**Chapter 1**

**INTRODUCTION AND BACKGROUND**

Internet of Things devices have become increasingly prevalent in various domains, including smart homes, healthcare, transportation, and industrial automation. As the number of IoT devices continues to grow, so does the potential for security challenges. One of the primary concerns in IoT security is the vulnerability of routing protocols to modification and manipulation attacks. Internet of Things devices have become increasingly prevalent in various domains, including smart homes, healthcare, transportation, and industrial automation. As the number of IoT devices continues to grow, so does the potential for security challenges. One of the primary concerns in IoT security is the vulnerability of routing protocols to modification and manipulation attacks. Understanding the Impact of Routing Protocol Vulnerabilities. Routing protocols play a critical role in IoT networks by determining the path for packet transmission. However, their susceptibility to modification and manipulation attacks can have far-reaching consequences. These attacks can lead to unauthorized access to sensitive data, disruption of critical services, and even physical harm in certain applications such as healthcare and industrial automation .

* 1. **Statement of Problem Area**

The existing routing protocols used in IoT networks are vulnerable to manipulation and modification attacks, which can compromise the integrity and confidentiality of the data being transmitted. These attacks can lead to unauthorized access, data tampering, and disruptions in the IoT network. The current state of IoT routing protocols reveals a significant vulnerability to various forms of attacks, particularly modification and manipulation attacks. Many existing routing protocols lack robust security measures to protect against such attacks, leaving IoT devices and networks exposed to potential breaches and disruptions. Addressing these vulnerabilities is critical for ensuring the integrity and reliability of IoT networks. Modification and manipulation attacks can lead to unauthorized access, data breaches, and disruptions in critical IoT services. As a result, the development of a dedicated routing module to mitigate these attacks is essential for strengthening IoT security.

* 1. **Literature Survey**

**[1]“Secure routing protocols for IoT networks: a comprehensive survey"**

**Abstract:**

IoT devices are the integral part of this century. It is estimated that more than 40 billion devices are connected and this number is increasing exponentially due to the heavy dependency of IoT with every field. These devices collect their concerned data through their sensors and allow the business to work smoothly. The routing protocols used by these IoT devices play a vital role in delivery of collected data packets. Routing protocols governs several factors among which security as well as fast delivery are the major ones. Several researchers have proposed various routing protocols that can handle the secure as well as efficient source to destination route for the packets. But still due to various shortcomings in the area of security and fast delivery of packets there is need for better as well as more optimized routing protocol. Our paper aims to review some of the latest research paper published in this area so that the researchers can get to know about the latest work in this field and carry on with their research.

**Publisher:** A. Ullah

**Published in:** International Journal of Innovative Research in Engineering & Management (IJIREM) ISSN: 2350-0557, Volume-9, Issue-5, October 2022.

# [2]“A Security Routing Protocol for Internet of Things Based on RPL”

**Abstract:**

RPL is a lightweight IPv6 network routing protocol specifically designed by IETF, which can make full use of the energy of intelligent devices and compute the resource to build the flexible topological structure. The routing protocol establishes a hierarchical clustering network topology, the intelligent device of the network establishes the backup path in different clusters during the route discovery phase, enable backup paths to ensure data routing when a network is compromised. Setting up a test prototype network, simulating some attacks against the routing protocols in the network. The test results show that the M-RPL network can effectively resist the routing attacks. M-RPL provides a solution to ensure the Internet of Things (IoT) security.

# Publisher: [Guojun Ma](https://ieeexplore.ieee.org/author/37531491600), [Qingqi Pei](https://ieeexplore.ieee.org/author/37294380000).

**Published in**: IEEE[2017 International Conference on Networking and Network Applications (NaNA)](https://ieeexplore.ieee.org/xpl/conhome/8246105/proceeding).

**[3]"A survey of security in wireless sensor networks"**

**Abstract:**

# The security in wireless sensor networks (WSNS) is a very important issue. These networks may be exposed it different attacks. With this in mind, researchers propose in this area variety of security techniques for this purpose, and this article describes security in wireless sensor networks. Discussed threats and attacks of wireless sensor networks. The article also aims to provide the basic information related to determining essential requirements for the protection WSNs. Lastly, we mention some security mechanisms against these threats and attacks in Wireless Sensor Network.

**Publisher:** Fatimah Khalil Aljwari, Hajer Abdullah Alwadei and Aseel Abdullah Alfaidi

# Published in: International Journal of Computer Science & Information Technology (IJCSIT) Vol 14, No 3, June 2022.

# [4]"Secure routing in the Internet of Things: a survey"

**Abstract:**

# The [Internet of Things](https://www.sciencedirect.com/topics/computer-science/internet-of-things) (IoT) could be described as the pervasive and global network which aids and provides a system for the monitoring and control of the physical world through the collection, processing and analysis of generated data by IoT sensor devices. It is projected that by 2020 the number of connected devices is estimated to grow exponentially to 50 billion. The main drivers for this growth are our everyday devices such as cars, refrigerators, fans, lights, mobile phones and other operational technologies including the manufacturing infrastructures which are now becoming [connected systems](https://www.sciencedirect.com/topics/engineering/connected-system) across the world. It is apparent that security will pose a fundamental enabling factor for the successful deployment and use of most IoT applications and in particular secure routing among IoT [sensor nodes](https://www.sciencedirect.com/topics/engineering/sensor-node) thus, mechanisms need to be designed to provide secure routing communications for devices enabled by the IoT technology. This survey analyzes existing routing protocols and mechanisms to secure routing communications in IoT, as well as the [open research](https://www.sciencedirect.com/topics/computer-science/open-research) issues.

# Publisher: David Airehrour, Jairo Gutierrez, Sayan Kumar Ray.

# Published in: journal of network and computer applications.

* 1. **Purpose**

**1.3.1 Purpose of the Project**

The project's purpose extends to maintaining network integrity, reliability, and performance despite the introduction of advanced security features. By implementing robust authentication, anomaly detection, and secure message forwarding within the routing protocol, the module aims to prevent potential attackers from exploiting RPL vulnerabilities. The design considerations must ensure that the security enhancements do not impede the network's functionality or efficiency, allowing for a seamless integration with existing IoT systems and ensuring interoperability. Overall, the purpose is to balance enhanced security measures with the limited resources available in IoT networks, ensuring that the protection against routing attacks is stringent, yet practical for the vast and diverse landscape of IoT applications.

**1.3.2 Objective of the Project**

**The Prime Objectives of the project are as follows:**

* Assess the current vulnerabilities of RPL to identify how modification and manipulation attacks can occur, focusing on attack vectors such as rank attacks, sybil attacks, and others that could disrupt the network.
* Designing a Routing Module for IoT Routing Protocols to Address Modification and Manipulation Attacks using standardized IPV6 Routing Protocol for Low-Power and Lossy.
* Integrate with RPL: Seamlessly integrate the secure mechanisms into the standard RPL framework so that the module enhances the existing routing protocol without requiring significant changes to the protocol itself or to the application layers.
* Develop Authentication and Authorization Protocols: Design robust authentication and authorization procedures that can securely manage the addition and removal of nodes within the network, thereby preventing unauthorized access and control.
* Facilitate Intrusion Detection and Response: Embed intrusion detection capabilities within the module that can recognize signs of modification or manipulation and respond appropriately to mitigate any threats.
* Validate and Test: Validate the module's effectiveness through rigorous testing in simulated and real-world scenarios to ensure it adequately addresses the attacks without negatively impacting the protocol's original functionality.

**1.3.3 Justification of the Project**

The urgency to fortify Internet of Things networks against routing attacks is underscored by the growing dependence of our societal infrastructure on IoT technology. The standard routing protocol for IoT, RPL, is tailored to the unique network and device constraints within these systems but remains vulnerable to sophisticated modification and manipulation attacks. These attacks not only compromise the confidentiality, integrity, and availability of data but can also result in the disruption of critical IoT services in smart cities, healthcare monitoring, industrial control systems, and more. Given the potential catastrophic outcomes of such disruptions, investing in a dedicated routing module to bolster security against such threats is both necessary and timely. It reinforces the trust in IoT infrastructure by mitigating risks and ensuring reliable data transmission across nodes.

