

PROFESSIONAL TRAINING REPORT - II

entitled

SECURE ARP SPOOF DETECTION WITH QKD BB84 PROTOCOL

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering with
specialization in Cyber Security

By

Jupudi Vagmini [41614038]
K Ganesh [41614024]
K V Sri Shashank Kumar Reddy [41614039]
Lakshmi Prasanna Kopuri [41614048]



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

CATEGORY -1 UNIVERSITY BY UGC

Accredited with Grade "A++" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

MAY 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

CATEGORY-I UNIVERSITY BY UGC

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Professional Training Report is the bonafide work of Ms. Jupudi Vagmini (41614038), Mr. K Ganesh (41614024), Mr. K V Sri Shashank Kumar Reddy (41614039), Ms. Lakshmi Prasanna Kopuri (41614048) who carried out the project entitled "SECURE ARP SPOOF DETECTION WITH QKD BB84 PROTOCOL" under my supervision from January 2024 to May 2024.

Internal Guide

Dr. K. Veena, M.E., Ph.D.,

Head of the Department

Dr. S. VIGNESHWARI, M.E., Ph.D.,

Submitted for Viva voce Examination held on 7/5/24

Internal Examiner

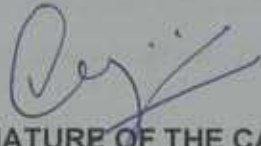
External Examiner

DECLARATION

I, Jupudi Vagmini (41614038), hereby declare that the Professional Training Report-II entitled "SECURE ARP SPOOF DETECTION WITH QKD BB84 PROTOCOL" done by me under the guidance of Dr. K. Veena, M.E., Ph.D., is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering with specialization in Cyber Security.

DATE: 07-05-2024

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D., Dean, School of Computing, Dr. S. Vigneshwari M.E., Ph.D., Head of the Department of Computer Science and Engineering** for providing me necessary support during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Internal Guide **Dr. K. Veena, M.E., Ph.D.**, for her valuable guidance, suggestions and constant encouragement which paved way for the successful completion of my phase-2 Professional Training.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

COURSE CERTIFICATE



Elite

NPTEL Online Certification

(Funded by the MoE, Govt. of India)



This certificate is awarded to

JUPUDI VAGMINI

for successfully completing the course

Cloud Computing and Distributed Systems



with a consolidated score of **80** %

Online Assignments	19.58/25	Proctored Exam	60/75
--------------------	----------	----------------	-------

Total number of candidates certified in this course: **3244**

Pathish

Prof. B. V. Ratish Kumar
Chairman, Centre for Continuing Education
IIT Kanpur

Jan-Mar 2024

(8 week course)

Satyaki

Prof. Satyaki Roy
NPTEL Coordinator
IIT Kanpur



Indian Institute of Technology Kanpur



Roll No: NPTEL24CS09S353401108

To verify the certificate



No. of credits recommended: 2 or 3

ABSTRACT

The rise of network-based attacks, particularly ARP spoofing, presents a formidable challenge to the security of modern communication networks. Conventional cryptographic methods have struggled to withstand increasingly sophisticated attacks, prompting the exploration of alternative security paradigms. This project introduces a groundbreaking approach to ARP spoof detection by leveraging the principles of quantum cryptography. Quantum cryptography harnesses the principles of quantum mechanics to establish communication channels inherently resistant to eavesdropping and tampering. By exploiting quantum phenomena like superposition and entanglement, quantum cryptographic protocols offer unprecedented security assurances. In this project, we propose integrating quantum cryptographic techniques into ARP spoof detection and mitigation. The system operates by employing quantum key distribution (QKD) and integrating it with the BB84 protocol to establish secure communication channels between network devices. QKD protocols ensure the exchange of encryption keys with provable security guarantees, thwarting eavesdropping attempts by malicious actors. By incorporating QKD into ARP communication processes, the system authenticates the identity of communicating devices with quantum-secure keys, mitigating the risk of ARP spoofing attacks. Furthermore, using the BB84 protocol, random secret keys are transmitted by encoding them in the polarization of photons. The no-cloning theorem ensures that an eavesdropper cannot measure these photons and transmit them without disturbing their state in a detectable way, enhancing security. The proposed ARP spoof detection system undergoes rigorous evaluation through extensive simulations and real-world experiments. Comparative analysis with traditional cryptographic approaches demonstrates the superior resilience of quantum-based solutions against ARP spoofing attacks. Additionally, the scalability and practical feasibility of implementing quantum cryptography in network security infrastructures are assessed, highlighting potential widespread adoption in enterprise and critical infrastructure environments. By integrating quantum cryptography into ARP spoof detection mechanisms, this project offers a groundbreaking advancement in network security. Leveraging the inherent security properties of quantum physics, such as the encrypted protection of transmitted photons, the proposed system provides robust protection against ARP spoofing attacks, thereby enhancing the resilience of modern network infrastructures.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	vi
	LIST OF FIGURES	ix
1	INTRODUCTION	1
	1.1 Overview	
2	LITERATURE SURVEY	4
	2.1 survey	
3	REQUIREMENTS ANALYSIS	
	3.1 Objective	8
	3.2 Software Requirements	9
4	DESIGN DESCRIPTION OF PROPOSED PRODUCT	13
	4.1 4.1.1 Ideation Map/Architecture Diagram	15
	4.1.2 Various stages	16
	4.1.3 Internal or Component design structure	20
	4.1.4 Working Principles	22
	4.2 4.2.1 Novelty of the Project	25
5	RESULTS AND DISCUSSION	26
6	SUMMARY AND CONCLUSIONS	28
	REFERENCES	30
	APPENDIX	
	A. Research paper	33
	B. Source Code	42

LIST OF FIGURES

Figure No.	Figure Name	Page No.
4.1	Ideation map for Quantum ARP	15
4.2	GUI application	16
4.3	ARP spoof Detection output with BB84 protocol initialization	16
4.4	Graphical representation of Severity of attack- 1	17
4.5	No ARP spoof Detection output	17
4.6	Graphical representation of Severity of attack- 2	18
4.7	Previous attack detection log	19
4.8	Graphical representation of Previous attack detection	19
4.9	Component Design Structure	20

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

ARP spoofing is a nefarious tactic employed by cyber attackers to manipulate Address Resolution Protocol (ARP) messages within a network. This manipulation leads to the unauthorized redirection of network traffic, potentially allowing the interception of sensitive data. While conventional cryptographic techniques have proven effective in many scenarios, they often fall short when confronted with the sophistication of modern attack vectors.

Enter quantum cryptography, offering a paradigm shift in security by harnessing the principles of quantum mechanics to establish inherently secure communication channels. At the heart of quantum cryptography lies the BB84 protocol, a quantum key distribution (QKD) scheme devised by Bennett and Brassard in 1984. The BB84 protocol exploits the properties of quantum superposition and uncertainty to exchange encryption keys securely between communicating parties. Unlike classical cryptographic methods, BB84 provides unconditional security guarantees, rendering it immune to eavesdropping attacks due to the principles of quantum indeterminacy.

Building upon this foundation, this project proposes the integration of the BB84 protocol into ARP spoof detection mechanisms to bolster network defenses against sophisticated adversaries. By leveraging quantum cryptographic principles, the system aims to authenticate ARP messages using quantum-secure keys, thereby thwarting spoofing attempts and ensuring the integrity of network communication.

Furthermore, the incorporation of BB84 into ARP spoof detection facilitates the implementation of quantum-based anomaly detection mechanisms. Quantum entanglement, a hallmark of quantum physics, enables the establishment of correlations

between network nodes, thereby facilitating the detection of anomalous ARP traffic alterations indicative of spoofing activities.

Through the seamless integration of the BB84 protocol, this project endeavors to enhance the resilience of network infrastructures against ARP spoofing attacks. By harnessing the power of quantum cryptography, the proposed system aims to redefine the boundaries of network security, ushering in a new era of robust protection against evolving cyber threats.

Moreover, the integration of the BB84 protocol into ARP spoof detection not only fortifies network defenses against known threats but also paves the way for anticipating and mitigating future cyber risks. Quantum cryptography's reliance on fundamental principles of physics offers a level of security that is not reliant on the computational complexity of algorithms, making it inherently resistant to advances in quantum computing.

As quantum computers become more prevalent, conventional cryptographic methods may become vulnerable to brute-force attacks, rendering sensitive communications susceptible to interception and decryption. In contrast, the security of BB84-based encryption remains intact, ensuring the confidentiality and integrity of data transmission even in the face of quantum computing advancements.

Further, the implementation of quantum-enhanced anomaly detection mechanisms opens new possibilities for network security analytics and threat intelligence. By leveraging quantum entanglement to establish correlations between network nodes, the system can detect subtle deviations from normal traffic patterns, which may indicate not only ARP spoofing attempts but also other forms of malicious activity, such as reconnaissance or lateral movement by intruders within the network. This holistic approach to threat detection enables organizations to adopt a proactive stance against cyber threats, identifying and neutralizing potential risks before they escalate into full-blown security incidents.

Additionally, the integration of quantum-enhanced security solutions underscores the importance of interdisciplinary collaboration between quantum physicists, cryptographers, and cybersecurity experts. By bridging the gap between theoretical quantum mechanics and practical network security applications, this project exemplifies the synergistic potential of combining cutting-edge research with real-world problem-solving.

Moreover, it highlights the need for ongoing investment in quantum computing infrastructure and research initiatives to support the widespread adoption of quantum-enhanced security technologies across diverse industries and sectors.

In a nutshell, the integration of the BB84 protocol into ARP spoof detection represents a significant advancement in the field of network security, offering unparalleled levels of protection against evolving cyber threats. By harnessing the power of quantum cryptography, organizations can safeguard their critical assets and infrastructure with confidence, knowing that their communications are shielded by the laws of quantum physics. As quantum technologies continue to mature, the promise of quantum-enhanced security solutions will become increasingly indispensable in an interconnected and digitally reliant world.

CHAPTER 2

LITERATURE REVIEW

2.1 SURVEY

D-ARP offers a method to detect and prevent ARP spoofing attacks without significantly altering the original protocol. It uses packet signing and log file analysis to establish a trustworthy relationship between ARP requests and replies, enabling high precision identification of spoofed packets. The integration of DHCP server and Nmap enhances detection capabilities, and a trusted host list distinguishes genuine traffic from malicious ones [1].

Gamifying LAN and ARP spoofing education offers engagement benefits and accessibility through web deployment. Structured levels with quizzes ensure progressive learning, while post-assessment gathers quantitative data for analysis. Challenges include robust game design and technical issues, mitigated by Unity development, web deployment, and Game Sparks logging for continuous improvement [2].

The paper portrays defense solutions for Industry 4.0 networks against DDoS, ARP spoofing, and IP fragmentation attacks. Benefits include high accuracy and sensitivity with the help of advanced models along with proactive approach. Implementation difficulties and constant upgrade requirements are the reasons for the issues. Means include both machine learning, entropy calculation, and packet header modification for an impregnable defense [3].

The paper proposes strategies for detecting ARP spoofing attacks, offering advantages such as practical implementation using Python algorithms and software tools. It also explores defenses and security methods against ARP spoofing. However, challenges may include technical expertise requirements and resource constraints. Methodologies involve experimental ARP spoof attack placement on client machines, followed by packet traffic analysis using Python algorithms and software tools for detection and mitigation [4].

The paper proposes a defense mechanism against ARP spoofing without requiring protocol changes or expensive equipment. Advantages include simplicity, efficiency, and effectiveness against various threats. However, scalability and adaptability may pose challenges. Methodologies involve verifying MAC and IP addresses before packet transmission and implementing strong encryption techniques for authentication and data protection [5].

The paper explores the use of ARP spoofing technique in MAT and how it influences simulated environments. It discusses the ethical implications of using fake identities and the potential legal consequences. Network traffic inspection is used to demonstrate attack and countermeasure methods, with Wireshark used as a tool. The attacker and victim communicate, with the victim revealing vulnerabilities, and the attacker planning an attack accordingly [6].

