Republic of the Philippines
POLYTECHNIC UNIVERSITY OF THE PHILIPPINES
ACADEMIC YEAR 2024 – 2025
COLLEGE OF COMPUTER AND INFORMATION SCIENCES

Optimizing Network Security Protocols Using Finite Automata: A Case Study on Non Deterministic Routing and Attack Detection in Distributed Systems

Presented to the Faculty of the College of Computer and Information Sciences
Polytechnic University of the Philippines
Sta. Mesa, Manila

In Partial Fulfilment of the Requirements in
COSC 302: Automata and Language Theory

Submitted by:

Reyes, Arwen Angelique
Rolle, Xavier
Romales, Justine Carl
Villalobos, Kristine Faye

January 2025

Chapter 1

THE PROBLEM AND ITS BACKGROUND

1.1. Introduction

A distributed system is a collection of autonomous computing elements that appears to its users as a single coherent system. This definition refers to two characteristic features of distributed systems. The first one is that a distributed system is a collection of computing elements each being able to behave independently of each other. A computing element, which we will generally refer to as a node, can be either a hardware device or a software process. A second element is that users (be they people or applications) believe they are dealing with a single system. This means that one way or another the autonomous nodes need to collaborate. How to establish this collaboration lies at the heart of developing distributed systems. (Van Steen & Tanenbaum, 2016).

The rapid growth of distributed systems has significantly advanced technology, allowing for seamless global communication and collaboration. However, this growth has also introduced serious challenges in protecting these systems from cyber threats. Distributed systems consist of multiple interconnected components that exchange data in real-time. Distributed systems may face several security challenges and problems due to their interconnective nature, including man-made problems, such as cyberattacks, and natural disasters that could disrupt the system's functionality (GeeksForGeeks, 2024), When problems occur in routing, whether due to cyberattacks or other disruptions, it is crucial to secure the data transmission process, particularly in transferring packets between nodes. Ensuring robust routing mechanisms and protecting the

integrity of transmitted data are essential steps to mitigate these risks and maintain system reliability. To mitigate these potential interruptions, the application of the concept of non-determinism may allow network systems to operate with flexibility and adapt to unforeseen disruptions. Non-determinism enables a concise representation of circuit behaviors, which is crucial for logic synthesis and optimization tasks (Mishchenko et al., n.d). By incorporating non-deterministic behaviors, such as multiple potential routing paths or alternative routes, a distributed system can dynamically adjust to changes in the network. This flexibility ensures that, in the event of a cyberattack, node failure, or network congestion, the system can reroute data through available paths without compromising performance or security.

The objective of this research is to explore the practical application of finite automata, particularly nondeterministic finite automata (NFA), in enhancing network security protocols within distributed systems. Unlike deterministic approaches that rely on fixed rules and sequences, the flexibility of nondeterministic models allows systems to address a wider range of unpredictable scenarios. The research aims to know and understand how finite automata, particularly NFAs, can be effectively applied to detect and dynamically respond to network attacks, with an emphasis on non deterministic routing scenarios.

1.2. Background of the Study

Distributed systems are built to consist of multiple independent computing nodes that work together as a single unit, allowing for the exchange of data and communication on a global scale. This type of architecture provides several benefits, such as scalability, flexibility, and fault tolerance, which makes it crucial for modern-day applications like cloud computing, telecommunications, and large-scale networks used in enterprises.

However, as these systems grow more complex, they encounter considerable challenges, particularly in terms of security and reliability. The very nature of interconnected networks makes them vulnerable to a range of issues, including cyberattacks, network congestion, and hardware malfunctions. Cyberattacks, like Distributed Denial of Service (DDoS), can target weaknesses in routing protocols, leading to network failures and bringing the system to a halt. Additionally, natural disruptions or technical breakdowns can cause data loss or delays, compromising the reliability of the system.

Traditional methods of managing network routing in distributed systems are often based on deterministic approaches, where fixed routes are established for data transfer between nodes. While these methods offer stability and predictability, they lack the flexibility needed to handle dynamic and unpredictable disruptions, such as sudden traffic spikes, node failures, or malicious interference. As a result, these systems can struggle to maintain optimal performance when facing unforeseen circumstances, which highlights the need for more flexible and resilient routing techniques. One promising solution to these problems lies in the concept of non-determinism, which comes from the field of automata theory. Non-deterministic models, such as Nondeterministic Finite Automata (NFA), allow for multiple possible routes or transitions from a given state. This flexibility enables distributed systems to dynamically adjust to changes in network conditions, ensuring that data is still able to be routed through alternative paths even when disruptions occur, all without sacrificing security or performance. By introducing this adaptability, NFAs can potentially improve the system's fault tolerance, routing efficiency, and ability to detect anomalies, making the system more resilient against cyber threats and system failures.

1.3. Statement of the Problem

The Internet, supported by distributed systems, has revolutionized communication and collaboration globally. These systems rely on interconnected nodes to provide seamless data sharing but are vulnerable to cyberattacks, network congestion, and system failures. Traditional deterministic approaches, such as fixed routing, struggle to adapt to the unpredictable nature of distributed environments. This limits their ability to address real-time fault tolerance, adaptive routing, and evolving security threats.

Nondeterministic finite automata (NFA) offer theoretical advantages in flexibility and adaptability by enabling systems to evaluate multiple pathways simultaneously. This capability could improve fault tolerance, dynamic routing, and anomaly detection. However, the application of NFA in distributed systems remains underexplored, creating a gap in leveraging their potential to enhance system security and reliability. The central research question guiding this study is;

How can nondeterministic finite automata (NFA) be applied to enhance the security and adaptability of routing mechanisms in distributed systems, particularly in response to cyberattacks and network disruptions?

Sub Questions

1. What theoretical benefits do NFAs offer in improving routing flexibility and fault tolerance in distributed systems?
2. How do NFA-based security protocols compare to traditional deterministic approaches in handling unpredictable network scenarios?