Furthermore, the absence of such security measures can lead to larger systemic risks and hamper the adoption of IoT technologies. As IoT networks are typically composed of a multitude of resource-constrained devices, traditional security solutions are often impractical due to their computational overhead. This project aims to develop solutions that conform to the resource limitations of IoT devices, ensuring that security does not come at the expense of the network's operational capabilities.

**Chapter 2**

**SYSTEM FUNCTIONAL SPECIFICATION**

The purpose of this software requirements specification is to define the specifications for designing a routing module for IoT that addresses manipulation and modification attacks. The IoT Routing Module is a critical component in ensuring the secure and efficient transfer of data in an IoT network. The module is designed to prevent manipulation and modification attacks on the data as it travels through the network. This document will outline the functional and non-functional requirements of the IoT Routing Module, providing a clear understanding of its scope and capabilities. Internet of Things devices have become increasingly prevalent in various domains, including smart homes, healthcare, transportation, and industrial automation. As the number of IoT devices continues to grow, so does the potential for security challenges. One of the primary concerns in IoT security is the vulnerability of routing protocols to modification and manipulation attacks [1].

Routing protocols play a critical role in IoT networks by determining the path for packet transmission. However, their susceptibility to modification and manipulation attacks can have far-reaching consequences. These attacks can lead to unauthorized access to sensitive data, disruption of critical services, and even physical harm in certain applications such as healthcare and industrial automation [2]. Furthermore, the distributed and resource-constrained nature of IoT devices exacerbates the challenges of securing routing protocols. Traditional security mechanisms may not be sufficient to address the unique requirements of IoT environments, necessitating the development of specialized solutions tailored to IoT routing protocols.

The current state of IoT routing protocols reveals a significant vulnerability to various forms of attacks, particularly modification and manipulation attacks. Many existing routing protocols lack robust security measures to protect against such attacks, leaving IoT devices and networks exposed to potential breaches and disruptions. Addressing these vulnerabilities is critical for ensuring the integrity and reliability of IoT networks. Modification and manipulation attacks can lead to unauthorized access, data breaches, and disruptions in critical IoT services. As a result, the development of a dedicated routing module to mitigate these attacks is essential for strengthening IoT security. In this project, we will explore the design and implementation of a routing module specifically tailored to address these security concerns in IoT environments.

**2.1 Function Performed**

The IoT Routing Module will be responsible for inspecting and securely routing data packets within the IoT network. It will implement validation and authentication mechanisms to verify the integrity of the data and ensure its secure delivery to the intended recipients [5]. To address the vulnerabilities in existing routing protocols, the IoT Routing Module will implement Lamport's Keyed Hashing Chain Scheme, providing a secure and efficient method for data transmission within IoT networks. This scheme will help protect against manipulation and modification attacks, ensuring the integrity and confidentiality of the data.

Within the scope of the project to design a routing module for IoT routing protocols, the primary function is to secure the data communication between interconnected IoT devices against modification and manipulation attacks. The module operates by implementing advanced cryptographic methods, trust-based systems, or anomaly detection techniques that work seamlessly with the RPL standards to authenticate and validate data packets as they traverse the network. The function encompasses the prevention of unauthorized data alteration, the identification of malicious nodes attempting to tamper with the routing information, and the assurance of the integrity and authenticity of the messages communicated between devices.

Additionally, the routing module is tasked with maintaining the efficiency and reliability of the network, despite the added security layers. It performs the function of monitoring network traffic to detect any anomalies or patterns indicative of routing attacks, all while ensuring that the additional security measures do not introduce significant overhead that could degrade network performance. The module is designed to dynamically adapt to network changes, such as the addition or removal of nodes, ensuring that the network is resilient to attacks even as its topology evolves. Overall, the module functions as a guardian of data flow within IoT networks, reconciling the seemingly competing demands of advanced security and operational efficiency. In RPL networks (IPv6 Routing Protocol for Low-Power and Lossy Networks), authentication of messages can be validated using a hash-based chaining mechanism, although this is not part of the standard RPL specification.

1. **Initial Setup**: Each node in the RPL network is preloaded with a secret key unique to that node. This key is used to generate a cryptographic hash chain, which is a sequence of hash values where each value is the hash of the previous value in the sequence.
2. **Hash Chain Generation**: Starting from a random initial value, the node repeatedly applies the hash function to generate a sequence of hash values (the hash chain). The final result is known as the anchor of the chain, and it can be securely distributed or made public in a trustworthy manner.
3. **Authentication Process**:
   * When a node sends a message, it includes in the message the next unused hash value from its hash chain.
   * Along with this, it attaches a Message Integrity Code, computed using the secret key and the content of the message, to guarantee the integrity and prove the authenticity of the message.
4. **Verification**:
   * Upon receiving a message, the neighbouring node checks the included hash value against its own computed hash value (assuming that it has received the anchor or previous valid hashes from the same chain).
   * If the hash value included in the message can be hashed to reach a known valid hash in the receiver’s computed chain, the message is considered authentic.
   * The receiver then verifies the MIC using the same hashing mechanism. If the MIC matches, the message integrity is confirmed.
5. **Moving to Next Hash Value**: Once a hash value is used for message authentication, the next value in the chain is used for subsequent messages. This one-time-use approach for hash values helps in preventing replay attacks.
   1. **User Input/Output Specification**

**User Input Specification:**

* Message M: The message that needs to be authenticated by the RPL nodes.
* Key: The secret key obtained from the root/gateway of the IoT network.
* Node Identity: The identity of the node participating in the routing process.

**User Output Specification:**

* Authentication Result: Indicates whether the message M is authenticated or not.
* Authentication Ticket: The generated authentication ticket used for validation.
* Routing Decision: If applicable, the routing decision made based on the authenticated message.
  1. **External and Internal Limitations and Restrictions**

**External Limitations and Restrictions:**

* **Resource Constraints**: IoT devices typically have limited computational power, memory, and energy resources. Your methodology should be lightweight and efficient to operate within these constraints.
* **Network Dynamics:** IoT networks can be dynamic, with nodes joining, leaving, and moving frequently. Your methodology should be adaptable to such changes without causing significant overhead.
* **Interoperability:** Since IoT environments may consist of heterogeneous devices from different manufacturers, ensuring interoperability and compatibility with existing RPL implementations or other routing protocols is crucial.
* **Adversarial Environment:** IoT networks may be susceptible to various attacks and security threats. Your methodology should be resilient to attacks such as message spoofing, replay attacks, and node compromise.