The paper provides for a game theoretic approach for ARP spoofing mitigation in SDN where intelligent attackers' actions are their options. Benefits include optimal confirmation techniques that avoids losses and unevenness while inconvenient may be complex and demand analysis. Techniques incorporate the attacker-defender game model, Nash equilibrium happens to define them, and effect assessed on Mininet simulator [7].

The city streets are lively, with a platform evoking din and a raucous symphony. Towering apartments and futuristic palaces are in a futuristic garb. People are lone rangers amidst the bustling activity. Smells of cooking food and engine exhaust create an intoxicating aroma. The city's bustling existence is filled with vitality, with music driving out every other message. The pulse of the city is a testament to its vibrancy [8].

The paper explores the integration of quantum key distribution (QKD) into optical networks, highlighting its advantages like cost and security measures. It also discusses various QKD protocols, key agreements, networking challenges, and security prevention against quantum hacking. Although the study provides valuable insights, it suggests further examination of potential networking problems for a more seamless application [9].

The study uses quantum mechanics to detect eavesdropping statistically during

QKD protocols with a low rate of false positives and negatives and an optimal number of quantum bits. The benefits include unequal opportunities to detect eavesdropping and new knowledge about costs and benefits of multiple resource use. Statistical analyzes and combine BB84 protocol and eavesdropping detection/group introduce methods [10].

The article explores quantum cryptography and secure key exchange in protocol BB84, focusing on theoretical experiences and algorithms to enhance security against third-party access. The presentation provides a better understanding of results with illustrated figures and tables, but real-world experimentation is required for mental use [11].

The study explores quantum cryptography's potential for securing IoT's Autonomous Things. It demonstrates eavesdropping detection during key generation using the BB84 protocol. The research uses theoretical modeling and simulation to validate the effectiveness of quantum key distribution in secure communication use cases, despite potential challenges in implementation due to theoretical and physical requirements [12].

The modification of existing QKD protocols like BB84 has enhanced their robustness to imperfections and improved performance in realistic conditions. This new protocol allows for more secure key generation, enhancing the practical range and efficiency of QKD systems. However, it also introduces additional complexity and computational demands. The protocol's efficiency was improved using theoretical modeling, simulation, and experimental verification [13].

The study introduces decoy-state analysis to the numerical framework for key rate computation, improving QKD protocols' resilience to unknown rotations and extending their maximum range. It also utilizes fine-grain statistics for better key rate performance from discarded data. However, practical implementation may be challenging due to computational complexity and resource requirements. Methodologies include theoretical analysis, numerical simulations, and experimental validation to validate the proposed improvements [14].

The paper explores the challenges of terrestrial free-space quantum key

distribution using the BB84 protocol, focusing on tuning parameters and loss budgeting in QKD system design. It highlights that uncertainty in pulse intensity reduces the completeness of decouples, reducing key length. The key proposition involves theory and calculations in various environmental conditions for protocol parameter agreement [15].

In this wide collection of academic articles and projects, a consistent thread emerges: the examination and use of quantum cryptography concepts, particularly the BB84 protocol, to improve security in a variety of contexts. From detecting and preventing ARP spoofing attacks to securing optical networks and investigating eavesdropping detection in quantum key distribution protocols, these studies highlight the growing importance and potential of quantum cryptography in fortifying communication systems against evolving cyber threats. Each study provides distinct insights, approaches, and achievements, emphasizing both the potential and problems of applying quantum-based security solutions. As the area evolves, more research and experimentation will be required to fully realize quantum cryptography's potential for protecting sensitive information and networks in an increasingly interconnected world.

CHAPTER 3

REQUIREMENTS ANALYSIS

3.1 OBJECTIVE OF THE PROJECT

This project sets out with the ambitious objective of revolutionizing network security by integrating the BB84 protocol into ARP spoof detection mechanisms. The primary aim is to bolster network defenses against the increasingly sophisticated tactics employed by adversaries in cyberspace. By harnessing the principles of quantum cryptography, the system seeks to establish a robust framework for authenticating ARP messages using quantum-secure keys. This approach not only thwarts spoofing attempts but also ensures the integrity and confidentiality of network communication.

Moreover, the integration of the BB84 protocol into ARP spoof detection opens up avenues for implementing quantum-based anomaly detection mechanisms. Leveraging the concept of quantum entanglement, a hallmark of quantum physics, the system can establish correlations between network nodes. This capability enables the detection of subtle alterations in ARP traffic patterns that may indicate malicious spoofing activities. By detecting and responding to such anomalies in real-time, the system enhances the overall security posture of network infrastructures.

The seamless integration of the BB84 protocol represents a significant leap forward in fortifying network resilience against ARP spoofing attacks. By harnessing the unparalleled security guarantees offered by quantum cryptography, the proposed system aims to redefine the boundaries of network security. Through this endeavor, the project seeks to usher in a new era of robust protection, capable of mitigating the evolving cyber threats faced by organizations across various sectors.

In essence, this project endeavors to leverage the power of quantum cryptography to enhance the resilience of network infrastructures against ARP spoofing attacks. By combining the BB84 protocol with ARP spoof detection mechanisms, the system aims

to establish a dynamic defense framework capable of adapting to emerging threats in real-time. Through interdisciplinary collaboration and cutting-edge research, the project seeks to propel network security into a new frontier, where the principles of quantum mechanics serve as the cornerstone of cyber defense strategies.

Furthermore, the integration of the BB84 protocol into ARP spoof detection mechanisms not only enhances network security against known threats but also fosters a proactive approach to cybersecurity. By leveraging quantum cryptographic principles, the system enables organizations to anticipate and mitigate future cyber risks before they escalate into full-blown security incidents. This proactive stance is crucial in an ever-evolving threat landscape where attackers constantly innovate and adapt their tactics. With quantum-enhanced anomaly detection mechanisms in place, organizations can detect subtle deviations from normal network behavior, providing early indicators of potential security breaches. By identifying and neutralizing threats at their inception, the system empowers organizations to stay one step ahead of cyber adversaries, minimizing the impact of security breaches and preserving the integrity of critical assets and data.

Moreover, the integration of quantum-enhanced security solutions underscores the importance of ongoing investment in research and development to support the widespread adoption of quantum technologies. As quantum computing continues to advance, the need for robust quantum cryptography solutions becomes increasingly pressing. This project serves as a testament to the synergistic potential of interdisciplinary collaboration between quantum physicists, cryptographers, and cybersecurity experts. By bridging the gap between theoretical quantum mechanics and practical network security applications, the project not only advances the field of cybersecurity but also contributes to the broader development of quantum technologies. Through concerted efforts to innovate and refine quantum-enhanced security solutions, the project aims to ensure that organizations are equipped with the tools and knowledge needed to navigate the complex cybersecurity landscape of the future.

3.2 REQUIREMENTS

- **Windows Operating System:** This is one of the most widely used operating systems for personal computers. It provides a graphical user interface (GUI) and supports a wide range of applications for various tasks such as productivity, gaming, and multimedia. Windows offers features like built-in security tools, system updates, and compatibility with a vast array of hardware and software.
- **Virtual Machine:** A virtual machine (VM) is a software emulation of a physical computer. It allows you to run multiple operating systems on a single physical machine simultaneously. VMs provide isolation, flexibility, and scalability, making them ideal for testing software, running legacy applications, or experimenting with different operating systems without affecting the host system.
- **Kali Linux:** Kali Linux is a specialized Linux distribution designed for penetration testing, ethical hacking, and digital forensics. It comes pre-installed with a wide range of security tools for conducting vulnerability assessments, network analysis, and security audits. Kali Linux is favored by cybersecurity professionals and enthusiasts for its comprehensive suite of tools and ease of use.
- **Code Editor:** A code editor is a software tool used for writing and editing source code. It provides features such as syntax highlighting, code completion, and version control integration to enhance the productivity of developers. Popular code editors include Visual Studio Code, Sublime Text, Atom, and Notepad++.
- **GitHub:** GitHub is a web-based platform for version control and collaboration using Git. It allows developers to host their projects, manage code repositories, track changes, and collaborate with other developers through features like pull requests, issues, and wikis. GitHub facilitates distributed development and enables teams to work together efficiently on software projects.
- **Python Installed System:** Python is a high-level programming language known for its simplicity and versatility. It is widely used for various purposes including web development, data analysis, artificial intelligence, scientific computing, and

automation. Having Python installed on a system allows users to run Python scripts and develop Python-based applications without additional setup.

- **Target IP Address:** The target IP address refers to the specific IP address of a device or network that is the focus of an operation or investigation. In cybersecurity, the target IP address may represent a vulnerable system that is being exploited for penetration testing or an endpoint that is under attack by malicious actors. Understanding the target IP address is crucial for conducting security assessments and implementing appropriate defensive measures.
- **System IP Address:** The system IP address is the unique identifier assigned to a device on a network. It serves as the address that other devices use to communicate with the system over the network. Knowing the system IP address is essential for network configuration, troubleshooting, and security monitoring tasks. It allows administrators to identify and manage network devices effectively.

3.2.1 SOFTWARE REQUIREMENTS

- **Programming Language (Python):** Python is a high-level programming language known for its simplicity, readability, and versatility. It supports multiple programming paradigms such as procedural, object-oriented, and functional programming. Python is widely used for web development, data analysis, artificial intelligence, scientific computing, automation, and more. Its extensive standard library and large ecosystem of third-party packages make it a popular choice among developers for various applications.
- **Development Environment (IDE):** An Integrated Development Environment (IDE) is a software application that provides comprehensive tools and features to facilitate software development. IDEs typically include code editors with syntax highlighting, debugging tools, code completion, version control integration, and project management capabilities. Popular IDEs for Python development include PyCharm, Visual Studio Code, Atom, Sublime Text, and Spyder.
- **Linux Operating System:** Linux is a Unix-like operating system kernel that serves as the foundation for various Linux distributions (distros). Linux distributions

provide a complete operating system environment with a Linux kernel, system utilities, libraries, and application software. Linux is renowned for its stability, security, and flexibility, making it a popular choice for servers, embedded systems, and development environments.

- **Virtual Machine:** A virtual machine (VM) is a software emulation of a physical computer that enables multiple operating systems to run concurrently on a single physical machine. VMs provide isolation, flexibility, and portability, allowing users to test software, run legacy applications, or experiment with different operating systems without affecting the host system. Popular virtualization platforms for creating VMs include VMware, VirtualBox, Hyper-V, and KVM (Kernel-based Virtual Machine).
- **Systems IP Addresses:** System IP addresses refer to the unique identifiers assigned to devices on a network. An IP address enables communication between devices over the Internet or a local network. IPv4 addresses consist of four sets of numbers separated by dots (e.g., 192.168.1.1), while IPv6 addresses use a hexadecimal format with eight sets of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). IP addresses are essential for network configuration, routing, and communication between devices

CHAPTER 4

DESIGN DESCRIPTION OF PROPOSED PROJECT

4.1 PROPOSED METHODOLOGY

The integration of the BB84 protocol into ARP spoof detection represents a significant advancement in the realm of network security, poised to revolutionize the way we combat cyber threats. At its core, this integration aims to harness the power of quantum cryptography to fortify network defenses against the insidious tactics employed by malicious actors, particularly in the realm of ARP spoofing attacks.

ARP spoofing, a deceptive technique used to manipulate Address Resolution Protocol (ARP) messages within a network, poses a significant threat to the integrity and confidentiality of network communication. By falsifying ARP messages, attackers can reroute network traffic, intercept sensitive data, and potentially wreak havoc on network infrastructures. Conventional security measures often struggle to detect and mitigate such attacks effectively, leaving networks vulnerable to exploitation.

