network
View Zoom
Simulation control
Run Speed limit
N...
Enter notes her
Create Mote Type: Compile Contiki for sky
Browse
Clean
Compile
Create
Compile commands
Mote interfaces
Tips
Compilation output
Terminal
My simulation - Cooja:...
Mouse integration ...
Auto capture keyboard ...
Right Ctrl

Description: Sky Mote Type #sky1

Contiki process / Firmware: /home/user/contiki/examples/hello-world/hello-world.c

```
  CC       ../../core/loader/symtab.c
cp ../../tools/empty-symbols.c symbols.c
cp ../../tools/empty-symbols.h symbols.h
  CC       symbols.c
  AR       contiki-sky.a
  CC       hello-world.c
  CC       ../../platform/sky/./contiki-sky-main.c
  LD       hello-world.sky
rm hello-world.co obj_sky/contiki-sky-main.o
```

APPENDIX 1: COMPILED MOTE FOR AN ATTACK

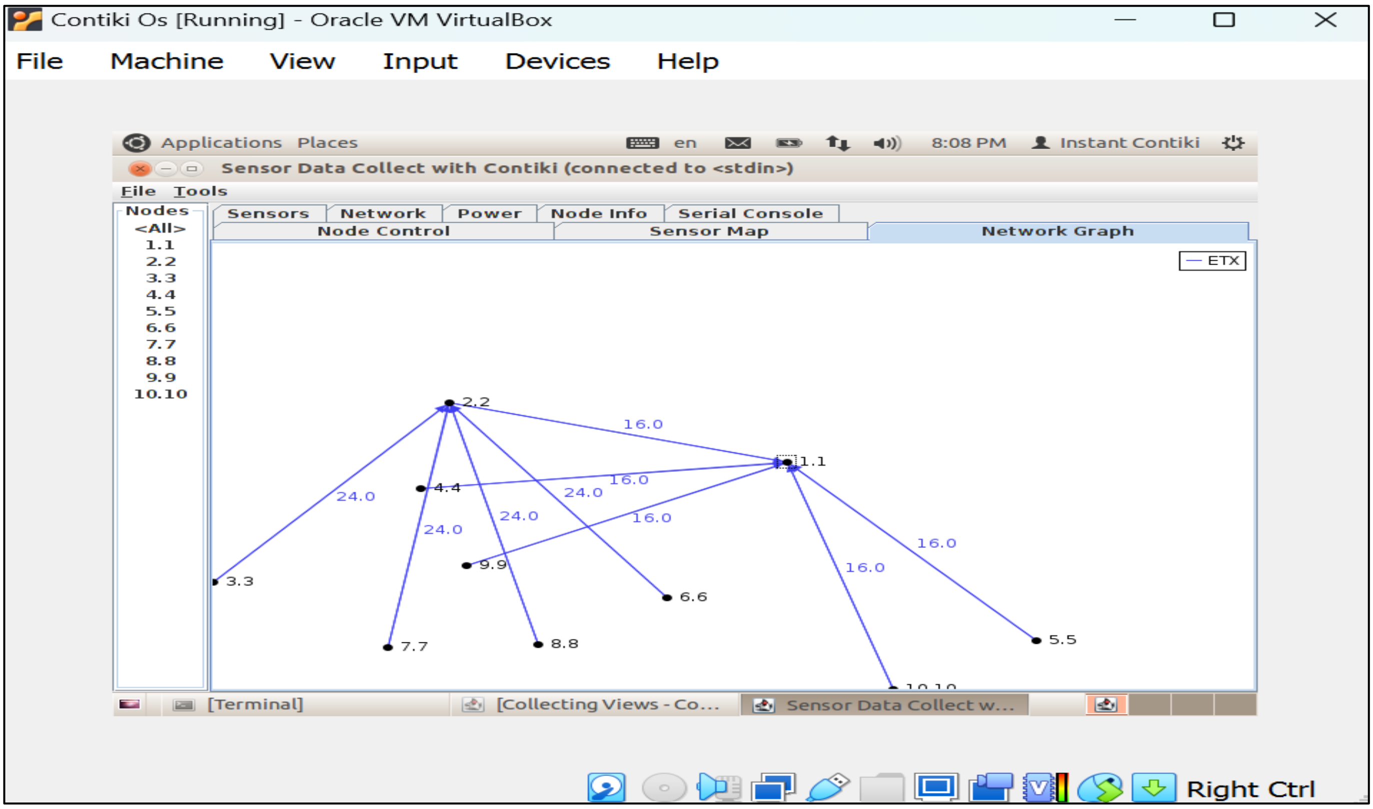

Contiki Os [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
en
10:28 PM
Instant Contiki
My simulation - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Network
View Zoom
Simulation control
Run Speed limit
N...
Enter notes her
Create Mote Type: Compile Contiki for sky
Browse
Clean
Compile
Create
Compile commands
Mote interfaces
Tips
Compilation output
Terminal
My simulation - Cooja:...
Mouse integration ...
Auto capture keyboard ...
Right Ctrl