3. Can NFAs be effectively applied for dynamic anomaly detection and real-time threat mitigation?
4. How can nondeterministic routing mechanisms increase the resilience and scalability of distributed systems in response to disruptions like node failures or cyberattacks?

By addressing this question, the research aims to contribute to the development of more secure and resilient distributed systems capable of effectively responding to evolving security threats.

1.4. Objective of the Study

General Objective

To explore the application of nondeterministic finite automata (NFA) in enhancing the security, flexibility, and fault tolerance of distributed systems, particularly in addressing network disruptions and cyber threats.

Specific Objectives

1. **Apply NFA on a Theoretical Level to Distributed Systems**

   To analyze the theoretical capabilities of NFAs in providing flexible and adaptive solutions for distributed systems.

2. **Analyze the Security Benefits of NFA**

   Explore how NFAs can enhance network security by providing flexible and adaptive routing mechanisms to mitigate risks and vulnerabilities.

3. **Identify the Gaps & Limitations of Deterministic Approaches in Distributed Systems**

   To examine the limitations of deterministic approaches in managing security, routing, and fault tolerance challenges in distributed systems.

4. **Propose a Methodology for Integration**

   Outline a structured methodology for incorporating NFA-based designs into distributed system architectures, focusing on adaptability and scalability.

1.5. Significance of the Study

Different sectors will benefit from this study, including network security professionals, system architects, future researchers, technology developers, policymakers, and the general public. It will help address the growing need for innovative approaches to enhancing distributed systems' security and adaptability using nondeterministic finite automata (NFA).

For **network security professionals and system administrators**, the study will introduce an adaptive approach to routing and anomaly detection, offering a practical solution for maintaining system stability during cyberattacks, node failures, and network congestion. By using NFAs, network security strategies will become more flexible and better equipped to handle unpredictable threats. This will allow professionals to improve system resilience and ensure secure data transmission. For **system architects and technology developers**, the study will provide insights into designing scalable and resilient distributed systems that can dynamically adjust to real-time disruptions. The findings of this research will encourage the development of more robust network infrastructures capable of supporting the demands of complex,

interconnected environments. For **future researchers**, the study will contribute knowledge in automata theory, network security, and distributed systems. It will provide valuable data on the effectiveness of NFA-based protocols in handling dynamic network environments and offer a framework for further research on integrating theoretical concepts with practical applications in network security. For **policymakers and industry stakeholders**, the study will offer insights that can inform cybersecurity policies and best practices. The findings will support efforts to encourage investment in adaptive security technologies to protect critical infrastructures and promote innovation in the field of network security.

The study will also indirectly benefit the general public by contributing to the development of more secure and reliable distributed systems. As these systems form the backbone of modern communication and commerce, improving their security and adaptability will help protect sensitive data and ensure continuous access to essential services.

1.6. Scope and Delimitations

This study will focus on exploring the application of finite automata, particularly nondeterministic finite automata (NFA), in optimizing network security protocols for distributed systems. It will examine how NFAs can improve the flexibility and adaptability of routing mechanisms, enabling distributed systems to handle dynamic and unpredictable network conditions, such as cyberattacks, node failures, and congestion. The research will also investigate the use of NFAs for anomaly detection by modeling and analyzing system behaviors to identify potential threats or irregularities. The study will cover theoretical frameworks, algorithmic design, and potential practical implementations of NFAs in distributed environments.

Additionally, it will include case studies and simulations to demonstrate the effectiveness of these approaches in enhancing the security and reliability of distributed systems.

However the study may encounter the following limitations;

1. While NFAs provide a flexible framework, their implementation in real-world distributed systems may face computational overhead due to the complexity of managing multiple potential states and paths.
2. The study will be limited to simulations and theoretical analyses and may not involve direct deployment in large-scale distributed systems. Furthermore,
3. The research will not be able to address all aspects of network security, such as physical layer vulnerabilities or user authentication protocols, focusing primarily on routing and anomaly detection. Finally,
4. While the study will aim to demonstrate the feasibility of using NFAs for enhanced security, the practical integration of these models into existing systems may require additional research and development beyond the scope of this paper.

1.7. Definition of Terms

This section defines the key terms used in the study to provide clarity and a common understanding.

Term	Definition
Distributed Systems	A collection of autonomous computing elements (nodes), such as computers or software processes, that work together to appear as a single, coherent system to users. These systems enable global collaboration and data sharing but are susceptible to vulnerabilities like cyberattacks and node failures (Van Steen & Tanenbaum, 2016).
Nondeterministic Finite Automata (NFA)	A theoretical model in automata theory that allows multiple possible transitions from a single state for a given input. This flexibility enables NFAs to represent dynamic and unpredictable behaviors in systems, such as alternative routing paths or fault-tolerant mechanisms (Mishchenko & Brayton, n.d.).
Routing	The process of selecting paths in a network for transmitting data packets from a source to a destination. Effective routing ensures the efficient delivery of data and adapts to network disruptions like congestion or node failures.
Fault Tolerance	The ability of a system to continue functioning correctly despite the failure of one or more of its

	components. In distributed systems, fault tolerance ensures reliability by dynamically rerouting tasks or data (GeeksForGeeks, 2024).
Cyberattacks	Malicious attempts to disrupt, damage, or gain unauthorized access to computer systems, networks, or data. Cyberattacks pose a significant threat to distributed systems by exploiting their interconnected nature (Hamdi & Mosbah, 2009).
Dynamic Routing	A type of network routing that adapts to changes in real-time, such as increased traffic, node failures, or cyberattacks. Dynamic routing ensures data packets are delivered efficiently without delays or loss.
Anomaly Detection	The process of identifying unusual patterns or behaviors in a system that may indicate errors, failures, or malicious activities. Anomaly detection is essential in distributed systems for maintaining security and operational integrity (Zhao et al., 2021).
Deterministic Finite Automata (DFA)	A type of finite automaton in which each state has exactly one transition for each input symbol. DFAs are often used for modeling predictable and static behaviors but lack the flexibility to handle dynamic environments.