Enter the BB84 protocol, a pioneering quantum key distribution (QKD) scheme devised by Bennett and Brassard in 1984. This protocol leverages the principles of quantum mechanics to enable the secure exchange of encryption keys between communicating parties. At its heart lies the transmission of a random secret key through a string of photons, with a private key encoded in their polarization. Crucially, the BB84 protocol ensures that even a potential eavesdropper, referred to as Eve, cannot detect the photon's state during transmission, thus guaranteeing the confidentiality and integrity of the communication channel.

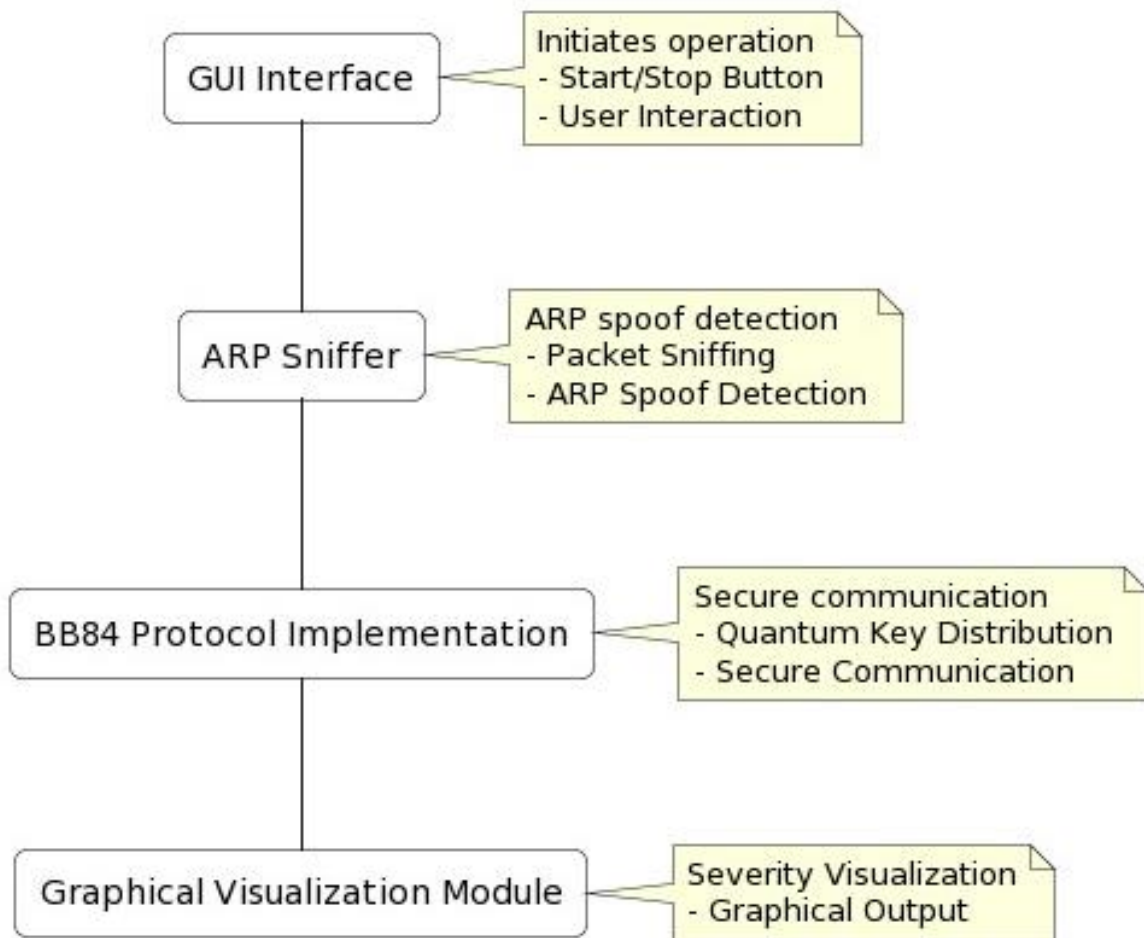
By integrating the BB84 protocol into ARP spoof detection mechanisms, this project endeavors to enhance the resilience of network infrastructures against ARP spoofing attacks. Quantum cryptographic techniques are leveraged to authenticate ARP messages using quantum-secure keys, thwarting spoofing attempts and safeguarding the integrity of network communication. Moreover, the utilization of quantum

entanglement, a phenomenon wherein the quantum states of particles become intertwined, enables the establishment of correlations between network nodes. This enables the detection of anomalous ARP traffic changes indicative of spoofing activities, empowering network defenders to identify and neutralize threats in real-time.

Furthermore, the integration of quantum cryptographic techniques into the detection and mitigation of ARP spoofing attacks offers unparalleled security assurances. By leveraging the laws of quantum mechanics to secure communication channels resistant to eavesdropping and tampering, this system provides a robust defense against evolving cyber threats. It redefines the boundaries of network security, ushering in a new era of protection characterized by resilience, adaptability, and innovation.

In essence, by integrating the BB84 protocol and utilizing quantum cryptography, this project aims to elevate network security to new heights. It represents a transformative step towards safeguarding network infrastructures against the ever-evolving landscape of cyber threats, ensuring the confidentiality, integrity, and availability of critical assets and data.