**Internal Limitations and Restrictions:**

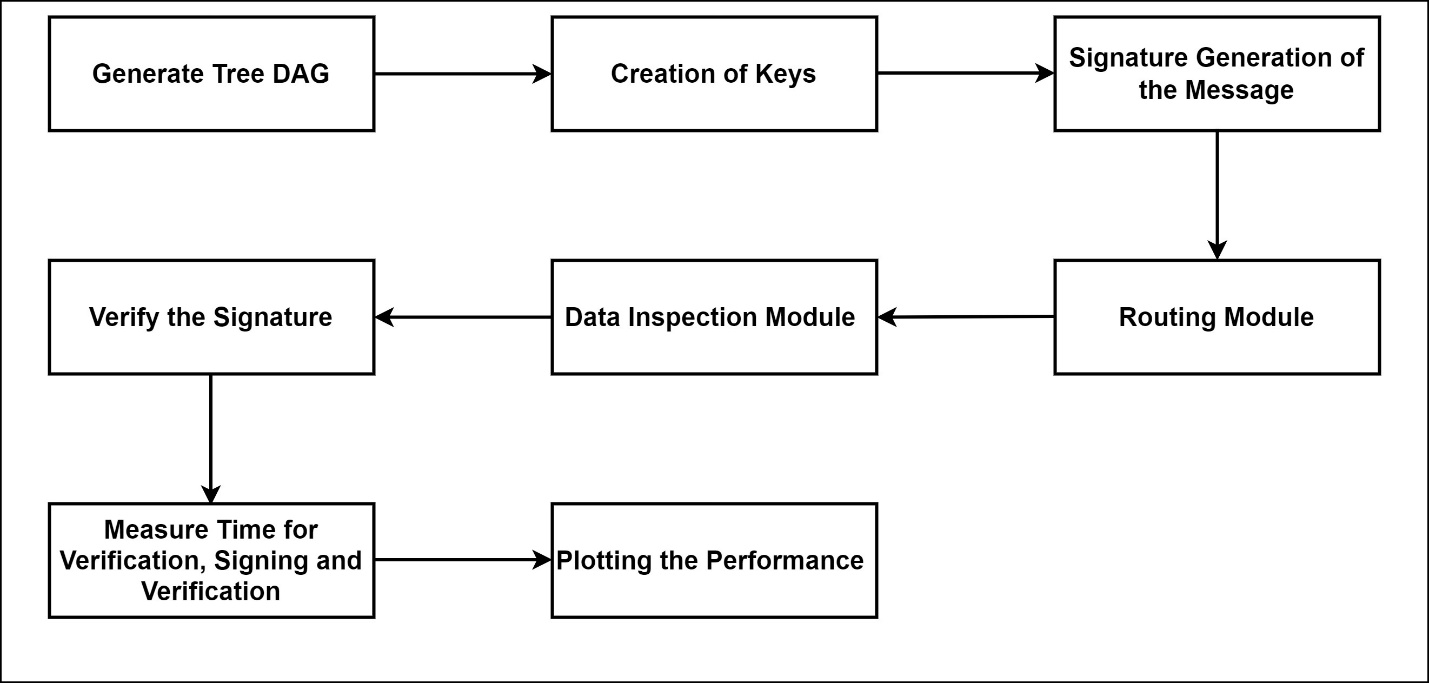
* **Key Management:** The security of your methodology relies on the secure distribution and management of keys. Developing an efficient and secure key management scheme is essential to prevent unauthorized access and key compromise.
* **Scalability:** As the IoT network grows in size, the scalability of your methodology becomes crucial. Ensure that your approach can handle large-scale deployments without sacrificing performance or security.
* **Message Overhead:** Adding security mechanisms to RPL messages may increase message overhead, leading to higher energy consumption and reduced network efficiency. Balancing security requirements with resource constraints is essential to minimize overhead.
* **False Positives/Negatives:** The authentication mechanism should accurately distinguish between legitimate and malicious messages. Minimizing false positives (legitimate messages identified as malicious) and false negatives (malicious messages identified as legitimate) is important to maintain network reliability and security.

**Chapter 3**

**SYSTEM DESIGN**

**3.1 Block diagram**

The system architecture shown in figure 3.1, for the IoT Routing Module consists of several key components that work together to ensure secure and efficient data transfer within the IoT network



**Figure 3.1: Block diagram**

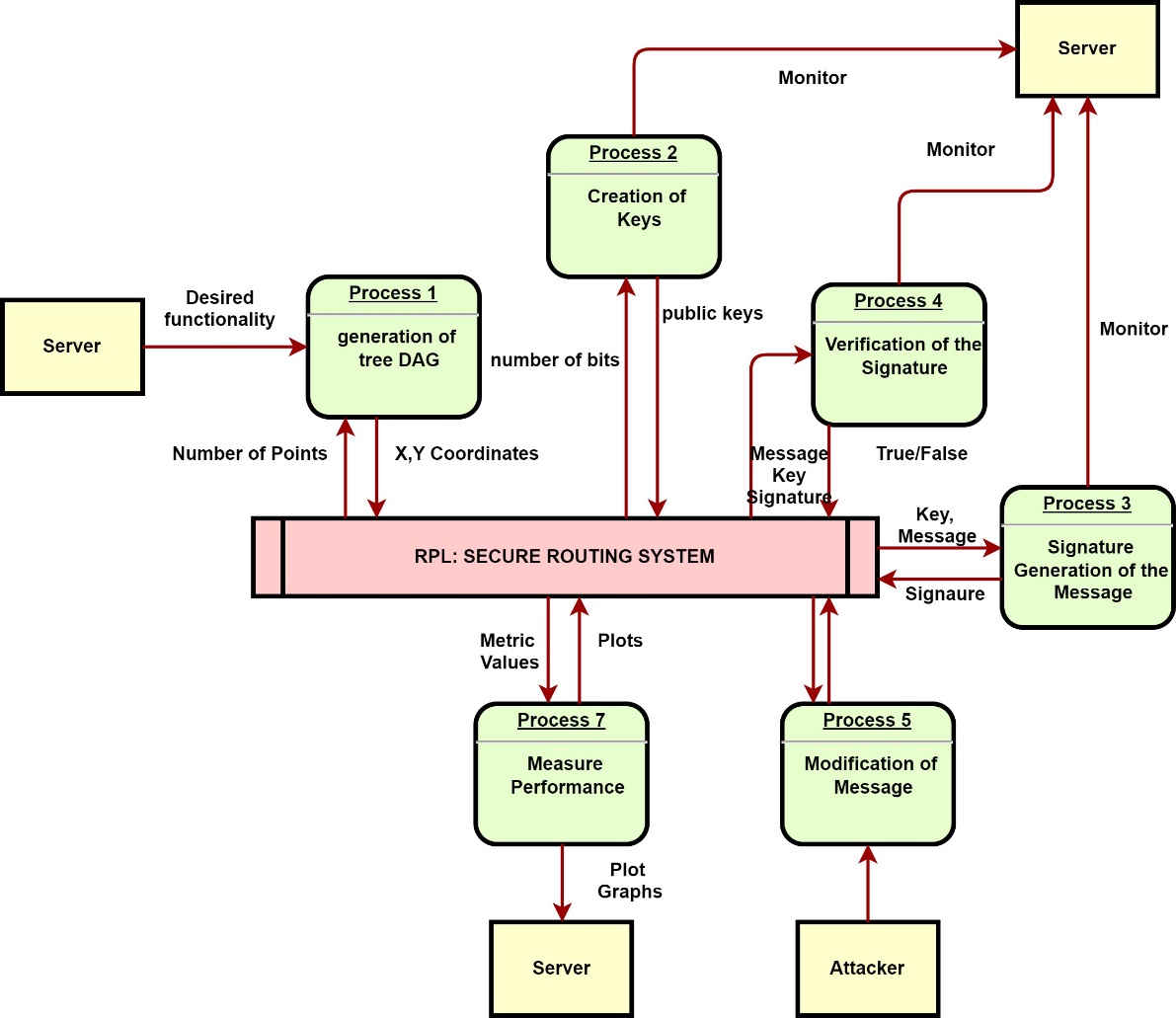
The first component of the system architecture is the Tree DAG generation module. This module is responsible for generating a secure and efficient tree Directed Acyclic Graph (DAG) structure that represents the topology of the IoT network. This structure will be used for routing decisions and to ensure that data is correctly transmitted between nodes in the network. The Tree DAG generation module plays a crucial role in creating a secure and efficient representation of the IoT network's topology. By generating a structured tree DAG, the module facilitates optimized routing decisions and ensures accurate data transmission between nodes in the network. This component forms the foundation for establishing a reliable communication framework within the IoT environment, enabling the routing module to effectively navigate the network and securely transfer data packets. Routing Module: The core component of the system, the Routing Module is responsible for inspecting and securely routing data packets within the IoT network. It implements validation, authentication, and encryption mechanisms to ensure the integrity and secure delivery of data. Data Inspection Unit: This component is responsible for inspecting incoming data packets to detect any signs of tampering or unauthorized modifications. It works in conjunction with the Routing Module to ensure the integrity of the data.