Chapter 2
REVIEW OF RELATED LITERATURE AND STUDIES

2.1. Related Literature

The process of computation was started from working on a single processor. This uniprocessor computing can be termed as centralized computing. As the demand for the increased processing capability grew, multiprocessor systems came to existence. The advent of multiprocessor systems led to the development of distributed systems with a high degree of scalability and resource sharing. Modern-day parallel computing is a subset of distributed computing. A distributed system is a collection of independent computers, interconnected via a network, capable of collaborating on a task. Distributed computing is computing performed in a distributed system.

Modern distributed systems can, and often will, consist of all kinds of nodes, ranging from very big high-performance computers to small plug computers or even smaller devices. A fundamental principle is that nodes can act independently from each other, although it should be obvious that if they ignore each other, then there is no use in putting them into the same distributed system. In practice, nodes are programmed to achieve common goals, which are realized by exchanging messages with each other. A node reacts to incoming messages, which are then processed and, in turn, leading to further communication through message passing. (Van Steen & Tanenbaum, 2016).

Security in distributed systems essentially can be divided into two important parts. The first part is the communication between users, including secure channels, more particularly: authentication, message integrity, and confidentiality. The other part involves the access rights to

the resources in distributed systems. It is important to define what a secure system is. One assumption is that security is absolute, but according to Wulf et al., security in the physical world is never absolute because none of the safes are expected to resist attacks that can happen in the system. From this point of view, users must feel confident about the security, but it cannot be said that users are guaranteed of anything that can happen (Wulf et al., n.d.). Clearly declaring that a system should be able to protect itself against all achievable security threats is not the way to actually build a secure system. It is almost understandable that hosts — such as client desktops and low-level servers — need to be protected from malicious outside agents. Applications have assumed major importance, and the design of them needs to be secure. Services must achieve confidentiality and integrity. As described, security in such systems presents a significant challenge for certain reasons. Different concepts are summarized for security in distributed systems. Security features can be defined depending on the environment in which applications are operating. Users must have some capabilities and policies that allow them easy access to the resources. It is important to mention that security must usually be applied in all layers, not in a specific one, because it is difficult to understand and manage the system (Hamdi & Mosbah, 2009).

To analyze the various elements of IT security that can occur in the system, a metamodel is developed. According to Miede and Nedyalkov (2010), a good security system must use three main parts: a core of basic IT security concepts, countermeasures, and attacks. The metamodel describes assets, threats, and security goals, and it also focuses on attacks. The metamodel is applied in real life using three attacks in distributed systems: incorrect lookup routing on peer-to-peer systems, XML bombs on service-oriented architectures, and black hole attacks on mobile ad hoc networks (Miede & Nedyalkov, 2010).

In networking, systems need to ensure rapid data transmission to minimize traffic and prevent delays for users. In a perfect scenario, using Dijkstra's Algorithm to find the most efficient path would be optimal for faster data transfers. Dijkstra's Algorithm efficiently determines the shortest paths within a network, optimizing data packet routing for faster delivery (Cormen et al., 2009). For instance, Dijkstra's Algorithm can calculate the shortest path between nodes in a network, ensuring that data packets follow the quickest and most efficient route to their destination. However, in real-world scenarios, distributed systems are prone to various vulnerabilities, such as node failures, network congestion, or interruptions in connectivity. Since Dijkstra's Algorithm operates on a static graph, it is not well-suited for dynamic environments where paths change frequently due to such interruptions. Additionally, the security schemes in the distributed storage systems mainly concentrate on data security in terms of integrity and availability of the data in the network (Harinath D. et al, 2017).

Finite automata (FA), or finite-state machines (FSM), provides a framework for understanding and managing the complexities inherent in distributed systems. Their capacity to model systems with a finite number of states and transitions makes them a potent tool for design, analysis, and verification. According to Mishchenko and Brayton (n.d), non-determinism allows for a compact representation of circuit behaviors, which is essential in logic synthesis and optimization processes. A network with non-deterministic behavior offers flexibility, ensures availability, and helps maintain a balanced approach to managing data packets within the system. Rerouting with NFA allows the system to dynamically change its path and can easily adapt to unexpected disruptions or changes in the network. By leveraging non-determinism, the system can evaluate multiple potential paths simultaneously, ensuring that data packets are not delayed or lost when one route becomes unavailable. A study conducted by Alexander Power and Gerald

Kotonya in 2019, where they explored the fault tolerance capabilities of NFA to enhance the reliability of IoT systems. Their approach termed Complex Patterns of Failure (CPoF), utilizes NFA within Complex Event Processing (CEP) to provide a modular and reusable framework for error detection and recovery in dynamic environments. This aligns with the idea that non-determinism allows for a compact representation of circuit behaviors, as NFAs can effectively categorize system defects through their Vulnerabilities, Faults, and Failures (VFF) framework.

Finite automata can be applied for protocol modeling and analysis in network protocols because they aid in describing the system states, transitions, and interactions. Gribkoff (2013) states that finite automata capture the inner states of systems and are applicable in protocols such as TCP and TLS. These protocols execute their phases, which include setting up a connection, data transfer, and closing the connection. These phases have rules that enable proper communication.

Another use is by Ashraf Abdel-Karim Helal Abu-Ein et al. (2011), which mentions the application of finite automata in network protocol testing. This research has an implication that it can apply in simulating the performance of protocols in detecting states mismatch, wrong transitions or even responses. All of these tests ensure that such protocols function as desired, also at challenging conditions such as saturated loads or corrupted packets.

Finite automata provide a strong foundation for checking protocol specifications and, thus, enhancing security by clearly defining states, inputs, and outputs. The vulnerability found by Abu-Ein et al. (2011) through automata models was related to unauthorized state transitions or packet loss, which would have resulted in protocol failures or security issues. Finite automata

test and model to assist developers in constructing effective and reliable communication protocols with a high degree of security.