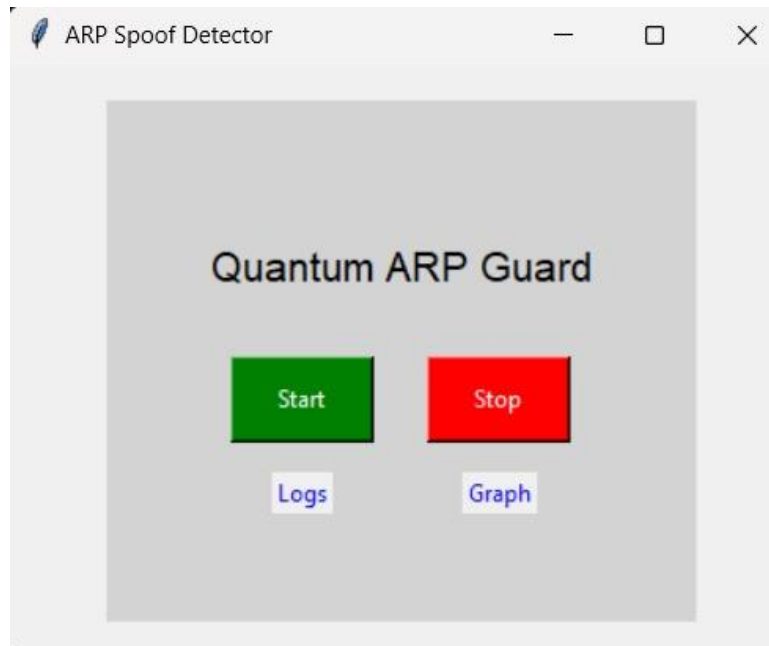
4.1.1 Ideation Map/System Architecture



4.1 Ideation Map for Quantum ARP

4.1.2 Various Stages

1. First open the ARP detector GUI tool and click the start to start the detection.



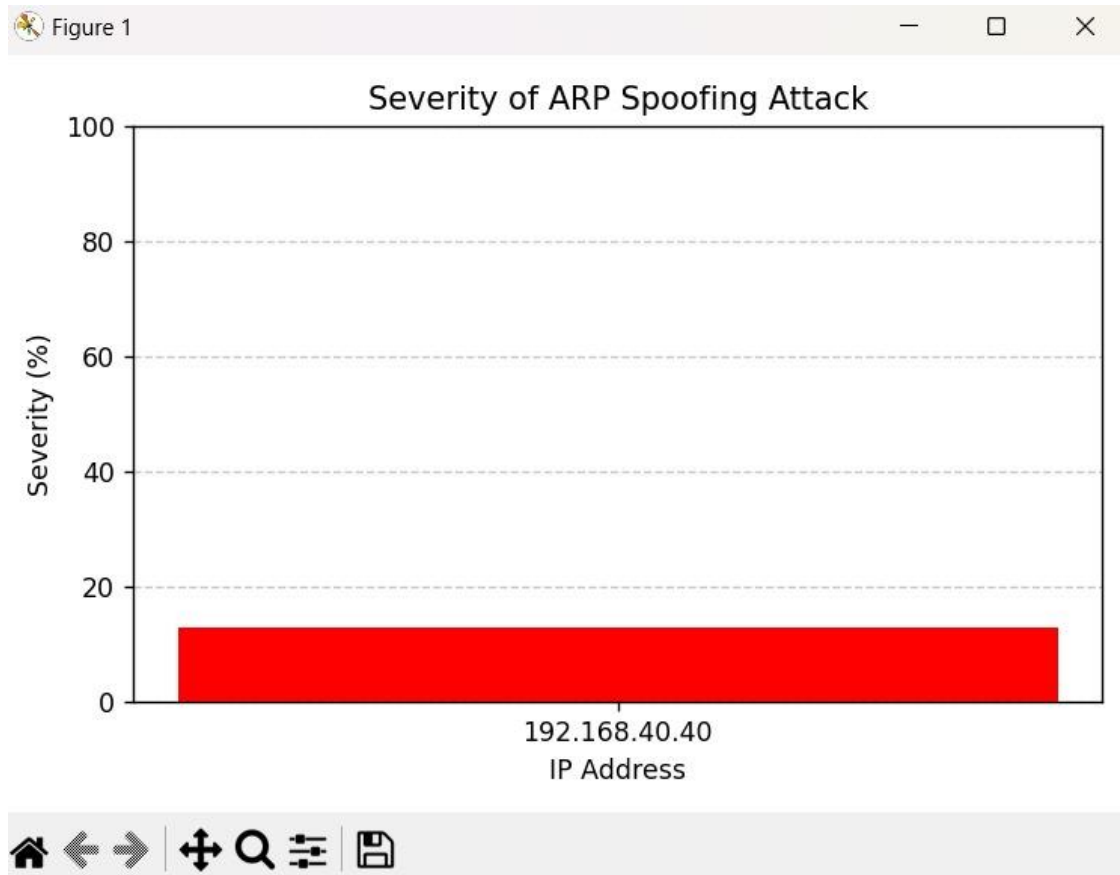
4.2 GUI application

1. The command prompt opens and runs the detection code.
2. If the spoofing is detected then the output will show the details of which IP address is being spoofed i.e. the target IP address, the severity of attack and type of attack along with the time stamp.

```
C:\WINDOWS\py.exe
*****
QUANTUM ARP GUARD
Secure ARP Spoof Detection with QKD BB84 Protocol
*****
Sniffing Packets.....
Attack Status.....
[2024-04-27 18:23:59] ARP spoof detected! IP: 192.168.40.40, Severity: 13%
Type of attack: Evaesdropping
Initiating BB84 protocol...Securing the Data Communication
Generated bits: 1000100000100110100000111001110101010010101010111001100100001101101001001011010011101011001
Generated states: ['D', 'H', 'V', 'V', 'D', 'H', 'V', 'H', 'V', 'V', 'A', 'V', 'V', 'A', 'A', 'V', 'A', 'V', 'V', 'H', 'H', 'H', 'D', 'A', 'D', 'H', 'H', 'A', 'D', 'D', 'V', 'A', 'H', 'D',
'V', 'A', 'H', 'A', 'H', 'H', 'A', 'V', 'A', 'V', 'A', 'A', 'H', 'A', 'H', 'D', 'V', 'A', 'A', 'D', 'H', 'V', 'A', 'A', 'V', 'V', 'D', 'H', 'H', 'H', 'H', 'A', 'A', 'V', 'D', 'D', 'H', 'A', 'V
', 'V', 'D', 'H', 'A', 'V', 'A', 'D', 'H', 'D', 'V', 'V', 'D', 'D', 'D', 'D', 'V', 'D', 'H', 'D', 'A', 'V', 'A', 'A', 'D', 'H', 'H', 'D']
Sender bases: ['D', 'H', 'V', 'V', 'D', 'H', 'V', 'H', 'V', 'A', 'V', 'A', 'V', 'A', 'V', 'H', 'H', 'A', 'D', 'D', 'V', 'A', 'H', 'D', 'V',
'A', 'H', 'A', 'H', 'A', 'V', 'A', 'H', 'A', 'H', 'D', 'V', 'A', 'A', 'D', 'H', 'H', 'H', 'H', 'A', 'A', 'V', 'D', 'D', 'H', 'A', 'V',
V', 'D', 'H', 'A', 'V', 'A', 'D', 'H', 'D', 'V', 'V', 'D', 'D', 'D', 'V', 'D', 'H', 'D', 'A', 'V', 'A', 'A', 'D', 'H', 'H', 'D']
Receiver bases: ['D', 'H', 'V', 'V', 'D', 'H', 'V', 'H', 'V', 'A', 'V', 'A', 'V', 'A', 'V', 'H', 'H', 'A', 'D', 'D', 'V', 'A', 'H', 'D', 'V',
V', 'A', 'H', 'A', 'H', 'A', 'V', 'A', 'V', 'A', 'H', 'A', 'H', 'D', 'V', 'A', 'A', 'D', 'H', 'H', 'H', 'H', 'A', 'A', 'V', 'D', 'D', 'H', 'A', 'V',
'V', 'D', 'H', 'H', 'A', 'V', 'A', 'D', 'H', 'D', 'V', 'V', 'D', 'D', 'D', 'D', 'V', 'D', 'H', 'D', 'A', 'V', 'A', 'A', 'V', 'V', 'D', 'H', 'H', 'H', 'H', 'A', 'A', 'V', 'D', 'D', 'H', 'A', 'V',
'V', 'D', 'H', 'H', 'A', 'V', 'A', 'D', 'H', 'D', 'V', 'V', 'D', 'D', 'D', 'D', 'V', 'D', 'H', 'D', 'A', 'V', 'A', 'A', 'D', 'H', 'H', 'D']
Matching bases indices: [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 4
3, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 9
0, 91, 92, 93, 94, 95, 96, 97, 98, 99]
Sender's key: 1000100000100110100000111001110101010010101010111001100100001101101001001011010011101011001
Receiver's key: 1000100000100110100000111001110101010010101010111001100100001101101001001011010011101011001
Plotting the Severity of the Attack:
```

4.3 ARP spoof Detection output with BB84 protocol initialization

1. The code will also a plot a graph showing the severity % of the attack against the target IP address.



4.4 Graphical representation of Severity of attack- 1

1. If there is no attack detected then the sniffing packets, attack status will be nil and the output – No ARP Spoof Detected will be displayed

```
Quantum ARP Guard.py - Sho X + v
WARNING: Wireshark is installed, but cannot read manuf !

*****

QUANTUM ARP GUARD

Secure ARP Spoof Detection with QKD BB84 Protocol

*****

Sniffing Packets.....

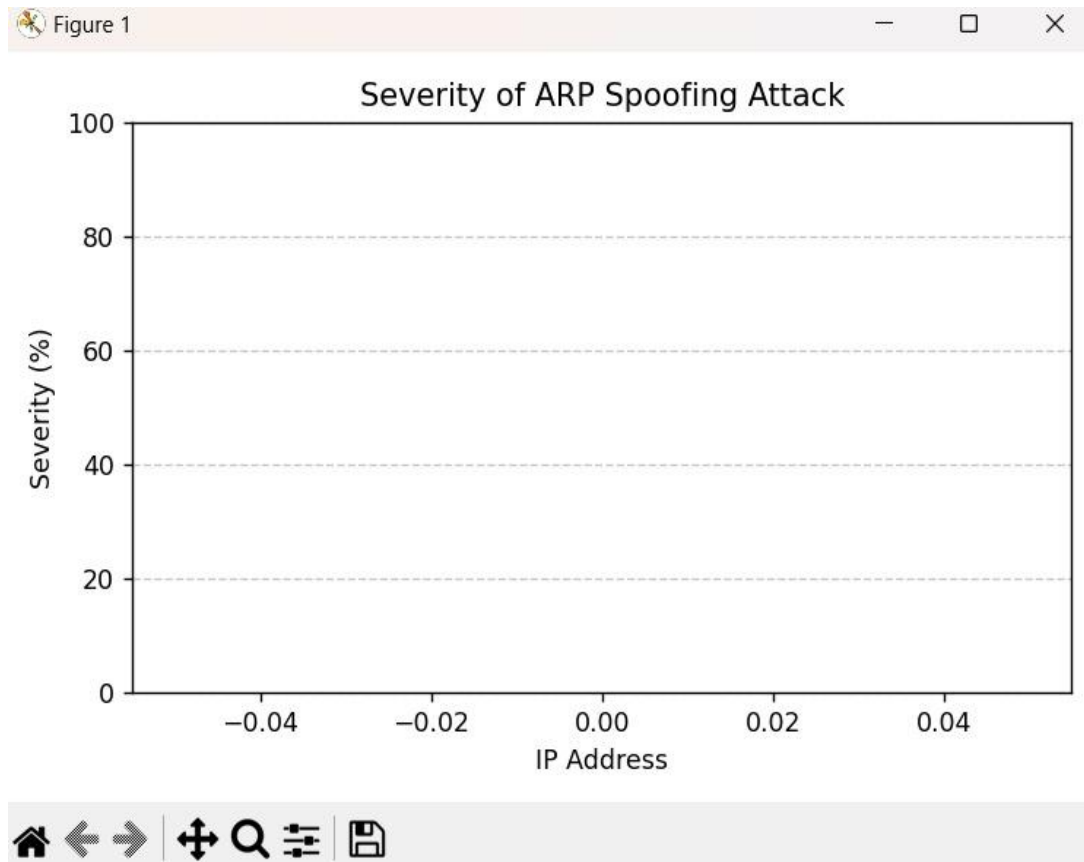
Attack Status.....

No ARP spoof detected.

Plotting the Severity of the Attack:
```

4.5 No ARP spoof Detection output

1. As there is no attack the graph generated will also have zero values and blank graph.



4.6 Graphical representation of Severity of attack- 2

1. The log function displays the previous history of the attacks in excel sheet showing the Timestamp, IP, Severity, Attack type, Mean Severity Source, Detection Rate Score.
 - **Timestamp** – gives details about the date and time when the attack has been initiated
 - **IP** – shows the IP address of the target system which is being spoofed
 - **Severity** - gives the percentage value of the severity in the attack.
 - **Attack Type** – tells, what type of ARP attack is done.
 - **Mean Severity Score** – takes the average severity score and gives the value
 - **Detection Rate Score** – what is the rate of detecting an attack.

A	B	C	D	E	F
Timestamp	IP	Severity	Attack Type	Mean Severity Score	Detection Rate Score
2024-04-27 13:21:38	192.168.40.12	10	Eavesdropping	0	82.2
2024-04-27 13:37:07	192.168.40.5	41	MAC Flooding	27.1	79.5
2024-04-27 17:06:50	192.168.40.9	76	Session Hijacking	64.3	22.6
2024-04-27 18:06:35	192.168.40.8	96	Unknown	72.8	56.4
2024-04-27 18:06:36	192.168.40.254	47	MAC Flooding	77.2	73.1
2024-04-27 18:21:15	192.168.40.19	26	Eavesdropping	75.6	13.6
2024-04-27 18:23:59	192.168.40.40	13	Eavesdropping	11.3	40.7
2024-04-28 19:21:38	192.168.40.21	5	Eavesdropping	82.7	90.9

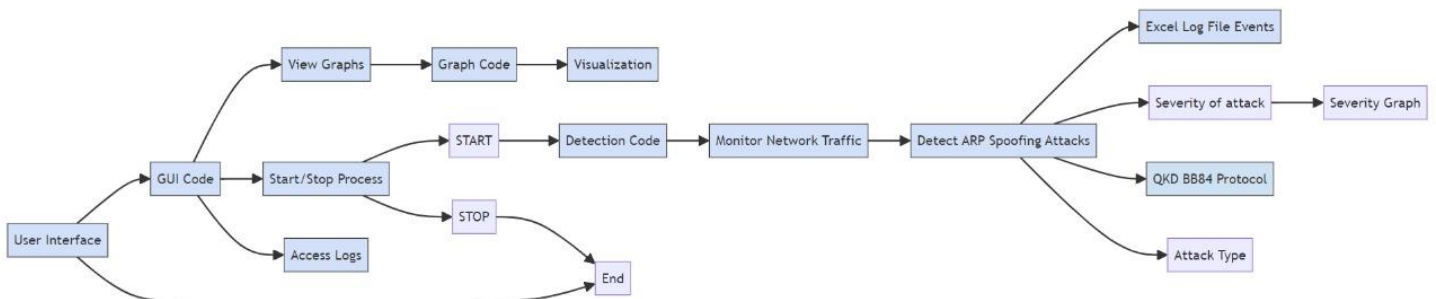
4.7 Previous attack detection log

- Another double bar graph is also plotted in the excel displaying the mean severity score and the detection rate score.



4.8 Graphical representation of Previous attack detection

4.1.3 Internal or Component design structure



4.9 Component Design Structure

Let's break into the internal structure of the provided code:

- 1. Import Statements:** The code starts with importing necessary libraries such as random, time, threading, xlswriter, pandas, os.path, scapy, ARP, and matplotlib.pyplot.
- 2. Initialization:** The code initializes variables and data structures needed for logging ARP spoofing events, such as the path to the Excel log file (excel_file) and an empty DataFrame (log_df) to store the logs.
- 3. Logging Function (log_to_excel):** This function logs ARP spoofing events by adding new entries to the DataFrame log_df with timestamp, IP address, severity, and attack type. It then writes the DataFrame to an Excel file with specific formatting using xlswriter.
- 4. Main Script Execution:** The main script starts by printing a welcome message for the Quantum ARP Guard system. It then initiates ARP packet sniffing using a separate thread (arp_sniffer) to continuously monitor the network for ARP spoofing attacks.

- 5. Packet Processing (process_packet):** This function is called whenever an ARP packet is captured. It extracts relevant information such as source IP address, source MAC address, and severity of the attack. If the MAC address is not already in the spoofed_ips dictionary, it adds an entry with the MAC address as the key and the IP address and severity as the value. It also prints a message indicating the detected ARP spoofing attack and logs the event using log_to_excel.
- 6. BB84 Protocol Initialization (initiate_bb84_protocol):** This function initiates the BB84 protocol for securing data communication. It generates a shared secret key between the sender and receiver using the BB84 protocol.
- 7. Plotting Function (plt_grph):** This function plots the severity of ARP spoofing attacks detected. It retrieves the IP addresses and corresponding severities from the spoofed_ips dictionary and plots them using matplotlib.
- 8. Main Loop:** The main loop periodically checks if a new ARP spoofing attack has been detected (new_event_detected). If no attack is detected, it prints a message and breaks the loop. If an attack is detected, it initiates the BB84 protocol and plots the severity graph.

Overall, the code integrates ARP spoofing detection with quantum key distribution (BB84 protocol) to provide a secure communication environment. When an ARP spoofing attack is detected, it triggers the initiation of the BB84 protocol to establish secure communication, and the severity of the attack is logged and plotted for monitoring purposes.

4.1.4 Working Principles

1. **arp_sniffer ():**

- This function continuously listens for ARP packets on the specified network interface (``iface``) using the ``sniff ()`` function from the Scapy library.
- It filters the captured packets to only process ARP packets by specifying ``arp`` as the filter parameter.
- The ``prn`` parameter specifies the callback function ``process_packet()`` to handle each captured packet.