The Key Generation module assumes a critical role in enhancing the security of data transmission within the IoT network. By creating unique cryptographic keys tailored for encryption and decryption purposes, this component strengthens the confidentiality of data exchanges, establishing a fortified layer of protection against unauthorized access and data breaches. The generation of distinct cryptographic keys ensures that sensitive information remains secure and uncompromised, fortifying the underlying security framework of the IoT routing module.

The IoT Routing Module utilizes Lamport's Keyed Hashing Chain scheme for message authentication and verification. This scheme generates a digital signature for each message using a cryptographic hash function and a secret key. This signature serves as a unique identifier of the message, ensuring its integrity and authenticity. The IoT Routing Module will be employed in various scenarios to facilitate secure data transfer within IoT networks. One such use case involves the exchange of sensitive information between IoT devices in a smart home environment. By utilizing the routing module, the smart home can ensure that data such as user preferences, security alerts, and environmental conditions are transmitted securely and confidentially between connected devices, bolstering the overall security posture of the network.

The verification of the signature is a crucial step in ensuring the authenticity and integrity of transmitted data. Through the use of Lamport's Keyed Hashing Chain scheme, the IoT Routing Module will implement a secure and efficient verification process. By using Lamport's Keyed Hashing Chain scheme, the IoT Routing Module can efficiently verify the authenticity and integrity of transmitted data. This scheme relies on a chain of cryptographic hash functions that generate digital signatures for each block of data. These signatures are then validated by comparing them with the corresponding public keys stored in a secure database.

**3.2 Data Flow Diagrams**

In order to visualize the flow of data within the IoT network and the interaction of various components, a data flow diagram can be created. This diagram shown in figure 3.2 will illustrate the movement of data packets through the IoT devices, routing module, data inspection unit, authentication and encryption unit, network interface, and other components within the system. Additionally, it will depict the flow of data through the scalability and adaptability layer, as well as the security and compliance unit. The data flow diagram will provide a comprehensive understanding of how data is processed, secured, and transmitted within the IoT network, highlighting the crucial role of the routing module and other key components. 

**Figure 3.2: Data flow diagram**

In order to evaluate the effectiveness of Lamport's Keyed Hashing Chain Scheme in addressing manipulation and modification attacks, it is important to analyze the verification time, key generation time, and signing time. This analysis will provide insights into the efficiency and computational overhead of using Lamport's Keyed Hashing Chain Scheme in the routing module. Through this analysis, the performance of the routing module in terms of verification time, key generation time, and signing time can be determined

**3.3 Description of System Operation**

1. Initialization:

* The root/gateway of the IoT network generates a secret key.
* Each participating node in the network obtains this key securely.

2. Message Authentication:

* When a node receives a RPL message (e.g., DIO or DAO), it needs to authenticate the message before acting upon it.
* The node combines the received message (M) with its own identity and the secret key.
* Using Lamport’s keyed hash chain method, the node generates an authentication ticket based on this combination.

3. Validation Process:

* When a neighbouring node receives the message along the route, it also verifies the message's authenticity using the same method.
* If the authentication ticket generated by the neighbouring node matches the expected value, the message is deemed authentic.

4. Routing Decision:

* Authenticated messages contribute to the routing decision-making process.
* Nodes select optimal routes based on the authenticated routing information provided in the RPL messages.

5. Dynamic Updates:

* As the network topology changes or new nodes join, the process of generating and validating authentication tickets continues to ensure message integrity.
* Nodes periodically update their authentication tickets based on the changing network conditions.

6. Key Rotation and Management:

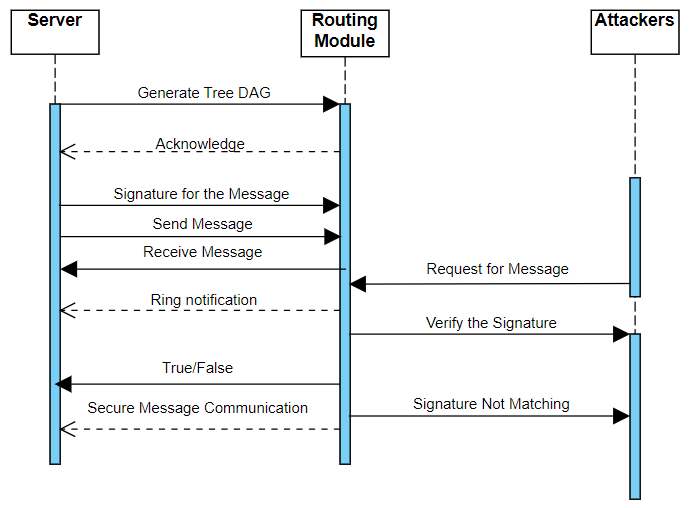
* To enhance security, keys may be rotated periodically or in response to security events.
* Key management mechanisms ensure secure distribution and storage of keys across the IoT network.

7. Resilience to Attacks:

* The system is designed to resist various attacks such as message spoofing, modification, or replay attacks.
* By combining node identity with the secret key and using hash-based authentication, the system provides robust protection against unauthorized access and manipulation of RPL messages.

**3.4 Sequence diagram**

In the sequence diagram presented in figure 3.3, the flow illustrates the process of an IoT device securely joining a Routing Protocol for Low Power and Lossy Networks (RPL) with Destination-Oriented Directed Acyclic Graph (DODAG) network, facilitated by a border router using Lamport's Key Hashing scheme. Initially, the IoT device initiates the network joining process by sending a join request to the border router. Upon receiving the request, the border router generates a cryptographic key using Lamport's Key Hashing scheme, encrypts it, and sends it back to the IoT device. The IoT device decrypts the received key, verifies its authenticity using Lamport's Key Hashing, and gets authenticated by the border router. Subsequently, the border router adds the IoT device to the network and starts routing data packets to it. Data exchange occurs bidirectionally between the IoT device and the border router, ensuring secure communication within the RPL network.

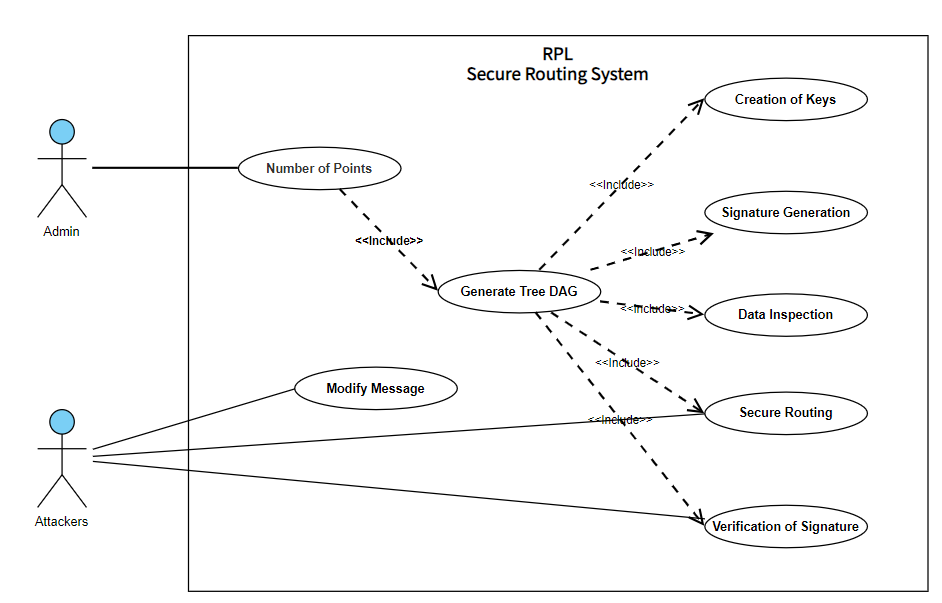


**Figure 3.4: Sequence Diagram**

IoT Device: The IoT device initiates the process to join the RPL network securely using Lamport's Key Hashing scheme. The IoT device sends data packets securely to other devices or the border router using Lamport's Key Hashing for message authentication. The IoT device receives data packets securely from other devices or the border router, verifying their authenticity using Lamport's Key Hashing. Manage Keys: The border router manages cryptographic keys using Lamport's Key Hashing scheme for secure communication with IoT devices. Route Messages: The border router routes data packets securely between IoT devices and external networks, ensuring integrity and authenticity using Lamport's Key Hashing. Provide Access: The border router provides secure access to the RPL network for authorized devices, employing Lamport's Key Hashing for authentication and key management.