Liu et al. (2024) has a research study which presents a model which uses temporal logical modeling for capturing behavior patterns in distributed systems. While being concerned with deep learning techniques, the underlying principles of state representation and transitions are pretty close to that of finite automata. This approach will be able to model the temporal dependencies within system logs which would allow the combination of temporal analysis with finite automata for anomaly detection in the distributed environment. The study helps understand how sequences of events can be effectively processed.

Zhao et al. (2021) study the anomaly detection capability in distributed systems by carrying out an analysis of system log. This approach models events in log as state transitions, a process that analogously mimics finite automata in tracking and analysing sequential patterns of behavior in a system. Through this study, the scientists demonstrated how anomalies could be identified by representing log entries as states and their interaction as transitions. This work points out the feasibility of finite automata for monitoring distributed systems and can be used to find some unexpected deviations that could imply cyber threats or anomalies.

Finite automata (FA), including Deterministic Finite Automata (DFA) and Nondeterministic Finite Automata (NFA) are both types of **Finite State Machines**, and are fundamental concepts in theoretical computer science with practical applications in network security. Their relationship to network security lies in their ability to model, analyze, and implement security mechanisms that ensure the integrity, confidentiality, and availability of systems. Protocol modelling is a crucial step in designing security protocols. It contributes to

diminishing ambiguity and misinterpretation of protocol specifications. For example, modelling a protocol using a finite-state machine can help to understand how it will interact with the changes and how it will behave with invalid inputs. Modeling with finite-state machines helps to understand the behaviour of complex protocol. Also, it offers accurate results and provides a clear perception of the system characteristics (Aljeaid, Ma, & Langensiepen, 2015).

When there's no intrusion or interruption, the network operates normally, the system uses a Deterministic Finite Automaton (DFA)-like structure, where the path selection is straightforward and follows a deterministic rule and Dijkstra's Algorithm identifies the shortest and fastest path for packet transmission to optimize performance. Considering that the Dijkstra algorithm is globally optimal, it can select the routing path with the minimum transmission loss of each link in a network (Zheng, Y.-L., et al., 2021, January 5). On the other hand, when an intrusion or interruption is detected, The system transitions into an Nondeterministic Finite Automaton (NFA)-like behavior, exploring multiple possible paths simultaneously to find an alternative route for packet transmission.

2.2. Related Studies

The application of finite automata (FA) and finite state machines (FSM) in network security has been extensively explored in various domains, demonstrating their potential for enhancing cryptographic protection, intrusion detection, and network protocol optimization. The following studies provide significant insights that directly contribute to the foundation and advancement of our research on optimizing network security protocols using finite automata.

A common theme among these studies is the use of FA-based techniques to improve network security mechanisms. Sharipbay et al. (2023) focused on developing cryptographic protection methods using finite automata models, emphasizing reversible automata to enhance security and key management. Similarly, James (2023) explored finite-state attack modeling in Smart Home IoT security, analyzing worst-case vulnerabilities and proposing iterative security fortifications to strengthen system resilience. Abu-Ein et al. (2011) investigated FSM-based network protocol testing, identifying protocol errors and optimizing test sequences to enhance security and reliability. Meanwhile, Vespa and Weng (2011) examined deterministic finite automata (DFA) optimization for scalable pattern matching in network intrusion detection systems (NIDS), focusing on memory-efficient encoding and rapid threat detection. These studies collectively reinforce the feasibility of FA-based security mechanisms, supporting non-deterministic routing, attack prevention, and real-time anomaly detection in distributed networks.

Each study employed distinct yet complementary methodologies that can be adapted to our research. Sharipbay et al. (2023) adopted a multi-phase approach, including mathematical cryptographic analysis, algorithm development for reversible automata, and software implementation for FA-based cryptosystems. James (2023) used a graph-based attack modeling framework, constructing finite-state attack graphs, analyzing worst-case vulnerabilities with the Common Vulnerability Scoring System (CVSS), and implementing iterative security fortification using shortest-path algorithms. Abu-Ein et al. (2011) applied FSM modeling to network protocols, defining state transitions, error detection mechanisms (output, transition, and state errors), and optimized test sequences to validate protocol security. Vespa and Weng (2011) developed DFA-based security engines, employing state characterization metrics,

memory-efficient encoding (self-addressable, character-aware, and split-level encoding), and high-performance pattern matching architectures for intrusion detection. These methodologies offer valuable techniques for FA-driven security implementations, including adaptive routing algorithms, graph-based attack detection, and protocol fortification—all of which are crucial for our study's approach to enhancing network security.

The studies collectively highlight the effectiveness of finite automata-based security models. Reversible FA models improve cryptographic security by complicating key decipherability, as demonstrated by Sharipbay et al. (2023). Finite-state attack modeling enhances threat predictability, enabling proactive security strategies, as explored by James (2023). FSM-based protocol validation strengthens network reliability and error detection, according to Abu-Ein et al. (2011). Furthermore, optimized DFA significantly reduces memory consumption (by over 80%) and accelerates threat detection in intrusion detection systems, as reported by Vespa and Weng (2011). These findings directly contribute to our research by providing proven methodologies for FA-driven security mechanisms, reinforcing the potential for non-deterministic routing to mitigate cyber threats.

The insights from these studies play a crucial role in refining our FA-based security model. Cryptographic security principles from reversible FA (Sharipbay et al., 2023) can be integrated into secure routing algorithms, preventing attackers from predicting network pathways. Finite-state attack modeling (James, 2023) aligns with our approach to attack detection and anomaly identification, ensuring that non-deterministic routing remains resilient against worst-case vulnerabilities. FSM-based protocol testing techniques (Abu-Ein et al., 2011) can be extended to validate and optimize FA-driven routing and security protocols.

Memory-efficient DFA optimizations (Vespa & Weng, 2011) can enhance pattern recognition in intrusion detection, allowing for real-time adaptive security responses. By synthesizing these findings, our research aims to develop a robust, scalable, and adaptive FA-based security framework for distributed networks, ensuring unpredictability, efficiency, and resilience against evolving cyber threats.