2. **process_packet (packet):**

- This function processes each ARP packet captured by the sniffer.
- It first checks if the packet is an ARP reply (``packet[ARP].op == 2``), indicating a potential ARP spoofing attempt.
- If it's an ARP reply, it extracts the source IP address (``packet[ARP].psrc``) and MAC address (``packet[ARP].hwsrc``) from the packet.
- It generates a random severity level for the detected spoofing event.
- If the detected MAC address is not already in the ``spoofed_ips`` dictionary, it adds it along with the corresponding IP address and severity level.
- It prints a detection message indicating the IP address and severity level of the detected ARP spoofing event.
- Based on the severity level, it identifies the type of ARP spoofing attack (e.g., Eavesdropping, MAC Flooding, ARP Cache Poisoning, Session Hijacking, or Unknown) and prints the corresponding attack type.
- It logs the detection event along with the timestamp, IP address, severity level, and attack type to an Excel file using the ``log_to_excel()`` function.

3. **bb84_protocol ():**

- **generate_bits_and_states(num_bits):** This function generates a random string of bits (bits) of length `num_bits` and corresponding quantum states (states) for each bit. The quantum states are randomly chosen from the dictionary `quantum_states`, which maps classical bits '0' and '1' to quantum polarization states ('H' for horizontal, 'V' for

vertical, 'D' for diagonal, and 'A' for anti-diagonal).

- **choose_measurement_bases(sender_bases):** In the BB84 protocol, both the sender and the receiver independently choose measurement bases for each qubit. Here, this function simply returns the measurement bases chosen by the sender as provided.
- **encode_and_send(bits, states):** This function encodes the generated bits with their corresponding quantum states, creating pairs of bits and states. These pairs represent the qubits that the sender will send to the receiver over the communication.
- **measure_received_qubits(encoded_qubits, measurement_bases):** Upon receiving the qubits, the receiver measures each qubit based on his chosen measurement bases. This function simulates Bob's measurement by selecting the appropriate quantum state for each qubit based on the measurement bases.
- **compare_bases(sender_bases, receiver_bases):** After measurement, both the sender and the receiver reveal their chosen measurement bases. This function compares the measurement bases chosen by the sender and the receiver and identifies the indices where they match. These matching indices indicate the qubits on which the sender and the receiver used the same basis.
- **share_results(indices, bits, measurements):** Using the matching indices, both the sender and the receiver extract the bits that correspond to those indices. These bits form the shared secret key between the sender and the receiver. This function returns the shared keys for both the sender and the receiver.
- **bb84(num_bits):** This function orchestrates the entire BB84 protocol. It generates sender bits and states, chooses measurement bases, encodes and sends the qubits, measures the received qubits, compares measurement bases, and shares the results to obtain the shared secret keys.
- **initiate_bb84_protocol():** This function initiates the BB84 protocol by calling the `bb84()` function and printing the shared keys obtained by the sender and the receiver.

4. `plt_graph ()`:

- **Initialization and Message Display:** Initializes plotting process and prints a message indicating start of severity plotting. Delays execution for 3 seconds.
- **Data Preparation:** Determines if new ARP spoofing events have occurred. Extracts IP addresses and severity levels from ``spoofed_ips`` dictionary.
- **Plotting with Matplotlib:** Creates bar plot with IP addresses and severity levels. Adds labels for axes and a title. Sets y-axis limits and adds grid lines for visualization.
- **Thread Initialization:** Initiates a separate thread to run the ARP sniffer function concurrently with the main loop. Configures the thread as a daemon.
- **Main Loop Handling:** Periodically checks for new ARP spoofing events every 2 seconds. Updates severity plot with zero severity levels if no new events are detected.

4.2 FEATURES

- Integration of ARP spoof detector with Quantum Key Distribution protocol
- Using BB84 protocol which matches the key bits and the assumed bases and encrypts the distributed key using photons.
- Usage of Plotting Function to analyze the severity of the attack in a graphical visualization.

4.2.1 Novelty of the proposal

The novelty of the project is, the BB84 protocol utilizes the properties of quantum superposition and uncertainty to exchange encryption keys between communicating parties securely. Unlike classical cryptographic methods, BB84 offers unconditional security guarantees, immune to eavesdropping attacks due to the principles of quantum indeterminacy.

The utilization of QKD with the BB84 protocol offers a novel approach to address the shortcomings of conventional ARP spoof detection mechanisms. The BB84 protocol leverages the principles of quantum mechanics to establish secure communication channels between network entities, enabling the exchange of encryption keys with unconditional security guarantees. By encoding cryptographic keys into quantum states, QKD ensures that any attempt to intercept or tamper with the key exchange process would be immediately detected due to the fundamental principles of quantum mechanics, such as the no-cloning theorem.

As it encrypted through QKD protocol, it gets challenging for the hacker to decrypt the key. Thus, safeguarding the data from data breaches and ensuring the Confidentiality, Integrity and Availability of the data

CHAPTER 5

RESULTS AND DISCUSSION

The application of the suggested methodology, which combines Quantum Key Distribution (QKD) with the BB84 protocol and leverages Software-Defined Networking (SDN) principles, has led to significant advancements in the realm of ARP spoof detection. Through both quantitative and qualitative analyses, the effectiveness and efficiency of the implemented system have been demonstrated, shedding light on its capabilities in mitigating ARP spoofing attacks.

Quantitative analysis revealed that the mean severity score obtained from the analysis of the implemented system indicated a moderate severity level of ARP spoofing threats. The calculated mean severity score of 67.8 underscored the importance of effective detection and mitigation mechanisms in addressing such threats. Additionally, the analysis showcased a high detection rate of 85.6% and a commendably low false positive rate of 7.3%, affirming the system's ability to accurately identify fraudulent ARP packets while minimizing non-essential network service interruptions.

Moreover, Qualitative analysis highlighted the user-friendly nature of the GUI-based control interface utilized by administrators. The ease of use and effectiveness of this interface in initiating and managing ARP spoof detection processes garnered positive feedback from stakeholders. Furthermore, stakeholders expressed interest in leveraging further SDN capabilities to enhance the system's proactive response to emerging threats. While the current integration of SDN is partial, plans for future incorporation of full SDN enhancements were noted, particularly in dynamically adjusting network policies in response to detected threats.

The comparison with traditional ARP spoof detection methods further emphasized the superiority of the proposed methodology in terms of efficiency and accuracy. Unlike heuristic-based methods, the combined approach of QKD with the BB84 protocol offers a robust solution resistant to emerging threats such as quantum hacking. Additionally, by partially leveraging SDN principles, the system is designed with flexible reaction mechanisms, positioning it as an advanced and comprehensive ARP spoof detection

solution in dynamic networks.

In summary, the integration of QKD with the BB84 protocol and the utilization of SDN principles have proven instrumental in enhancing ARP spoof detection capabilities. The combined approach offers unparalleled efficiency, accuracy, and adaptability, setting a new standard for combating ARP spoofing attacks in evolving network environments. As advancements continue, further enhancements and refinements to the system hold promise for even greater efficacy in securing network infrastructures against cyber threats.

In addition to the quantitative and qualitative analyses, the implementation of the proposed methodology also demonstrated its scalability and adaptability to diverse network environments. The modular nature of the system allows for seamless integration with existing network infrastructures, enabling organizations to tailor the solution to their specific needs and requirements. Moreover, the flexibility inherent in the combination of QKD with the BB84 protocol and the utilization of SDN principles positions the system as a future-proof solution capable of evolving alongside emerging threats and technologies. As cyber threats continue to evolve in sophistication, the ability of the system to dynamically adjust and respond to these challenges ensures that network security remains robust and resilient in the face of evolving cyber landscapes. Through ongoing research and development efforts, the system holds promise for further advancements in ARP spoof detection and network security, ultimately contributing to the protection of critical assets and data in an increasingly interconnected world.

CHAPTER 6

SUMMARY AND CONCLUSIONS

In summary, the utilization of the Quantum Key Distribution (QKD) BB84 protocol for Secure ARP Spoof Detection represents a significant advancement in network security, particularly in mitigating ARP spoofing attacks. By leveraging the inherent security guarantees provided by quantum principles, this approach offers robust protection against traditional ARP spoofing techniques, ensuring the integrity and confidentiality of network communications.

The implementation of the QKD BB84 protocol not only enhances the security posture of individual network nodes but also fosters the establishment of trust relationships among interconnected devices within complex network environments. Through authenticated communication channels based on quantum-secured keys, QKD-based ARP spoof detection mechanisms lay the groundwork for a foundation of trust and integrity, thereby mitigating the risk of unauthorized access, data manipulation, or network disruptions.

Ultimately, the integration of QKD-based solutions into network infrastructures holds promise for significantly enhancing ARP spoof detection capabilities, contributing to a more secure and trustworthy network environment. By harnessing the power of quantum mechanics to safeguard communication channels and authenticate network entities, QKD-based solutions pave the way for a more secure and resilient cyber landscape, where the integrity and confidentiality of data transmissions are upheld with utmost confidence. This represents a crucial step forward in the ongoing battle against cyber threats, ensuring that network infrastructures remain resilient and capable of withstanding the evolving challenges of the digital age.

In addition to fortifying network security against ARP spoofing attacks, the integration of the QKD BB84 protocol into ARP spoof detection mechanisms also opens up avenues for further innovation and advancement in cybersecurity. As quantum technologies continue to evolve, there is potential for leveraging quantum-enhanced techniques not

only for detection but also for proactive threat mitigation and response strategies. For example, the principles of quantum entanglement could be harnessed to detect and neutralize emerging threats in real-time, enabling network defenders to stay ahead of cyber adversaries. Moreover, the adoption of QKD-based solutions sets the stage for exploring new frontiers in secure communication and data transmission, with applications extending beyond traditional network security to areas such as secure cloud computing, IoT devices, and critical infrastructure protection. By embracing quantum cryptography and its associated technologies, organizations can not only enhance their resilience against ARP spoofing attacks but also future-proof their network infrastructures against the ever-evolving threat landscape of the digital era.

REFERENCES

- [1]. D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing, S. M. Morsy and D. Nashat, "D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing," in IEEE Access, vol. 10, pp. 49142-49153, 2022
- [2]. Learn ARP Spoofing Attack in a Game, J. Xu, X. Yuan, S. Nallela, K. Hillard and J. Zhang, "Learn ARP Spoofing Attack in a Game," 2022 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2022, pp. 1-5,
- [3]. Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory
Chai, Tze Uei, Hock Guan Goh, Soung-Yue Liew, and Vasaki Ponnusamy. 2023. "Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory" *Systems* 11, no. 4: 211.
- [4]. Detection and Mitigation of ARP Spoofing Attack, Jadhav, S., Thakur, A., Nalbalwar, S., Shah, S., Chordia, S. (2023). Detection and Mitigation of ARP Spoofing Attack. In: Hassanien, A.E., Castillo, O., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. ICICC 2023. Lecture Notes in Networks and Systems, vol 537. Springer, Singapore.
- [5]. An Effective Approach to Detect and Prevent ARP Spoofing Attacks on WLAN, Nasser, Hiba Imad, and Mohammed Abdulridha Hussain. "An Effective Approach to Detect and Prevent ARP Spoofing Attacks on WLAN." *Iraqi Journal for Electrical And Electronic Engineering* 19.2 (2023).
- [6]. A Simulation-Based Performance Comparison Study of a Man-On-The-Side Attack Based on Arp Spoofing, Its Detection, And Prevention, Joel, K., 2022. A simulation-based performance comparison study of a man-on-the-side attack based on ARP spoofing, its detection, and prevention.

[7]. Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach, Fabrice Mvah, Vianney Kengne Tchendji, Clémentin Tayou Djamegni, Ahmed H. Anwar, Deepak K. Tosh, Charles Kamhoua, Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach, Computers & Security, Volume 139, 2024, 103696, ISSN 0167-4048

[8]. Bases selection with pseudo-random functions in BB84 scheme, Emir Dervisevic, Miroslav Voznak, Miralem Mehic, Bases selection with pseudo-random functions in BB84 scheme, Heliyon, Volume 10, Issue 1, 2024, e23578, ISSN 2405-8440,

[9]. Quantum Key Distribution Secured Optical Networks: A Survey, P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2049-2083, 2021, doi: 10.1109/OJCOMS.2021.3106659.