Description: Sky Mote Type #sky1

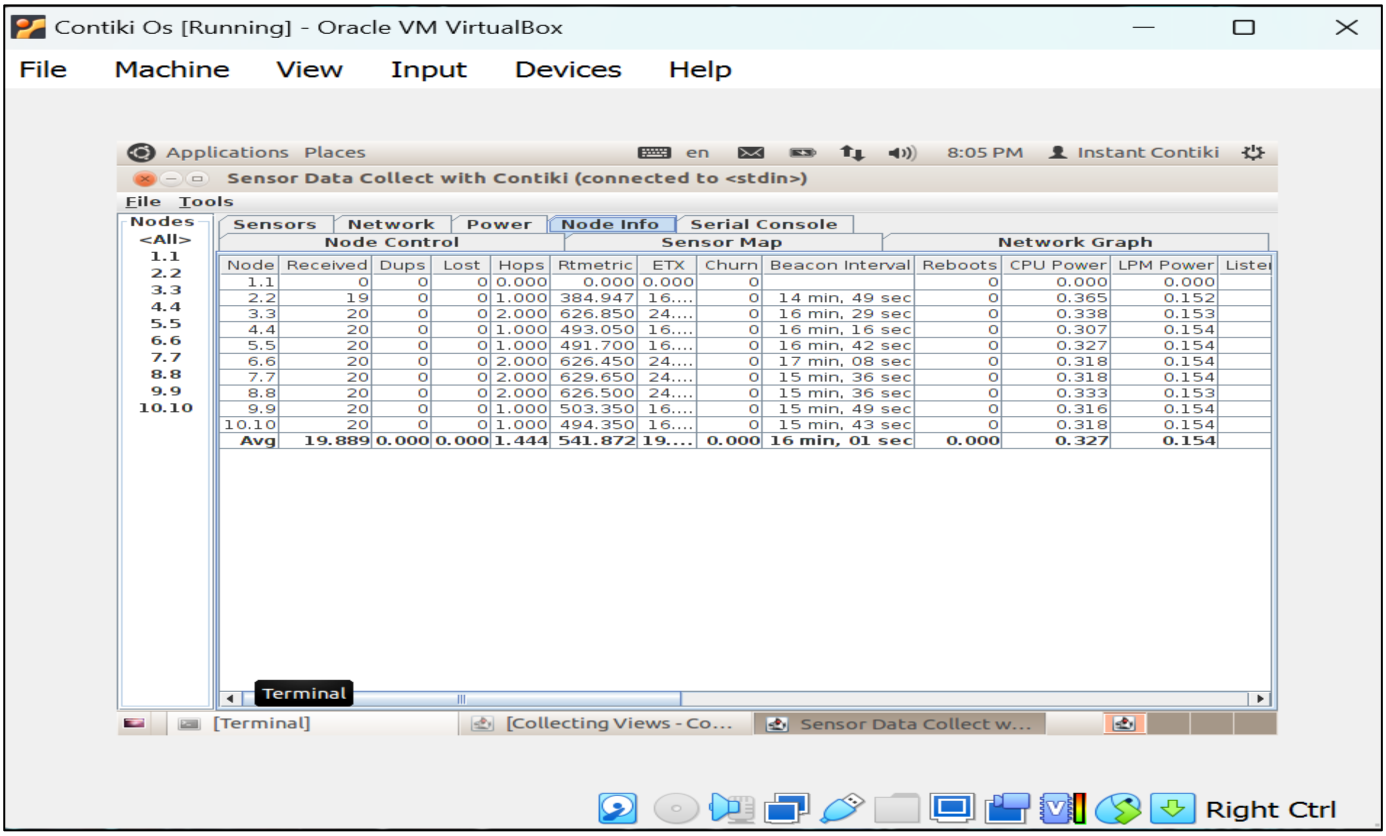
Contiki process / Firmware: /home/user/contiki/examples/ipv6/rpl-collect/udp-sender.c

```
  CC       udp-sender.c
udp-sender.c: In function 'collect_common_send':
udp-sender.c:140:9: warning: passing argument 1 of 'rpl_get_parent_rank' from incompatible pointer type [enabled by d
In file included from udp-sender.c:34:0:
../../../core/./net/rpl/rpl.h:247:12: note: expected 'struct uip_lladdr_t *' but argument is of type 'union rimeaddr_t *'
  CC       ../../../platform/sky/./contiki-sky-main.c
  LD       udp-sender.sky
rm obj_sky/contiki-sky-main.o udp-sender.co
```

APPENDIX 3: NETWORK GRAPH



APPENDIX 4: NODES INFORMATION



Node	Received	Dups	Lost	Hops	Rtmetric	ETX	Churn	Beacon Interval	Reboots	CPU Power	LPM Power	Lister
1.1	0	0	0	0.000	0.000	0.000	0		0	0.000	0.000	
2.2	19	0	0	1.000	384.947	16....	0	14 min, 49 sec	0	0.365	0.152	
3.3	20	0	0	2.000	626.850	24....	0	16 min, 29 sec	0	0.338	0.153	
4.4	20	0	0	1.000	493.050	16....	0	16 min, 16 sec	0	0.307	0.154	
5.5	20	0	0	1.000	491.700	16....	0	16 min, 42 sec	0	0.327	0.154	
6.6	20	0	0	2.000	626.450	24....	0	17 min, 08 sec	0	0.318	0.154	
7.7	20	0	0	2.000	629.650	24....	0	15 min, 36 sec	0	0.318	0.154	
8.8	20	0	0	2.000	626.500	24....	0	15 min, 36 sec	0	0.333	0.153	
9.9	20	0	0	1.000	503.350	16....	0	15 min, 49 sec	0	0.316	0.154	
10.10	20	0	0	1.000	494.350	16....	0	15 min, 43 sec	0	0.318	0.154	
Avg	**19.889**	**0.000**	**0.000**	**1.444**	**541.872**	**19....**	**0.000**	**16 min, 01 sec**	**0.000**	**0.327**	**0.154**	