2.3. Synthesis of the Review of Literature and Studies

Literature 1:

Title and Author(s): ***A Brief Introduction to Distributed Systems*** by Maarten van Steen and Andrew S. Tanenbaum

- Summary: The paper introduces distributed systems, which consist of interconnected autonomous computers appearing as a single coherent system to users. The authors discuss the rapid evolution of computing power, the rise of high-speed networks, and miniaturization leading to the widespread deployment of distributed systems. They explain the fundamental features, such as autonomy and coherence, along with their design goals like resource sharing, transparency, openness, and scalability. Key challenges such as managing failure, synchronization, and consistency are highlighted, alongside the role of middleware to simplify development. The authors also delve into the different types of distributed systems, including high-performance systems, information systems, and pervasive systems.
- Learning Outcome: Readers will gain an understanding of the foundational concepts and challenges in distributed systems. They will learn about design goals, including resource

accessibility and distribution transparency, as well as key middleware services like communication and reliability. The document also introduces practical applications and architectures like cluster, grid, and cloud computing. By the end, readers will recognize the complexity of developing distributed systems and the need to balance trade-offs like transparency and performance.

- Open Problems: Synchronization and coordination without a global clock are difficult, particularly in systems with independent nodes. Scalability issues persist, especially in geographical and administrative contexts, where network latency, trust, and conflicting policies pose problems. Achieving consistent replication and fault tolerance while maintaining performance is still an open area of research. As distributed systems evolve, integrating transparency with flexibility and security across various platforms continues to demand innovative solutions.

Literature 2:

Title and Author(s): ***A DSL Framework for Policy-Based Security of Distributed Systems*** by Hédi Hamdi and Mohamed Mosbah

- Summary: The paper showed the challenge of securing distributed systems, emphasizing how diverse environments, data types, and communication layers complicate implementing effective security measures. The authors propose a domain-specific language (DSL) framework for specifying, verifying, and implementing security policies. Their approach aims to create modular security policies independent of the system's underlying architecture. This ensures that developers, even those without specialized expertise in security, can define and apply robust security measures. The framework's

modularity and abstraction make it adaptable to various distributed systems, addressing their unique requirements.

- Learning Outcome: Readers will understand the importance of a policy-based approach in addressing distributed system security issues. They will gain insights into the challenges associated with securing both communication and application layers. The framework presented illustrates how DSL can simplify the specification and implementation of modular security policies. Readers will also appreciate the abstraction that allows non-experts to develop security mechanisms, making this approach accessible and practical in real-world scenarios.
- Open Problems: Ensuring seamless integration of policies in real-time scenarios and minimizing performance trade-offs are areas that need further exploration. Additionally, as threats evolve, the DSL framework must adapt to incorporate predictive security measures and automate responses to unexpected vulnerabilities.

Literature 3:

Title and Author(s): ***A Generic Metamodel for IT Security Attack Modeling for Distributed Systems*** by André Miede, Nedislav Nedyalkov, Christian Gottron, André König, Nicolas Repp, and Ralf Steinmetz

- Summary: The paper addresses the challenge of understanding and discussing IT security in distributed systems, emphasizing the gaps in communication between domain specialists and IT experts. The authors propose a generic metamodel that captures core IT security concepts and their interrelationships, focusing on attack scenarios. The metamodel is applied to various distributed system contexts, including peer-to-peer

systems, service-oriented architectures, and mobile ad hoc networks. By providing a structured framework, the study enables a clearer understanding of security issues and facilitates better collaboration among stakeholders involved in developing security-critical IT systems.

- Learning Outcome: Readers will learn the importance of a metamodel approach to bridge the communication gap between IT security experts and other stakeholders. They will understand how the proposed framework can analyze and model IT security attacks across different distributed system scenarios. This allows them to identify potential threats and design more robust countermeasures for secure IT systems, especially in complex environments like mobile and service-oriented architectures.
- Open Problems: Future work is needed to adapt it to the evolving nature of cyber threats and emerging technologies. Another open challenge is improving scalability and usability to address increasingly complex and dynamic distributed systems. Integrating this model with automated tools for real-time threat detection and mitigation remains an area for further research and development.

Literature 4:

Title and Author(s): ***A Review on Security Issues and Attacks in Distributed Systems*** By Depavath Harinath, P. Satyanarayana, and M. V. Ramana Murthy

- Summary: The paper explores the security challenges faced by distributed systems, which are widely used in various fields due to their ability to share resources and computing power efficiently. It explains different types of distributed systems, including cluster computing, grid computing, distributed storage, and distributed databases. The authors

highlight security risks such as unauthorized access, data breaches, and system attacks, including Distributed Denial of Service (DDoS) and identity attacks. Various security mechanisms, including authentication methods like Kerberos and firewall protection, are discussed to address these challenges. The paper emphasizes that securing distributed environments is complex due to their open nature and the use of public resources.

- Learning Outcome: Readers will gain an understanding of the different security risks that distributed systems will encounter and the techniques that will be used to mitigate them. They will learn about the importance of securing computing clusters, grid systems, storage networks, and databases through encryption, authentication protocols, and intrusion detection systems. The paper will provide insights into how organizations will implement security measures like firewalls and multi-level access control to protect their infrastructure. Readers will also understand how attacks such as DDoS and identity theft will impact distributed systems and how ongoing research will work toward developing more robust security models.
- Open Problems: Challenges remain in ensuring the adaptability and scalability of security solutions in distributed environments. The increasing sophistication of cyber threats, such as advanced persistent threats and zero-day attacks, poses a challenge for existing security models. Another open problem is the balance between security and system performance, as implementing strong security protocols can sometimes reduce efficiency. Ensuring seamless security in cloud-based distributed systems and handling the evolving nature of cyber threats remain critical areas for future research.