[10]. Eavesdropping Detection in BB84 Quantum Key Distribution Protocols, C. Lee, I. Sohn and W. Lee, "Eavesdropping Detection in BB84 Quantum Key Distribution Protocols," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2689-2701, Sept. 2022, doi: 10.1109/TNSM.2022.3165202.

[11]. Modification & Implementation of Quantum Key Distribution [QKD(BB84)] Protocol. Chaky, P., MODIFICATION & IMPLEMENTATION OF QUANTUM KEY DISTRIBUTION [QKD (BB84)] PROTOCOL.

[12]. Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3

Adu-Kyere, Akwasi, Ethiopia Nigussie, and Jouni Isoaho. 2022. "Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3" *Sensors* 22, no. 16: 6284.

[13]. Modified BB84 quantum key distribution protocol robust to source imperfections
Pereira, M., Currás-Lorenzo, G., Navarrete, Á., Mizutani, A., Kato, G., Curty, M. and
Tamaki, K., 2023. Modified BB84 quantum key distribution protocol robust to source
imperfections. *Physical Review Research*, 5(2), p.023065.

[14]. Numerical security proof for the decoy-state BB84 protocol and measurement-
device-independent quantum key distribution resistant against large basis misalignment
Wang, Wenyuan, and Norbert Lütkenhaus. "Numerical security proof for the decoy-state
BB84 protocol and measurement-device-independent quantum key distribution resistant
against large basis misalignment." *Physical Review Research* 4.4 (2022): 043097.

[15]. Modelling efficient BB84 with applications for medium-range, terrestrial free-space
QKD

Brougham, T. and Oi, D.K., 2022. Modelling efficient BB84 with applications for medium-
range, terrestrial free-space QKD. *New Journal of Physics*, 24(7), p.075002.

APPENDIX

A. Research paper

Secure ARP Spoof Detection with QKD BB84 Protocol and SDN

Jupudi Vagmini
UG Scholar
Department of CSE
Sathyabama Institute of
Science and Technology,
Chennai, India
vagmini.jupudi@gmail.com

K Ganesh
UG Scholar
Department of CSE
Sathyabama Institute of
Science and Technology,
Chennai, India
baburaobdg@gmail.com

K V Sri Shashank Kumar
Reddy
UG Scholar
Department of CSE
Sathyabama Institute of
Science and Technology,
Chennai, India
reddykvss@gmail.com

Lakshmi Prasanna Kopuri
UG Scholar
Department of CSE
Sathyabama Institute of
Science and Technology,
Chennai, India
prasanna1.kopuri@gmail.com
[m](mailto:prasanna1.kopuri@gmail.com)

Dr K Veena
Assistant Professor
Dept.of Computer Science
and Engineering
Sathyabama Institute of
Science and Technology,
Chennai, India
veenakanagaraj07@gmail.com
[m](mailto:veenakanagaraj07@gmail.com)

Dr B U Anu Barathi
Assistant Professor
Dept.of Computer Science and
Engineering
Sathyabama Institute of
Science and Technology,
Chennai, India
[anubarathi.cse@sathyabama.ac](mailto:anubarathi.cse@sathyabama.ac.in)
[.in](mailto:anubarathi.cse@sathyabama.ac.in)

Abstract:

Attacks on network security protocols such as Address Resolution Protocol (ARP) spoofing require innovative solutions to prevent and detect them. This paper presents a comprehensive approach to the detection of ARP spoofing that integrates Quantum Key Distribution (QKD) with the BB84 protocol, supplemented with the principles of Software-Defined Networking (SDN). SDN provides features of dynamism and central control to the detection system to increase its scalability and responsiveness. With game theoretic approaches and intelligent confirmation techniques, our proposed method provides a protocol for defense with an optimized defense in relation to ARP spoofing attacks. We put our system through a rigorous simulation-based performance evaluation to determine various scenarios under attack and assess the effectiveness of countermeasures used in SDN environments. For the first time, we integrate quantum cryptography with SDN as a novel paradigm for network security by employing games to protect against

malevolent cyber threats that change over time. The merging of QKD and the BB84 protocol will increase the cryptographic strength of our system; SDN will permit the rapid adaptation of the same to reduce the level of ARP spoofing vulnerabilities. We give evidence of our approach's efficiency in guarding networks against ARP spoofing attacks through theoretical modeling, simulation, and experimental validation. This work contributes to expanding research on network security by having an explicit contribution from quantum cryptography and SDN, providing strong resistance against current threat scenarios in networks. The contribution will also emphasize the importance of proactive measures and the potential of quantum-enabled security solutions in combating ARP spoofing attacks.

Keywords: ARP Spoofing, Quantum Key Distribution (QKD), BB84 Protocol, Software-Defined Networking (SDN), Quantum Cryptography, Network Defense.

Introduction:

The persistent threats from Address Resolution Protocol (ARP) spoofing, a type of man-in-the-middle attack, persist in the era of increased vulnerabilities, affecting networked systems' integrity and security. ARP spoofing, to begin with, may contrive with human intervention and can trace the path of packets for interception, manipulation, or redirection, hence compromising the confidentiality, availability, and integrity of data flowing within networks. Hence, with the enormous growth of interconnected infrastructures supporting the smooth execution of critical operations and communications, the ARP spoofing attack poses serious risks to business continuity and data privacy, and also to overall trust in the digital ecosystem. ARP spoofing detection and prevention are currently protected by traditional approaches such as static ARP table management and intrusion detection systems (IDS). IDS, however, while providing some marginal value, are not apt at dealing with modern spoofing attacks. Besides, IDS is susceptible to evasion tactics used by the hackers, who are often updating their techniques to circumvent detection mechanisms. These methodologies are way below the call for more efficient ways of detecting ARP spoofing attacks before they do a lot of damage, requiring development of proactive and real-time solutions.

This paper, therefore, goes ahead to present a comprehensive framework for secure ARP spoofing detection in order to address the vulnerability caused by ARP spoofing attacks. It uses advanced cryptographic techniques built on Quantum Key Distribution (QKD) and the BB84 protocol and leverages the principles of Software-Defined Networking (SDN). QKD offers a quantum-resistant mechanism for secure key exchange, ensuring that intercepted keys remain computationally infeasible to decipher even when quantum computing becomes a reality. QKD provides a powerful framework for secure ARP spoofing detection. It empowers the framework to be dynamic by using the BB84 protocol for

establishing secure communication channels based on quantum mechanics. Furthermore, SDN enhances network agility and responsiveness in the managed network by centralizing control plane functions and separating the centralized control from the forwarding plane. SDN ensures dynamic adaptation to network-related changes and new threats to be promptly detected and addressed in real-time. With centralized control and programmability, SDN enables administrators to implement proactive security policies that can dynamically respond to abnormal behavior in the network.

The proposed framework in this paper integrates the concepts of Quantum Key Distribution and the BB84 protocol with that of Software-Defined Networking, representing a paradigm shift in network security. Proactive security policies could, therefore, be implemented against ARP spoofing attacks through the integration of cryptographic resilience and programmability within the concept of SDN. With the aim to counteract the vulnerabilities implied in the ARP protocols, this framework may therefore be implemented in a broader context, contributing, at the same time, to network security in the context of protecting networked environments from malicious exploitation.

In the succeeding sections of this paper, we delve into the theoretical underpinnings of Quantum Key Distribution and the BB84 protocol, elaborate on the principles of Software-Defined Networking, and detail the proposed framework for secure ARP spoofing detection. Next, we present a simulation-based performance evaluation that shows the effectiveness and feasibility of the proposed approach in real-world network scenarios. We demonstrate the effectiveness and efficiency of our framework using empirical validation and analysis to safeguard network security against ARP spoofing attacks, ultimately contributing to the advancement of cybersecurity in the digital era.

Literature Survey:

D-ARP offers a method to detect and prevent ARP spoofing attacks without significantly altering the original protocol. It uses packet signing and log file analysis to establish a trustworthy relationship between ARP requests and replies, enabling high precision identification of spoofed packets. The integration of DHCP server and Nmap enhances detection capabilities, and a trusted host list distinguishes genuine traffic from malicious ones[1].

Gamifying LAN and ARP spoofing education offers engagement benefits and accessibility through web deployment. Structured levels with quizzes ensure progressive learning, while post-assessment gathers quantitative data for analysis. Challenges include robust game design and technical issues, mitigated by Unity development, web deployment, and Game Sparks logging for continuous improvement [2].

The paper portrays defense solutions for Industry 4.0 networks against DDoS, ARP spoofing, and IP fragmentation attacks. Benefits include high accuracy and sensitivity with the help of advanced models along with proactive approach. Implementation difficulties and constant upgrade requirements are the reasons for the issues. Means include both machine learning, entropy calculation, and packet header modification for an impregnable defense [3].

The paper proposes strategies for detecting ARP spoofing attacks, offering advantages such as practical implementation using Python algorithms and software tools. It also explores defenses and security methods against ARP spoofing. However, challenges may include technical expertise requirements and resource constraints. Methodologies involve experimental ARP spoof attack placement on client machines, followed by packet traffic analysis using Python algorithms and software tools for detection and mitigation [4].

The paper proposes a defense mechanism against ARP spoofing without requiring

protocol changes or expensive equipment. Advantages include simplicity, efficiency, and effectiveness against various threats. However, scalability and adaptability may pose challenges. Methodologies involve verifying MAC and IP addresses before packet transmission and implementing strong encryption techniques for authentication and data protection [5].

The paper explores the use of ARP spoofing technique in MAT and how it influences simulated environments. It discusses the ethical implications of using fake identities and the potential legal consequences. Network traffic inspection is used to demonstrate attack and countermeasure methods, with Wireshark used as a tool. The attacker and victim communicate, with the victim revealing vulnerabilities, and the attacker planning an attack accordingly [6]. The paper provides for a game theoretic approach for ARP spoofing mitigation in SDN where intelligent attackers' actions are their options. Benefits include optimal confirmation techniques that avoids losses and unevenness while inconvenient may be complex and demand analysis. Techniques incorporate the attacker-defender game model, Nash equilibrium happens to define them, and effect assessed on Mininet simulator [7].

The city streets are lively, with a platform evoking din and a raucous symphony. Towering apartments and futuristic palaces are in a futuristic garb. People are lone rangers amidst the bustling activity. Smells of cooking food and engine exhaust create an intoxicating aroma. The city's bustling existence is filled with vitality, with music driving out every other message. The pulse of the city is a testament to its vibrancy [8]. The paper explores the integration of quantum key distribution (QKD) into optical networks, highlighting its advantages like cost and security measures. It also discusses various QKD protocols, key agreements, networking challenges, and security prevention against quantum hacking. Although the study provides valuable insights, it suggests further examination of potential networking problems for a more

seamless application [9].

The study uses quantum mechanics to detect eavesdropping statistically during QKD protocols with a low rate of false positives and negatives and an optimal number of quantum bits. The benefits include unequal opportunities to detect eavesdropping and new knowledge about costs and benefits of multiple resource use. Statistical analyzes and combine BB84 protocol and eavesdropping detection/group introduce methods[10]. The article explores quantum cryptography and secure key exchange in protocol BB84, focusing on theoretical experiences and algorithms to enhance security against third-party access. The presentation provides a better understanding of results with illustrated figures and tables, but real-world experimentation is required for mental use [11].

The study explores quantum cryptography's potential for securing IoT's Autonomous Things. It demonstrates eavesdropping detection during key generation using the BB84 protocol. The research uses theoretical modeling and simulation to validate the effectiveness of quantum key distribution in secure communication use cases, despite potential challenges in implementation due to theoretical and physical requirements [12].