**3.5 Use case Diagram**

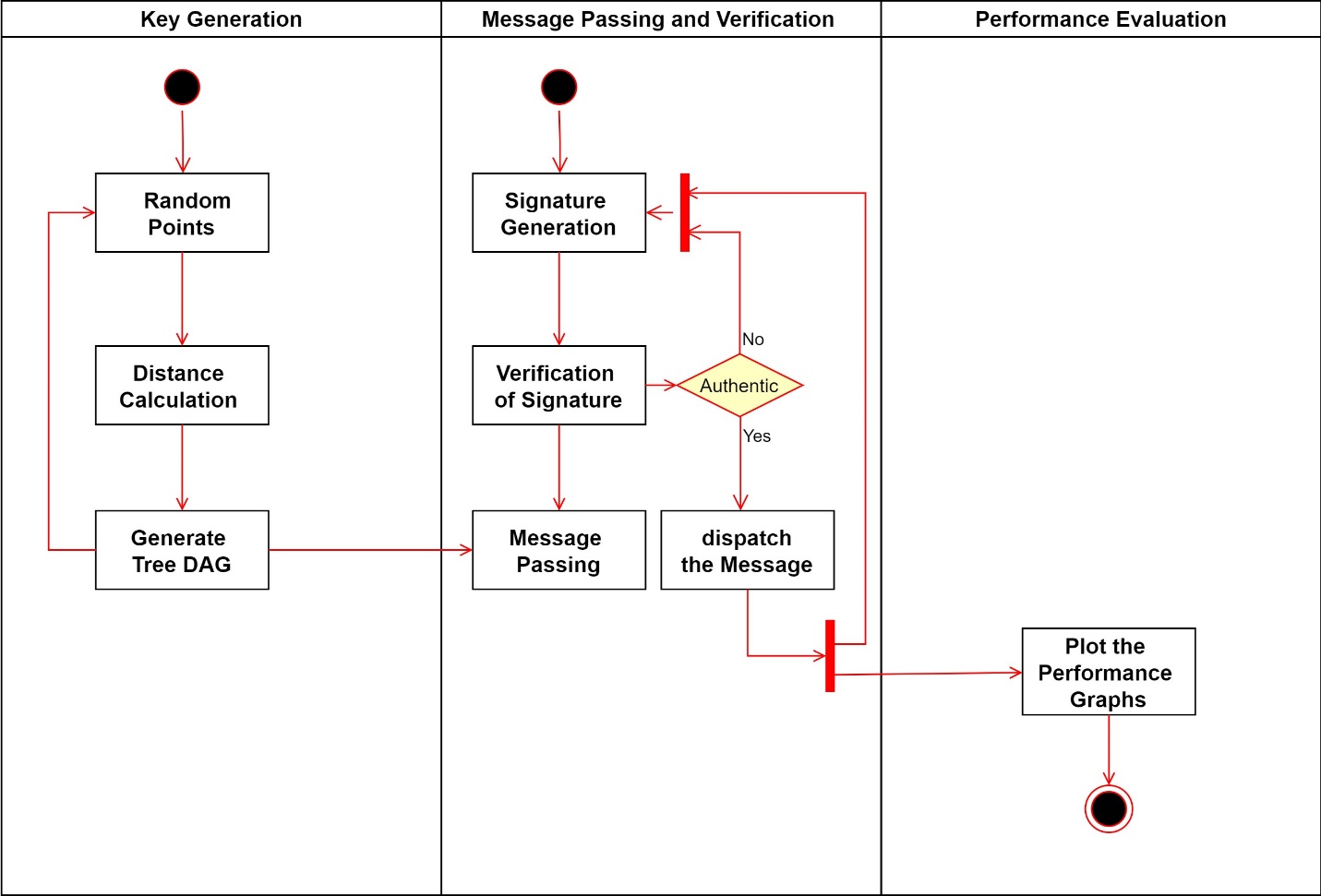
In this use case diagram in figure 3.4, the primary actors are IoT devices and the border router. The IoT devices interact with the RPL network by joining, sending, and receiving data securely using Lamport's Key Hashing scheme for message authentication. The border router manages cryptographic keys and ensures secure communication between IoT devices and external networks, also leveraging Lamport's Key Hashing for security purposes. These use cases illustrate the essential functionalities of a secure RPL with DODAG implementation using Lamport's Key Hashing scheme for IoT devices.



**Figure 3.5: Use Case diagram**

**3.6 Algorithm Specification flowchart**

This diagram will outline the sequence of actions and interactions among different system components, including data processing, encryption, authentication, and data transmission. It will provide a comprehensive visualization of the workflow within the routing module, demonstrating how various activities are coordinated and executed to ensure secure and efficient data transfer within the IoT network. By displaying the activities and their relationships in a graphical format, the activity diagram will offer a clear understanding of the routing module's operational workflow and its integration with other system components. This visualization will be valuable for stakeholders and developers to comprehend the module's functionality and identify opportunities for further optimization and refinement.



**Figure 3.6: flow chart**

**3.7 Implementation Languages**

Python is a solid choice for implementing the Secure RPL algorithm, especially considering its suitability for rapid prototyping, readability, and extensive library support. However, if you're looking for alternative languages for specific reasons, here are some suggestions based on different criteria:

**Performance and Efficiency:** If performance is a critical factor, especially in resource-constrained IoT environments where computational resources are limited, languages like C or C++ might be more appropriate. These languages provide finer control over memory management and execution speed, making them ideal for optimizing performance-critical parts of the algorithm.

**Platform Compatibility:** If your IoT network consists of devices with diverse platforms and architectures, a language like Java might be a good choice due to its platform independence. Java programs can run on any platform with the Java Virtual Machine (JVM), allowing you to develop applications that can be deployed across a wide range of devices without modification.

**Security and Memory Safety:** Rust is a language known for its focus on memory safety and security. If security is a primary concern, especially in IoT environments where vulnerabilities can have severe consequences, Rust's memory safety features can help prevent common security vulnerabilities like buffer overflows and memory corruption.

**Developer Familiarity and Ecosystem:** If you and your team are already familiar with a particular language or ecosystem, it may be advantageous to leverage that expertise. For example, if your team has experience with JavaScript and the Node.js ecosystem, you could use JavaScript for implementing the algorithm, benefiting from existing libraries and tools available in the JavaScript ecosystem.

**Interoperability:** If your IoT network includes devices running different operating systems or programming languages, choosing a language with good interoperability can simplify integration. For example, languages like Python, Go, and Kotlin offer good interoperability with C/C++ code, allowing you to leverage existing libraries or components written in those languages.

**Chapter 4**

**SYSTEM VERIFICATION**

**4.1 Functions to be Tested**

**Message Generation Function:**

* Ensure that the function responsible for generating RPL messages (e.g., DIO and DAO) correctly incorporates authentication information (such as authentication ticket) according to Secure RPL's methodology.
* Test the function with different input parameters, including message content, node identity, and secret key, to verify that the authentication information is generated accurately.

**Message Reception and Processing Function:**

* Test the function responsible for receiving and processing incoming RPL messages.
* Verify that the function correctly extracts authentication information from received messages and passes it to the message validation function for authentication.
* Test the function's behaviour under various scenarios, including the presence of authenticated and unauthenticated messages, to ensure correct message handling.