Literature 6:

Title and Author(s): ***A Theory of Non-Deterministic Networks*** by A. Mishchenko and R.K. Brayton

- Summary: The paper presents a theory for representing and manipulating non-deterministic multi-level networks. It explains how non-deterministic networks offer greater flexibility in circuit design compared to deterministic binary networks. The study explores different ways to interpret a non-deterministic network's behavior, showing how these interpretations align when the network operates deterministically. The paper also discusses network operations such as node minimization, elimination, and decomposition while ensuring that modifications maintain the network's intended behavior. The proposed theory is implemented in the MVSIS system, where comparisons are made to highlight the benefits of using non-deterministic networks in circuit optimization.
- Learning Outcomes: Readers will gain a deeper understanding of how non-deterministic networks can be used to optimize circuit design. They will learn how different interpretations of non-deterministic behavior influence circuit operations and how modifications can be made without compromising functionality. Additionally, they will be able to explore potential applications of non-deterministic networks in advanced computing architectures and digital hardware implementations.
- Open Problems: A key challenge in non-deterministic networks is ensuring that modifications do not introduce unintended behaviors, especially when applied to large-scale circuits. Further research is required to develop techniques that integrate non-deterministic principles into modern circuit design workflows while maintaining computational efficiency.

Literature 7:

Title and Author(s): ***Complex Patterns of Failure: Fault Tolerance via Complex Event Processing for IoT Systems*** by Alexander Power, Gerald Kotonya

- Summary: The paper addresses the challenge of fault tolerance (FT) in IoT systems, where existing FT mechanisms are often static, tightly coupled, and inflexible. It introduces Complex Patterns of Failure (CPoF), a method that enhances FT support using Complex Event Processing (CEP). The study defines system defects through a Vulnerabilities, Faults, and Failures (VFF) framework and uses non-deterministic finite automata (NFA) to implement error-detection strategies. CPoF is tested in an automated agriculture system, where it effectively identifies different types of errors, including reasonableness, timing, and reversal errors. The results demonstrate how CPoF can improve fault detection and response in dynamic IoT environments.
- Learning Outcomes: Readers will understand how Complex Event Processing can improve fault tolerance in IoT systems. They will learn about different types of system failures and how the Vulnerabilities, Faults, and Failures (VFF) framework can be applied to detect them. They will gain insight into how non-deterministic finite automata can enhance real-time error detection, leading to more resilient IoT infrastructures.
- Open Problems: The ability to scale this approach efficiently without adding excessive computational overhead remains a challenge. Ensuring that CPoF can adapt to new types of faults in real-time without requiring frequent manual updates. Further research is needed to refine this approach and evaluate its effectiveness in other IoT domains, such as healthcare and smart cities.

Literature 8:

Title and Author(s): ***Applications of Deterministic Finite Automata*** by Eric Gribkoff

- Summary: The paper explores practical applications of Deterministic Finite Automata (DFA) beyond theoretical studies, highlighting their relevance in computing and engineering. DFAs are widely used in protocol analysis, text parsing, video game character behavior, security analysis, CPU control units, natural language processing, and speech recognition. The study also discusses their role in mechanical devices such as elevators, vending machines, and traffic-sensitive lights. By examining real-world use cases, the paper demonstrates the importance of DFA in both software and hardware systems.
- Learning Outcomes: Readers will recognize the practical applications of DFA in various computing fields, from software development to hardware automation. They will gain an appreciation for how DFA principles are used in everyday technologies and how they contribute to efficient system design.
- Open Problems: Future research could explore optimizing DFA for more complex decision-making tasks in artificial intelligence and machine learning. Additionally, integrating DFA with quantum computing models may open new possibilities for automata-based computing.

Literature 10:

Title and Author(s): ***Using Finite State Machine at the Testing of Network Protocols*** by Ashraf Abdel-Karim Helal Abu-Ein, Hazem (Moh'd Said) Abdel Majid Hatamleh, Ahmed A.M. Sharadqeh

---

- Summary: The study explores the use of Finite State Machines (FSM) as a model for testing network protocols, particularly in ensuring compliance and compatibility of IPv6 protocols. The paper highlights how FSM can help detect errors in protocol operations and improve test sequence generation for better efficiency. The researchers discuss the importance of formalizing network protocols using FSM theory, presenting a structured way to analyze protocol behaviors and identify potential faults. Additionally, the paper introduces SDL (Specification and Description Language) as a tool to generate test sequences, which is a crucial step in automating the testing process. The study concludes that FSM-based models provide a reliable framework for verifying network protocol functionality while acknowledging the need for further research on test classification and sequence optimization.
- Learning Outcomes: Readers will gain an understanding of how FSM can be applied in network protocol testing, particularly in detecting errors and ensuring compatibility. They will be able to recognize the significance of formalizing protocols and how FSM-based models help in structuring test cases. Additionally, they will develop insights into using SDL as a tool for test sequence generation, which will be useful in automating network testing processes. Readers will also be encouraged to explore optimization techniques for enhancing the efficiency of test sequences in future research.
- Open Problems: One open problem is the need for further refinement in optimizing test sequence generation to ensure complete protocol coverage while minimizing redundancy. Another challenge is balancing security constraints with the need for effective testing, especially in protocols like IPv6 that incorporate safety mechanisms. Additionally, adapting FSM-based models for complex and evolving network protocols remains a

challenge, requiring further research into scalable and adaptable testing frameworks. Integrating FSM-based testing with real-world network environments presents difficulties in ensuring that theoretical models align with practical implementations.