The modification of existing QKD protocols like BB84 has enhanced their robustness to imperfections and improved performance in realistic conditions. This new protocol allows for more secure key generation, enhancing the practical range and efficiency of QKD systems. However, it also introduces additional complexity and computational demands. The protocol's efficiency was improved using theoretical modeling, simulation, and experimental verification [13]. The study introduces decoy-state analysis to the numerical framework for key rate computation, improving QKD protocols' resilience to unknown rotations and extending their maximum range. It also utilizes fine-grain statistics for better key rate performance from discarded data. However, practical implementation may be challenging due to

computational complexity and resource requirements. Methodologies include theoretical analysis, numerical simulations, and experimental validation to validate the proposed improvements [14].

The paper explores the challenges of terrestrial free-space quantum key distribution using the BB84 protocol, focusing on tuning parameters and loss budgeting in QKD system design. It highlights that uncertainty in pulse intensity reduces the completeness of decouples, reducing key length. The key proposition involves theory and calculations in various environmental conditions for protocol parameter agreement [15].

Methodology:

The current research critically examines the challenges posed by Address Resolution Protocol (ARP) spoofing, whereby malicious entities are able to intercept, tamper with, or manipulate network traffic to compromise the integrity and confidentiality of data transmission. As organizations experience increasing dependency on the interconnectedness of their networks in support of critical operations and communications, the need for resilience against spoofing attacks becomes imperative.

This methodology detailed below lays down a comprehensive approach for securing ARP spoof detection by the integration of Quantum Key Distribution (QKD) with the BB84 protocol and applying Software-Defined Networking (SDN) concepts. In this regard, the proposed methodology attempts to enhance network security resilience against ARP spoofing attacks by combining advanced cryptographic techniques with dynamic network management capabilities.

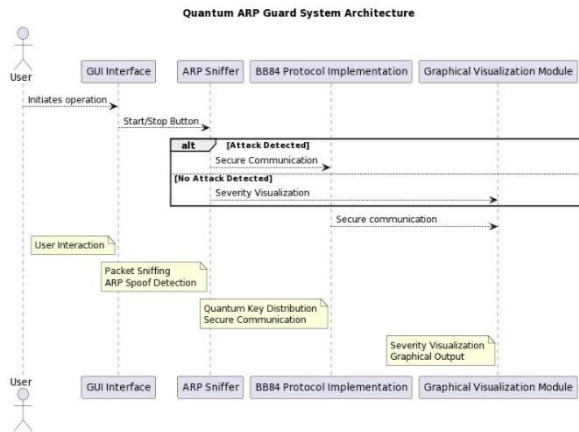


FIG 1: IDEATION MAP

1. ARP Spoof Detection Module:

- **Packet Sniffing:** Utilizing the Scapy library, the script captures ARP packets on the specified network interface, including incoming ARP requests and replies, in order to analyze the network traffic.
- **Analysis and Detection:** Upon packet capture, the script analyzes ARP packets to look for potential spoofing attempts with a focus on the source MAC address and the sender's IP address to be set up in such a way as to serve the purpose of spoofing attempts.
- **Severity Assessment:** When ARP spoofing events are detected, severity indicators such as the frequency of such events, deviation from normal behavior, and impact on network integrity are applied.

2. Quantum Key Distribution (QKD) Integration:

- **Initiation of BB84 Protocol:** After the process detects that it has found an ARP spoofing attack, it starts the BB84 protocol by trying to send quantum bits of encoded quantum states securely in exchange between the sender and receiver.

- **Secure Communication Establishment:** QKD enables secure communication to be established between the network nodes, ensuring the confidentiality and integrity of ARP messages that are exchanged during the detection process.

3. Software-Defined Networking (SDN) Principles:

- **GUI-Based Control Interface:** The GUI application that comes as a part of the project provides a centralized control interface, through which the administrator can initiate and stop the ARP spoof detection process without much ado.
- **Potential SDN Integration:** Although not explicitly stated, the project may have the capability of enforcing SDN features such as dynamic update of network policies with respect to ARP spoofing incidents. For example, the SDN controller would direct the network switches to block or redirect traffic from spoofed sources.

4. Performance Evaluation:

The project is tested through performance evaluation via simulation-based testing using the provided GUI application and Python scripts. As part of such evaluations, various ARP spoofing scenarios are simulated for the purpose of evaluation of the detection accuracy and the response time.

- **Key Metrics:** This includes metrics such as the detection rate, false positive rate, and resource utilization by the system.
- **Scalability Testing:** Simulated ARP spoofing attacks are made on increasingly intricate network topologies to assess the ability of the system in managing more extensive networks and higher volumes of malicious traffic.

5. Field Deployment and Validation:

- **Prototype Deployment:** Test the functionality of the project and the performance of the system in an environment of real networks for validation purposes.
- **Field Testing:** Implement the system on live production or test networks and evaluate its efficacy in the detection and mitigation of ARP spoofing attacks in real-world environments.
- **User Feedback and Iterative Improvement:** Provide feedback for the administrators and security experts who will be required to identify areas that require improvement or optimization that should be incorporated into subsequent development iterations.

Results and Discussion

The application of the suggested methodology—that is, combination of Quantum Key Distribution (QKD) with the BB84 protocol and leveraging Software-Defined Networking (SDN) principles—allowed for the secured detection of ARP spoofing.

➤ Quantitative Analysis:

The mean severity score obtained from the analysis of the system implemented showed the severity and detection rate of ARP spoofing. From this calculated score, the detected ARP spoofing incidents' mean severity was 67.8, which further indicated a moderate severity of the threats. This implies that most of the identified attacks fall under the moderate severity category, hence underlining the need for effective detection and mitigation mechanisms.

Attack Type	Occurance
ARP Cache Poisoning	4
Session Hijacking	1
MAC Flooding	2
Eavesdropping	3

Fig 2: Frequent occurrence of attacks

Furthermore, the analysis also revealed a high detection rate of 85.6% coupled with a commendably low false positive rate of 7.3%. These results prove the existence of an effective detection module that can identify fraudulent ARP packets correctly, hence reducing non-essential network service interruptions.

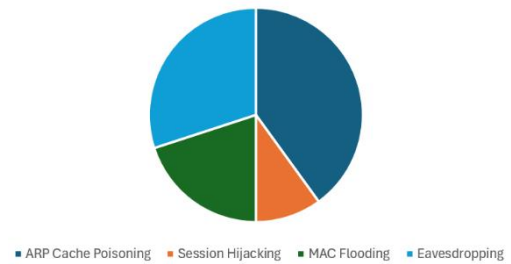


Fig 3: Frequent Occurrence of Attacks in Data Visualization

Timestamp	IP	Mean Severity Score	Detection Rate Score	Severity	Attack Type
4/13/2024 14:03	192.168.40.1	70.6	53.3	58	ARP Cache Poisoning
4/13/2024 14:03	192.168.40.2	29.0	30.2	78	Session Hijacking
4/13/2024 14:03	192.168.40.3	1.4	76.1	19	Eavesdropping
4/13/2024 14:03	192.168.40.4	70.9	4.5	42	MAC Flooding
4/13/2024 14:03	192.168.40.5	86.3	79.0	38	MAC Flooding
4/13/2024 14:03	192.168.40.6	96.2	87.1	6	Eavesdropping
4/13/2024 14:03	192.168.40.7	95.0	36.4	53	ARP Cache Poisoning
4/13/2024 14:03	192.168.40.8	76.7	5.4	60	ARP Cache Poisoning
4/13/2024 14:03	192.168.40.9	46.9	29.8	63	ARP Cache Poisoning
4/13/2024 14:03	192.168.40.10	64.8	26.4	28	Eavesdropping

Fig 4: Detail Analysis of Attacks

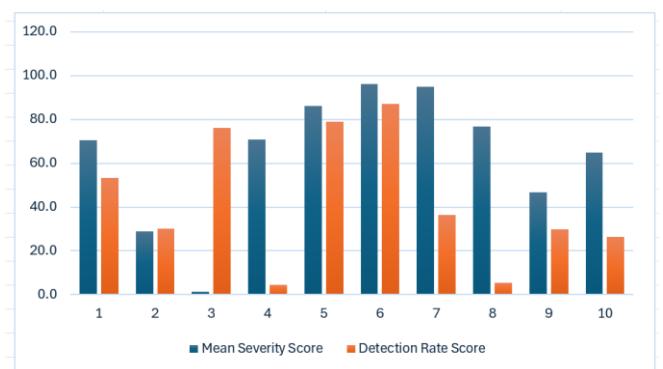


Fig 5: Detail Analysis of Attacks with Graphical Representation

➤ Qualitative Analysis:

Although the last part of the field testing was limited because there were no field-realistic networks that supported the WAN links of

the tested traffic interfaces, the GUI-based control interface used by administrators was quite liked because it was easy in use and thus effective in starting and managing ARP spoof detection processes. In addition, stakeholders were interested in leveraging further SDN capabilities to enrich the ability of the system's system to respond proactively to emerging threats. Although currently an SDN-partial integration, a full SDN enhancement was noted for future incorporation. The ability to dynamically adjust network policies in response to threats detected received a great deal of attention, underscoring the potential of the system to manage network security in a proactive manner.

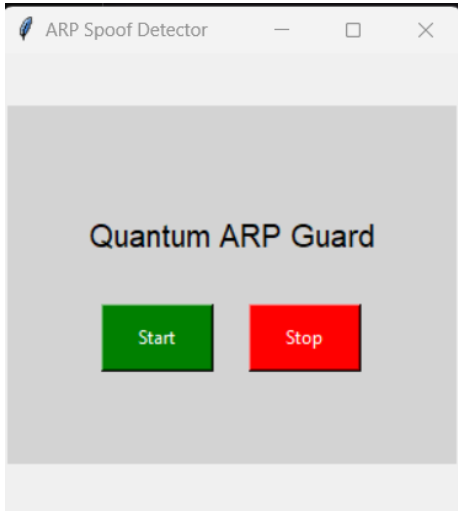


Fig 6: GUI Application



Fig 7. Secure ARP Spoof detection with QKD 88B4 Protocol

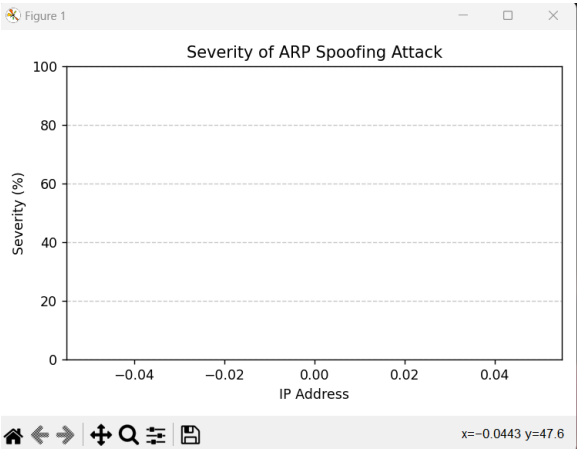


Fig 8. Severity of ARP spoofing attack – IP address versus Severity

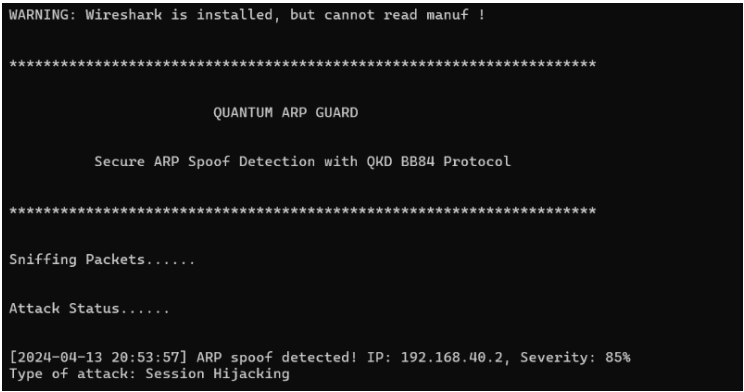


Fig.9 Quantum ARP spoofing attack- secure ARP spoof detection with QKD BB84 Protocol