**Message Authentication Function:**

* Test the message authentication function to ensure that it correctly generates authentication information (e.g., authentication ticket) based on Secure RPL's methodology.
* Verify that the generated authentication information matches the expected value for a given message, node identity, and secret key combination.
* Test the function's performance and resource usage to ensure efficiency, especially in resource-constrained environments.

**Message Validation Function:**

* Test the message validation function to verify its ability to authenticate incoming messages based on the provided authentication information.
* Ensure that the function correctly identifies authenticated messages and rejects unauthorized or tampered messages.
* Test the function's behaviour under different scenarios, including valid and invalid authentication information, to ensure robustness and security.

**Key Management Functions:**

* Test key generation, distribution, and rotation mechanisms to ensure secure and efficient management of secret keys used for message authentication.
* Verify that keys are securely generated, distributed to participating nodes, and rotated periodically or in response to security events.
* Test the functions' behaviour under various scenarios, including key distribution failures and key rotation events, to ensure reliability and security.

**Integration Testing:**

* Test the integration of Secure RPL into the existing ns2 simulation environment.
* Verify that Secure RPL interacts correctly with other components of the simulation, including the network topology, routing protocols, and application layer protocols.
* Test the behaviour of Secure RPL-enabled RPL protocol under various network scenarios and conditions to assess performance, scalability, and security.

**Security Testing:**

* Conduct security testing to assess the protocol's resilience against common security threats, such as message spoofing, tampering, or replay attacks.
* Verify that Secure RPL provides adequate protection against unauthorized access and manipulation of RPL messages, especially in hostile network environments.
* Test the protocol's response to security events and its ability to detect and mitigate security breaches.

**4.2 Test Cases for RPL Network Simulation**

The system verification phase for this project included creating a simulated RPL network environment to validate the functionality and resilience of the newly designed routing module. This simulation aimed to mimic real-world IoT network conditions and included a variety of test cases to ensure comprehensive coverage:

**1.Protocol Conformance Test**:

* **Description**: Determine whether the routing module complies with existing RPL standards.
* **Methodology**: Simulate the standard behaviour of the RPL and check if the module abides by the protocol specifications.
* **Expected Outcome**: Seamless integration with no deviations from the RPL standards.

**2.Attack Scenario Simulation**:

* **Description**: Verify the module's response to common routing attacks.
* **Methodology**: Introduce various attack vectors, such as version number attacks and Sybil attacks, and evaluate the module's detection and mitigation strategies.
* **Expected Outcome**: Accurate detection of attacks and timely execution of appropriate countermeasures to ensure network integrity.
* **Description**: Assess the impact of security features on the network's resource usage.
* **Methodology**: Monitor and compare the resource utilization of the network with and without the security module, focusing on power, memory, and computational overhead.
* **Expected Outcome**: Minimal increase in resource consumption, illustrating the module's efficiency in constrained environments.
  1. **Test Run Procedures and Results**

**Test Scenario Definition:**

* Define test scenarios that cover various aspects of Secure RPL functionality, including message authentication, validation, key management, and integration with the RPL protocol.
* Design test cases to simulate different network topologies, traffic patterns, and security threats relevant to IoT environments.

**Simulation Setup:**

* Configure ns2 to simulate the defined test scenarios, including network topology, node placement, traffic generation, and protocol parameters.
* Enable Secure RPL in the RPL protocol implementation and configure key management parameters, such as key generation, distribution, and rotation policies.

**Execution of Test Runs:**

* Run simulations for each test scenario using ns2, ensuring that Secure RPL is enabled and functioning correctly.
* Monitor simulation progress and collect relevant metrics, such as message delivery ratio, end-to-end delay, packet loss, and energy consumption.

**Analysis of Results:**

* Analyze simulation results to evaluate the performance and security of Secure RPL under different test scenarios.
* Assess the effectiveness of message authentication and validation mechanisms in detecting and preventing security threats, such as message spoofing or tampering.
* Evaluate the impact of Secure RPL on network performance metrics, such as routing efficiency, scalability, and resource utilization.

**Documentation of Test Results:**

* Document the outcomes of each test run, including observed behavior, performance metrics, and any anomalies or issues encountered.
* Provide detailed analysis and interpretation of simulation results, highlighting strengths, weaknesses, and areas for improvement in the Secure RPL implementation.

**Reporting and Presentation:**

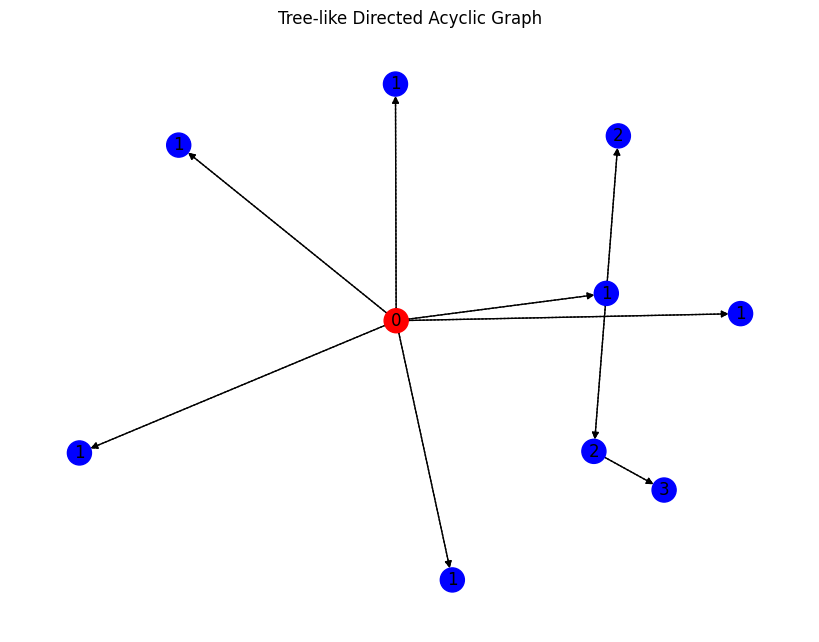
* Prepare a comprehensive test report summarizing the test procedures, results, and findings.
* Present the test report to stakeholders, including developers, researchers, and project managers, to communicate the performance and security characteristics of Secure RPL in ns2.

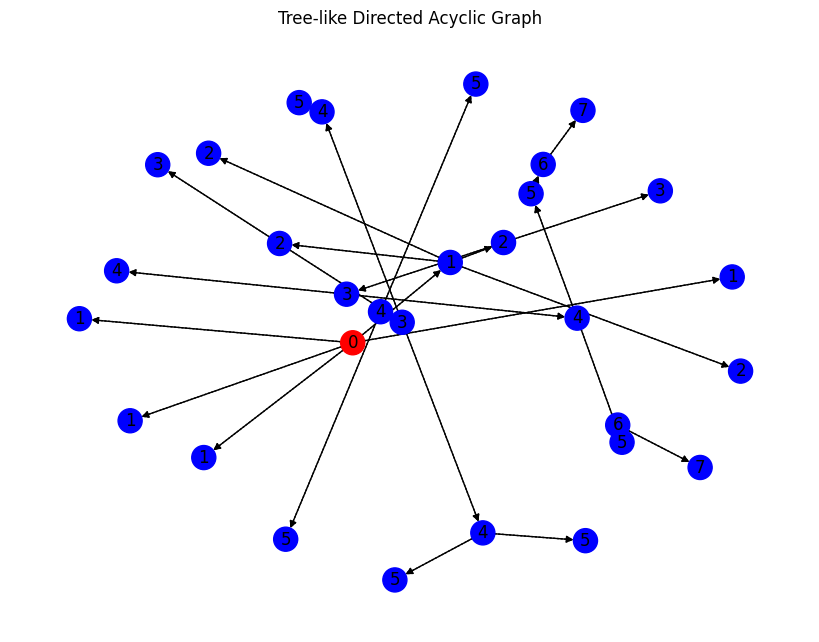
**Expected Results:**

* Successful execution of test scenarios with Secure RPL enabled in ns2 simulations.
* Verification of message authentication and validation mechanisms, ensuring correct handling of authenticated and unauthenticated messages.
* Analysis of performance metrics demonstrating the impact of Secure RPL on network efficiency, scalability, and security.
* Detection and mitigation of security threats, such as message spoofing or tampering, through effective key management and authentication mechanisms.
* Identification of any issues or limitations in the Secure RPL implementation and recommendations for future enhancements or optimizations.