Literature 11:

Title and Author(s): ***LogSpy: System Log Anomaly Detection for Distributed Systems*** by Haoming Li, Yuguo Li

- Summary: The study presents LogSpy, an anomaly detection method designed for distributed systems using system log analysis. Since system logs contain crucial information about a system's runtime behavior, LogSpy leverages natural language processing (NLP) and clustering algorithms for log template mining and feature extraction. Traditional convolutional neural networks (CNNs) struggle with the small number of negative sample data in distributed systems, limiting their effectiveness in anomaly detection. To address this, LogSpy introduces an attention mechanism that improves detection accuracy while optimizing the detection window and computational complexity. Experiments conducted on the OpenStack test platform demonstrate that LogSpy performs better than traditional anomaly detection methods in identifying issues in distributed systems.
- Learning Outcomes: Readers will understand the role of system log analysis in managing distributed systems and how it helps detect anomalies. They will learn how LogSpy combines NLP and clustering techniques for log processing and anomaly detection. Future readers will also gain insights into the limitations of traditional CNN-based approaches and how attention mechanisms can enhance detection accuracy. Additionally,

they will recognize the importance of optimizing computational complexity in real-world system monitoring.

- Open Problems: An open problem from the paper is the challenge of handling diverse log formats across different distributed systems, which may require more adaptable preprocessing techniques. Another issue is improving the efficiency of anomaly detection models, as increasing complexity may impact real-time performance. Further research is needed to generalize LogSpy's approach to other platforms beyond OpenStack, ensuring its effectiveness in various environments. Integrating LogSpy with existing security frameworks could be explored to enhance its role in cybersecurity applications.

Literature 12:

Title and Author(s): ***Temporal Logical Attention Network for Log-Based Anomaly Detection in Distributed Systems*** by Yang Liu, Shaochen Ren, Xuran Wang, and Mengjie Zhou

- Summary: The paper introduces the Temporal Logical Attention Network (TLAN), a deep learning model for detecting anomalies in distributed system logs. Unlike traditional methods that focus only on time-series patterns or component relationships separately, TLAN combines both through an attention-based mechanism. The model has four main components: multi-scale feature extraction, temporal-logical modeling, cross-component correlation analysis, and adaptive anomaly detection. These features allow it to identify complex system failures involving multiple components and cascading issues. Experiments on synthetic datasets demonstrate that TLAN outperforms existing techniques, achieving a 9.4% improvement in F1-score and reducing false alarms by 15.3%.

- Learning Outcomes: Readers will understand the importance of log-based anomaly detection in distributed systems and the challenges posed by complex component interactions. They will learn how deep learning techniques, particularly attention-based mechanisms, can improve detection accuracy by modeling both temporal sequences and logical dependencies. Additionally, they will gain insight into adaptive anomaly detection methods that adjust to different system loads. The paper will also help readers recognize the significance of multi-scale feature extraction in detecting both short-term and long-term anomalies.
- Open Problems: Despite its effectiveness, TLAN has limitations that open avenues for further research. The model struggles with detecting anomalies in network-related logs, suggesting a need for improved modeling of distributed communication patterns. Scalability is another concern, as optimizing the temporal-logical modeling component could reduce computational overhead for large-scale deployments. Integrating network topology data and traffic flow information might enhance detection accuracy. Future research could also explore transfer learning to make the model more adaptable across different system environments.

Literature 13:

Title and Author(s): ***Analysis of Security Protocols using Finite-State Machines*** by Dania Aljeaid, Xiaoqi Ma, and Caroline Langensiepen

- Summary: This paper explores the use of finite-state machines (FSM) in analyzing security protocols, particularly focusing on their ability to detect protocol vulnerabilities. The study proposes a modified authentication protocol and demonstrates how FSM can

be applied to verify its security properties. The research also utilizes an extended finite-state machine (EFSM) model, which incorporates state variables to represent complex transitions and behaviors. Through FSM modeling, the paper evaluates different security aspects, such as message integrity, authentication, and session key agreement, ensuring the protocol remains secure even in cases of invalid input or time delays.

- Learning Outcomes: Readers will gain an understanding of how finite-state machines can be used to analyze and verify the behavior of security protocols. They will learn about the importance of protocol modeling in identifying vulnerabilities and improving authentication mechanisms. Additionally, readers will explore the concept of extended finite-state machines (EFSM) and how they can represent more complex state transitions. The paper will also help them understand the significance of integrity verification methods, such as encrypt-then-authenticate, in preventing attacks
- Open Problems: Although FSM modeling proves effective for security protocol analysis, it has some limitations. One challenge is its scalability when applied to highly complex protocols with numerous states and transitions. Additionally, FSM-based verification may not comprehensively model real-world attacks, such as man-in-the-middle attacks, without further enhancements. The paper suggests future research using Petri nets to simulate communication between clients and servers, as well as testing the modified protocol against various cyber-attacks to improve its robustness.

Literature 14:

Title and Author(s): ***Exploring a New Adaptive Routing Based on the Dijkstra Algorithm in Optical Networks-on-Chip*** by Yan-Li Zheng, Ting-Ting Song, Jun-Xiong Chai, Xiao-Ping Yang, Meng-Meng Yu, Yun-Chao Zhu, Yong Liu, and Yi-Yuan Xie

- Summary: The paper presents an optimized routing method for Optical Networks-on-Chip (ONoCs) using the Dijkstra algorithm. The study aims to minimize transmission loss and power consumption in optical chip multiprocessor (CMP) systems. Traditional routing methods often suffer from high power loss due to multiple optical elements. The proposed method applies the Dijkstra algorithm to determine the path with the least transmission loss, leading to better energy efficiency. Simulations show that this approach significantly reduces transmission loss and power consumption without noticeably affecting network latency or throughput. The findings highlight the importance of adaptive routing for improving the efficiency of optical interconnections in modern computing systems.
- Learning Outcomes: Readers will gain an understanding of how optical networks-on-chip function and why reducing transmission loss is critical for improving performance and energy efficiency. They will learn how the Dijkstra algorithm can be applied in network routing to optimize power consumption. Additionally, they will explore the trade-offs between power efficiency and network performance, such as latency and throughput. The paper will also introduce readers to simulation tools like OPNET, which are used to evaluate network efficiency under different configurations

- Open Problems: There are still challenges in scalability and adaptability to different network topologies. The model focuses on mesh-based networks, and further research is needed to evaluate its effectiveness in more complex architectures. Future studies could explore the integration of machine learning techniques to dynamically adjust routing paths based on real-time network conditions. Ensuring that the reduced power consumption does not negatively impact reliability and error rates in high-performance computing environments.

Chapter 3

METHODOLOGY

This chapter outlines the methodology that will be used in conducting the study, "Optimizing Network Security Protocols Using Finite Automata: A Case Study on Non-Deterministic Routing and Attack Detection in Distributed Systems." It details the research design, research locale, population and sampling procedure, data collection procedure, and data analysis methods. The chosen methodology ensures that the study is structured and systematically conducted to achieve its objectives effectively.

3.1. Research Design

The study follows a **descriptive** and **analytical** research design, where existing theories, algorithms, and case studies related to network security, finite automata, and routing mechanisms will be examined. Through this approach, the research will assess the theoretical viability of applying NFA to non-deterministic routing and attack detection in distributed systems. The study will focus on identifying

patterns, challenges, and opportunities presented in prior works while highlighting gaps in existing research that could be addressed in future studies.

3.2. Research Locale

Since this research does not involve experimental and empirical testing, it does not have a specific research locale or sample population. Instead, the study will explore relevant academic publications, research papers, conference proceedings, and authoritative sources that discuss the intersection of automata theory, network security, and distributed computing. These sources will serve as the foundation for understanding how finite automata principles, particularly non-determinism, can contribute to enhancing security mechanisms in modern network environments.

3.3. Population and Sampling Procedure

3.4. Data Collection Procedure

The data collection process involves an extensive literature review of related studies that discuss theoretical applications of finite automata in network security. The research will focus on materials that explore deterministic vs. non-deterministic routing, anomaly detection in distributed systems, and automata-based security models. Studies that discuss traditional security protocols, their limitations, and potential improvements through non-deterministic approaches will also be reviewed. By synthesizing these works, the study will establish a strong theoretical foundation for evaluating the feasibility and impact of NFA-based routing mechanisms in cybersecurity.

3.5. Data Analysis

The study will use a **comparative** and **evaluative** approach, wherein various theoretical perspectives will be examined to determine the strengths and weaknesses of deterministic and non-deterministic security models. This will involve identifying common themes, theoretical arguments, and conclusions drawn from previous research. The analysis will be structured to highlight key insights, including how NFA improves adaptability in network security, the challenges of implementing non-deterministic models, and the potential integration of finite automata in modern cybersecurity frameworks.

References

1. Abu-Ein, A. A.-K., Hatamleh, H., & Sharadqeh, A. A. M. (2011). Using finite state machine at the testing of network protocols. *ResearchGate, 5*(10), 956–960. https://www.researchgate.net/publication/294553580_Using_finite_state_machine_at_the_testing_of_network_protocols
2. Aljeaid, D., Ma, X., & Langensiepen, C. (2015). Analysis of security protocols using finite-state machines. *International Journal of Advanced Research in Artificial Intelligence (IJARAI), 4*(4). https://doi.org/10.14569/IJARAI.2015.040407
3. Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to algorithms*. MIT Press.
4. GeeksforGeeks. (2024, July 23). Security in distributed system. *GeeksforGeeks*. https://www.geeksforgeeks.org/security-in-distributed-system/
5. Gribkoff, E. (2013). Applications of deterministic finite automata. *ECS 120, UC Davis*. https://www.cs.ucdavis.edu/~rogaway/classes/120/spring13/eric-dfa.pdf
6. Hamdi, H., & Mosbah, M. (2009). A DSL framework for policy-based security of distributed systems. *IEEE*. https://ieeexplore.ieee.org/document/5325382
7. Harinath, D., Satyanarayana, P., & Murthy, M. V. R. (2017). A review on security issues and attacks in distributed systems. *Journal of Advances in Information Technology*. https://www.jait.us/uploadfile/2017/0316/20170316101644848.pdf
8. Lindsay, D., Gill, S. S., Smirnova, D., & Garraghan, P. (n.d.). The evolution of distributed computing systems: From fundamentals to new frontiers. *Lancaster University & Queen Mary University of London*.

https://eprints.lancs.ac.uk/id/eprint/151376/1/COMP_D_20_00070_R2_Camera_Ready_.pdf

9. Li, H., & Li, Y. (2020). LogSpy: System log anomaly detection for distributed systems. *Proceedings of the International Conference on Artificial Intelligence and Computer Engineering (ICAICE)*. https://doi.org/10.1109/ICAICE51518.2020.00073
10. Liu, Y., Ren, S., Wang, X., & Zhou, M. (2024). Temporal logical attention network for log-based anomaly detection in distributed systems. *Sensors, 24*(24), 7949. https://www.mdpi.com/1424-8220/24/24/7949
11. Miede, A., Nedyalkov, N., Gottron, C., König, A., Repp, N., & Steinmetz, R. (2010). A generic metamodel for IT security attack modeling for distributed systems. *IEEE*. https://ieeexplore.ieee.org/document/5438057
12. Mishchenko, A., & Brayton, R. K. (n.d.). A theory of non-deterministic networks. *IEEE*. https://ieeexplore.ieee.org/abstract/document/1257887
13. Power, A., & Kotonya, G. (2019). Complex patterns of failure: Fault tolerance via complex event processing for IoT systems. *IEEE*. https://ieeexplore.ieee.org/document/8875363
14. Van Steen, M., & Tanenbaum, A. S. (2016). A brief introduction to distributed systems. *Computing, 98*(10). https://doi.org/10.1007/s00607-016-0508-7
15. Zheng, Y.-L., Song, T.-T., Chai, J.-X., Yang, X.-P., Yu, M.-M., Zhu, Y.-C., Liu, Y., & Xie, Y.-Y. (2021). Exploring a new adaptive routing based on the Dijkstra algorithm in optical networks-on-chip. *Micromachines*. https://pmc.ncbi.nlm.nih.gov/articles/PMC7824910/