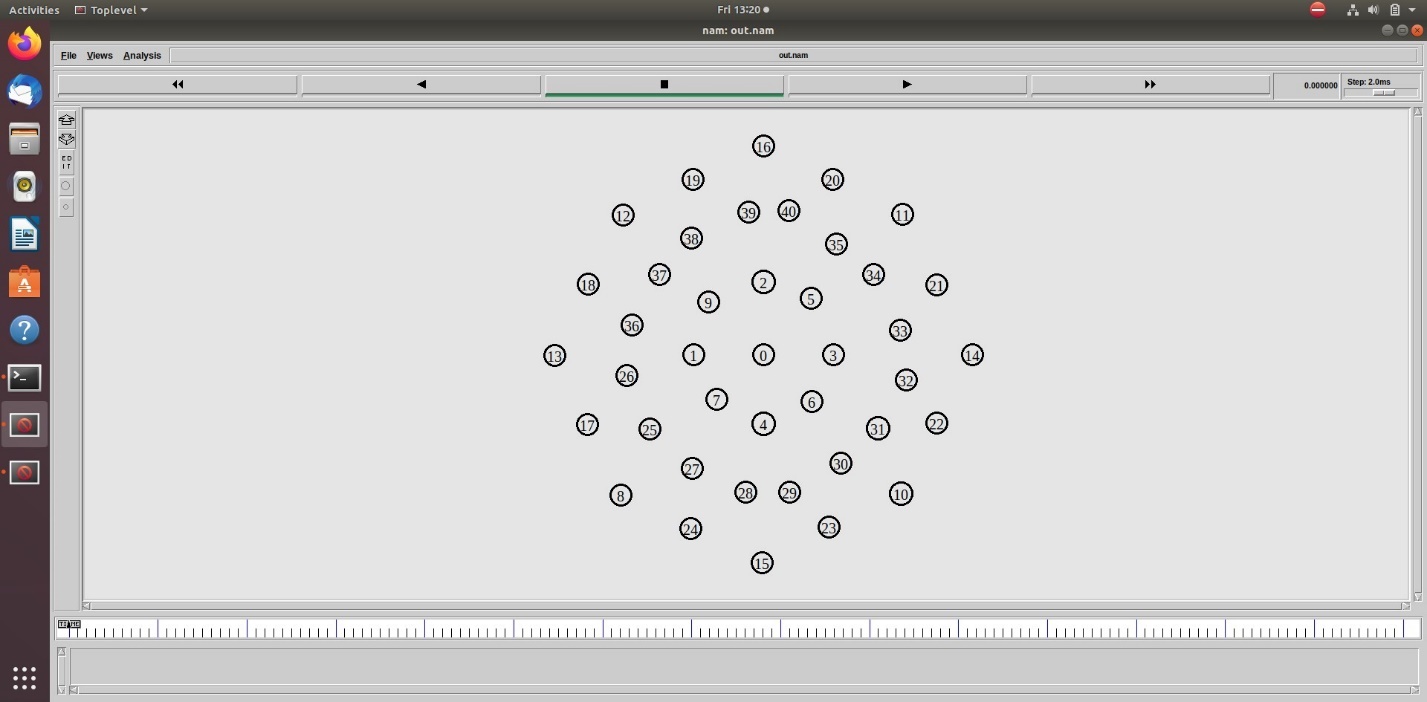
**Chapter 5**

**RESULTS**

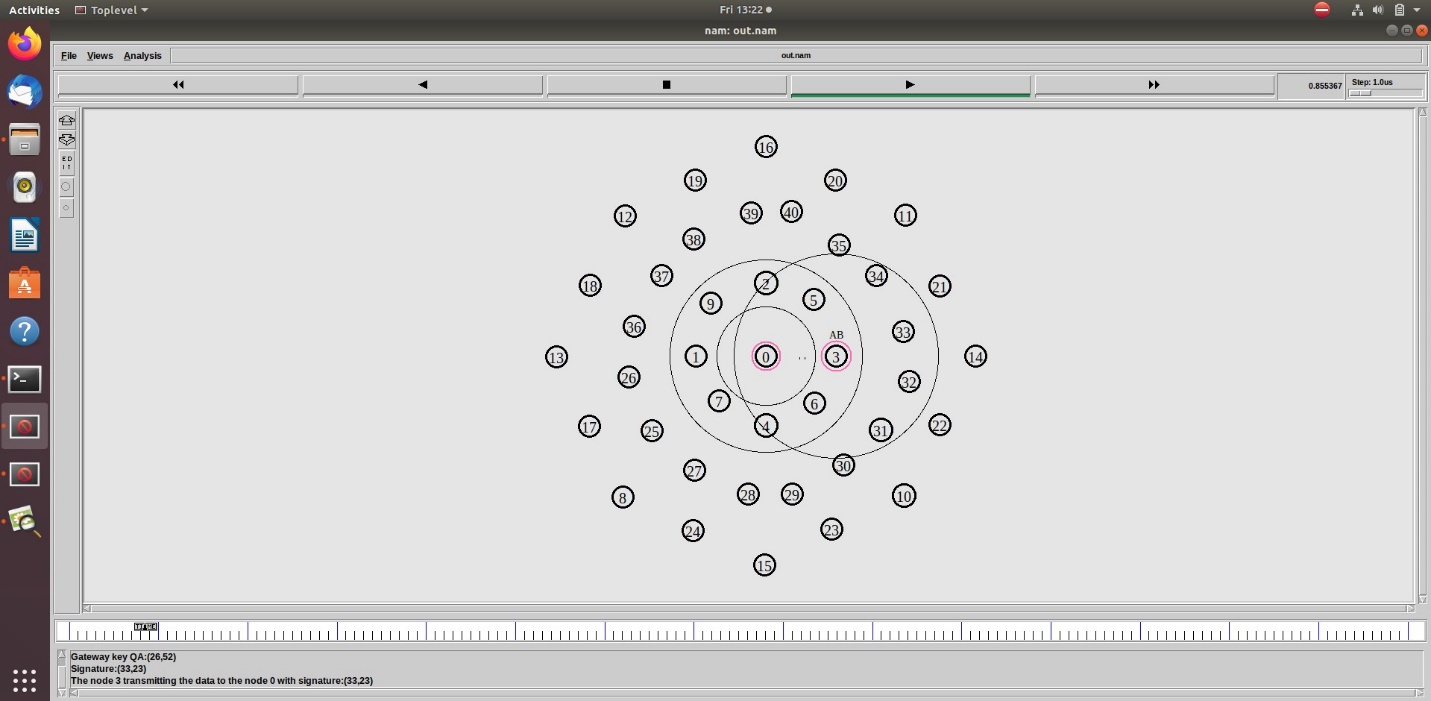
****

****

**Figure 5.1 Generation of Tree like directed acyclic graph**



**Figure 5.2 Deployment of nodes in the RPL Network**



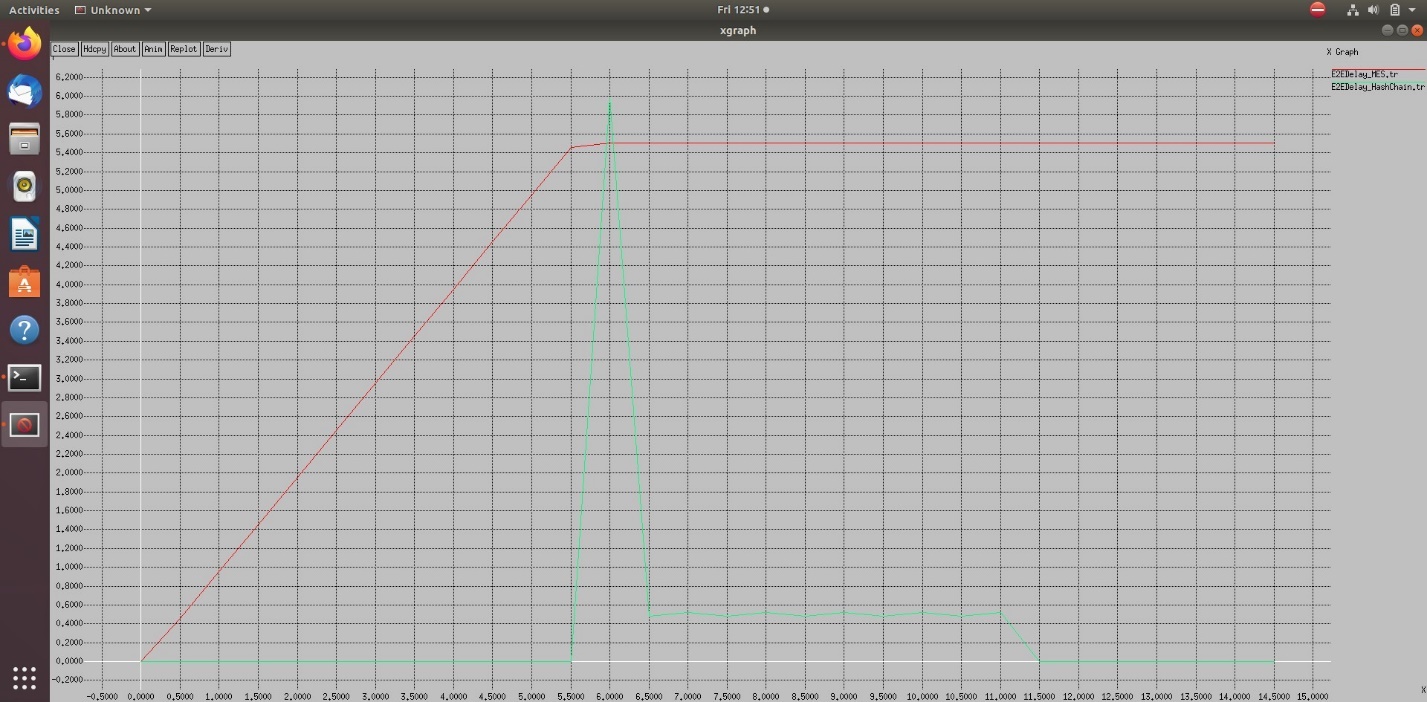
**Figure 5.3 Packets Distribution in the RPL Network**



**Figure 5.4 Packet Loss Analysis**



**Figure 5.5 Packet Delivery Ratio**



**Figure 5.6 Delay Ratio Analysis**

**Chapter 6**

**CONCLUSION**

**6.1 Summary**

This project embarked on the critical task of enhancing the security of Internet of Things routing protocols, with a focus on the widely adopted IPv6 Routing Protocol for Low-Power and Lossy Networks. As IoT devices become increasingly embedded in our daily lives and industrial systems, the need for robust security measures has never been more pronounced. Through the design and development of a specialized routing module, this project aimed to address the glaring vulnerabilities in the RPL, specifically targeting modification and manipulation attacks. The module's design integrated seamlessly with RPL, offering a fortified layer of security without compromising the efficiency and performance of the underlying network.

The project demonstrated that it is indeed possible to devise a routing solution that is secure, resource-efficient, and scalable. By conducting extensive analysis, the project was able to pinpoint weaknesses within the RPL and introduce a suite of security enhancements. These included novel Lamport's Keyed Hashing Chain Scheme designed to operate within the constraints of low-power and lossy networks. The routing module presented a holistic approach to IoT security, encompassing authentication, integrity checks, and intrusion response capabilities. In validation testing, the module showed that it could significantly mitigate risks associated with routing attacks while maintaining operational integrity and low overhead.

**6.2 Future Scope**

Looking to the future, the work begun in this project lays the groundwork for a series of evolutions within the field of IoT security. One area for further development is the deep integration of machine learning techniques to refine anomaly detection and predictive security measures. As IoT networks grow in complexity and scale, leveraging artificial intelligence could enable more dynamic and responsive security protocols that adapt to emerging threats in real-time. Another avenue for exploration is the implementation of blockchain or distributed ledger technologies to enhance trust management and maintain immutable logs of network activity—an essential feature for forensic analysis post-security incidents. Additionally, the further development of energy-efficient encryption mechanisms will remain a key focus, ensuring that the security of future IoT devices can be maintained even in the most resource-constrained environments. Finally, this project opens the door to cross-disciplinary collaboration, where insights from fields such as behavioural analytics, network theory, and software-defined networks can converge to create more intelligent and autonomous security systems. The route ahead for IoT security is indeed promising and necessary, as the very backbone of our increasingly connected world rests upon the assurance that our networks are safe, private, and resilient against threats.

**REFERENCES**

1. N. Janicijevic, M. Luki ´ c, and I. Mezei, “Routing protocol for low- ´ power and lossy wireless sensor networks,” in Proc. 19th Telecommun. Forum (TELFOR), 2011, pp. 234–237.
2. N. Janicijevic, M. Luki ´ c, and I. Mezei, “Routing protocol for low- ´ power and lossy wireless sensor networks,” in Proc. 19th Telecommun.Forum (TELFOR), 2011, pp. 234–237.
3. J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the Internet of Things: A survey of existing protocols and open research issues,” IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
4. A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, “A study of RPL DODAG version attacks,” in Monitoring and Securing Virtualized Networks and Services [LNCS 8508 (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)], A. Sperotto, G. Doyen, S. Latré, M. Charalambides, and B. Stiller, Eds. Heidelberg, Germany: Springer, 2014, pp. 92–104.
5. J. Granjal, E. Monteiro, and J. S. Silva, “Security in the integration of low-power wireless sensor networks with the Internet: A survey,” Ad Hoc Netw., vol. 24, pp. 264–287, Jan. 2015.
6. J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the Internet of Things: A survey of existing protocols and open research issues,” IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, 2nd Quart.,2015.
7. I. Tomic and J. A. McCann, “A survey of potential security issues in ´existing wireless sensor network protocols,” IEEE Internet Things J., vol. 4, no. 6, pp. 1910–1923, Dec. 2017.
8. V. Adat and B. B. Gupta, “Security in Internet of Things: Issues, challenges, taxonomy, and architecture,” Telecommun. Syst., vol. 67, no. 3,pp. 423–441, Mar. 2018.
9. M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating critical security issues of the IoT world: Present and future challenges,” IEEE Internet Things J., vol. 5, no. 4, pp. 2483–2495, Oct. 2018.
10. T. A. Ahanger and A. Aljumah, “Internet of Things: A comprehensive study of security issues and defense mechanisms,” IEEE Access, vol. 7, pp. 11020–11028, 2019.
11. H. A. Abdul-Ghani and D. Konstantas, “A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective,” J. Sens. Actuator Netw., vol. 8, no. 2, p. 22, Apr. 2019.
12. D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for Internet of Things: A survey,” J. Netw. Comput. Appl., vol. 66, pp. 198–213, May 2016.
13. A. Mayzaud, R. Badonnel, and I. Chrisment, “A taxonomy of attacks in RPL-based Internet of Things,” Int. J. Netw. Security, vol. 18, no. 3, pp. 459–473, 2016.
14. H.-S. Kim, J. Ko, D. E. Culler, and J. Paek, “Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey,” IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2502–2525, 4th Quart., 2017.
15. X. Liu, Z. Sheng, C. Yin, F. Ali, and D. Roggen, “Performance analysis of routing protocol for low power and lossy networks (RPL) in large scale networks,” IEEE Internet Things J., vol. 4, no. 6, pp. 2172–2185, Dec. 2017.