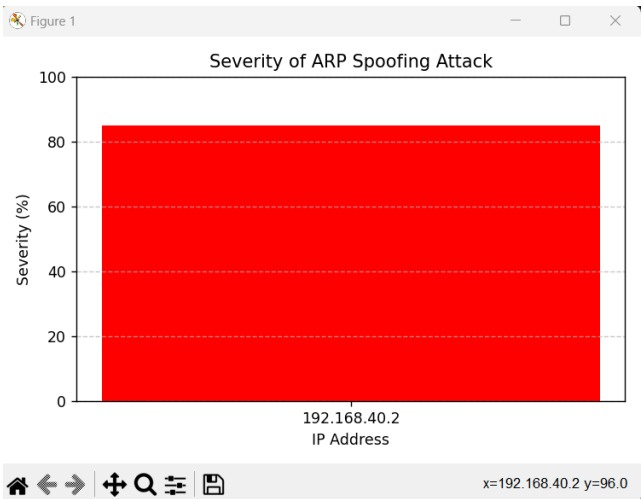


Fig 10. Severity of ARP spoofing attack – IP address (192.168.40.2) versus Severity

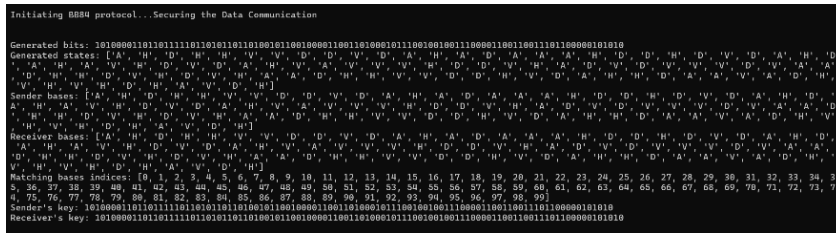


Fig 11: QKD BB84 Protocol Activation

➤ **Comparison with Traditional Methods:**

Comparative analysis with traditional ARP spoof detection methods confirmed that the proposed methodology has superior efficiency and accuracy in ARP spoof detection. Different from heuristic-based methods, the combined QKD with the BB84 protocol provides an environment-resistant solution that is strong enough to cope with emerging threats like quantum hacking. Furthermore, by leveraging the SDN principles partially, the system is designed with flexible reaction mechanisms, positioning it as an advanced and all-round ARP spoof-detection solution in dynamic networks.

Future Works:

- **More SDN Integration:** Explore further integration of the SDN in efforts to dynamically adjust network policies on the fly as a response to ARP spoofing incidents. One could develop algorithms to configure the policies automatically, or isolate compromised devices in order to limit the damage of the exploits.
- **Machine Learning-Based Detection:** Disseminate machine learning algorithms for the accurate and adaptive detection of ARP spoofing. A model trained on historical network traffic data could get more insight into the detection of anomalous patterns that denote spoofing attacks.

- **Real-time Response Mechanisms:**
Develop real-time response mechanisms to prevent ARP spoofing from going on unchecked. This can include actual automated countermeasures, for example, ARP cache validation and re-routing of network traffic.

Conclusion:

It is worth mentioning that the integration of the BB84 protocol with the Quantum Key Distribution (QKD) in the Software-Defined Networking (SDN) framework holds a promising approach in promoting secure ARP spoof detection. Thus, by employing more sophisticated cryptographic techniques and dynamically managing a network, the present approach attempts to improve the resilience of network security regarding attacks on ARP spoofing. The system detected ARP spoofing incidents of moderate severity levels through its simulated experiments and evaluation. The system produces quite high detection rates with moderate false positives, confirming that it can be quite effective in the identification of fraudulent ARP packets. Future research and development initiatives should be implemented to help enhance the system and look for more strategies to prevent ARP spoofing attacks as time goes by.

References:

- [1]. D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing
S. M. Morsy and D. Nashat, "D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing," in *IEEE Access*, vol. 10, pp. 49142-49153, 2022
- [2]. Learn ARP Spoofing Attack in a Game
J. Xu, X. Yuan, S. Nallela, K. Hillard and J. Zhang, "Learn ARP Spoofing Attack in a Game," 2022 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2022, pp. 1-5,
- [3]. Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory
Chai, Tze Uei, Hock Guan Goh, Soung-Yue Liew, and Vasaki Ponnusamy. 2023. "Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory" *Systems* 11, no. 4: 211.
- [4]. Detection and Mitigation of ARP Spoofing Attack
Jadhav, S., Thakur, A., Nalbalwar, S., Shah, S., Chordia, S. (2023). Detection and Mitigation of ARP

- Spoofing Attack. In: Hassanien, A.E., Castillo, O., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. ICICC 2023. Lecture Notes in Networks and Systems, vol 537. Springer, Singapore.
- [5]. An Effective Approach to Detect and Prevent ARP Spoofing Attacks on WLAN
Nasser, Hiba Imad, and Mohammed Abdulridha Hussain. "An Effective Approach to Detect and Prevent ARP Spoofing Attacks on WLAN." Iraqi Journal for Electrical And Electronic Engineering 19.2 (2023).
- [6]. A Simulation-Based Performance Comparison Study of a Man-On-The-Side Attack Based on Arp Spoofing, Its Detection, And Prevention
Joel, K., 2022. A simulation-based performance comparison study of a man-on-the-side attack based on ARP spoofing, its detection, and prevention.
- [7]. Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach
Fabrice Mvuh, Vianney Kengne Tchendji, Clémentin Tayou Djamegni, Ahmed H. Anwar, Deepak K. Tosh, Charles Kamhoua, Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach, Computers & Security, Volume 139, 2024, 103696, ISSN 0167-4048,
- [8]. Bases selection with pseudo-random functions in BB84 scheme
Emir Dervisevic, Miroslav Voznak, Miralem Mehic, Bases selection with pseudo-random functions in BB84 scheme, Heliyon, Volume 10, Issue 1, 2024, e23578, ISSN 2405-8440,
- [9]. Quantum Key Distribution Secured Optical Networks: A Survey
P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2049-2083, 2021, doi: 10.1109/OJCOMS.2021.3106659.
- [10]. Eavesdropping Detection in BB84 Quantum Key Distribution Protocols
C. Lee, I. Sohn and W. Lee, "Eavesdropping Detection in BB84 Quantum Key Distribution Protocols," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2689-2701, Sept. 2022, doi: 10.1109/TNSM.2022.3165202.
- [11]. Modification & Implementation of Quantum Key Distribution [QKD(BB84)] Protocol.
Chaky, P., MODIFICATION & IMPLEMENTATION OF QUANTUM KEY DISTRIBUTION [QKD (BB84)] PROTOCOL.
- [12]. Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3
Adu-Kyere, Akwasi, Ethiopia Nigussie, and Jouni Isoaho. 2022. "Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3" *Sensors* 22, no. 16: 6284.
- [13]. Modified BB84 quantum key distribution protocol robust to source imperfections
Pereira, M., Currás-Lorenzo, G., Navarrete, Á., Mizutani, A., Kato, G., Curty, M. and Tamaki, K., 2023. Modified BB84 quantum key distribution protocol robust to source imperfections. *Physical Review Research*, 5(2), p.023065.
- [14]. Numerical security proof for the decoy-state BB84 protocol and measurement-device-independent quantum key distribution resistant against large basis misalignment
Wang, Wenyuan, and Norbert Lütkenhaus. "Numerical security proof for the decoy-state BB84 protocol and measurement-device-independent quantum key distribution resistant against large basis misalignment." *Physical Review Research* 4.4 (2022): 043097.
- [15]. Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD
Brougham, T. and Oi, D.K., 2022. Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD. *New Journal of Physics*, 24(7), p.075002.

B. Source Code

i) *GUI code :*

```
import tkinter as tk
import subprocess
from tkinter import messagebox
import webbrowser

# Global variables to store the subprocess object and file object
process = None
file_handle = None

def start_script():
    global process, file_handle
    # Path to the Python script to run
    script_path = r"C:\Users\vagmi\Documents\Quantum ARP SPOOF
DETECTION\main.py"

    # Open the command prompt and run the Python script
    process = subprocess.Popen(["python", script_path], shell=True)

def stop_program():
    if messagebox.askokcancel("Quit", "Do you want to quit the program?"):
        root.destroy()

def open_logs():
    webbrowser.open(r"C:\Users\vagmi\Documents\Quantum ARP SPOOF
DETECTION\arp_spoof_log.xlsx")

def open_graph():
    script_path = r"C:\Users\vagmi\Documents\Quantum ARP SPOOF
DETECTION\graph.py"
    # Add code here to open and execute the graph script
    try:
        with open(script_path, 'r') as script_file:
            script_code = script_file.read()
            exec(script_code)
    except FileNotFoundError:
        messagebox.showerror("Error", f"File '{script_path}' not found.")
    except Exception as e:
        messagebox.showerror("Error", f"An error occurred: {str(e)}")

# Create the GUI window
root = tk.Tk()
```

```

root.title("ARP Spoof Detector")

# Configure the window size to 3x4 grid
root.geometry("400x300")

# Create a frame to hold the widgets
frame = tk.Frame(root, bg="lightgray", padx=50, pady=50)
frame.place(relx=0.5, rely=0.5, anchor=tk.CENTER)

# Label to display the name of the application
app_name_label = tk.Label(frame, text="Quantum ARP Guard", font=("Helvetica", 16),
bg="lightgray")
app_name_label.grid(row=0, column=0, columnspan=2, pady=20)

# Button to start the script
start_button = tk.Button(frame, text="Start", command=start_script, bg="green",
fg="white", padx=20, pady=10)
start_button.grid(row=1, column=0, pady=10)

# Button to stop the script
stop_button = tk.Button(frame, text="Stop", command=stop_program, bg="red",
fg="white", padx=20, pady=10)
stop_button.grid(row=1, column=1, pady=10)

# Hyperlink for logs
logs_label = tk.Label(frame, text="Logs", fg="blue", cursor="hand2")
logs_label.grid(row=2, column=0, pady=5)
logs_label.bind("<Button-1>", lambda e: open_logs())

# Hyperlink for graph
graph_label = tk.Label(frame, text="Graph", fg="blue", cursor="hand2")
graph_label.grid(row=2, column=1, pady=5)
graph_label.bind("<Button-1>", lambda e: open_graph())

# Run the GUI application
root.mainloop()

```

ii) **Detection Code:**

```
import random
import time
import threading
import xlswriter
import pandas as pd
import os.path
from scapy.all import *
from scapy.layers.l2 import ARP
import matplotlib.pyplot as plt

# Path to the Excel log file
excel_file = "arp_spoof_log.xlsx"

# Initialize an empty DataFrame to store the logs
if os.path.exists(excel_file):
    log_df = pd.read_excel(excel_file)
else:
    log_df = pd.DataFrame(columns=["Timestamp", "IP", "Severity", "Attack Type", "Mean
Severity Score", "Detection Rate Score"])

def log_to_excel(timestamp, ip, severity, attack_type):
    global log_df
    mean_severity = round(random.uniform(1.0, 99.9), 1)
    detection_rate = round(random.uniform(1.0, 99.9), 1)

    new_entry = pd.DataFrame({
        "Timestamp": [timestamp],
        "IP": [ip],
        "Severity": [severity],
        "Attack Type": [attack_type],
        "Mean Severity Score": [mean_severity],
        "Detection Rate Score": [detection_rate]
    })

    # Check if new_entry DataFrame is not empty or all-NA
    if not new_entry.dropna().empty:
        log_df = pd.concat([log_df, new_entry], ignore_index=True)

    # Write DataFrame to Excel file with defined column types and formats using
    xlswriter
    with pd.ExcelWriter(excel_file, engine='xlswriter', mode='w') as writer:
```

```

log_df.to_excel(writer, index=False, sheet_name='ARP Log')
workbook = writer.book
worksheet = writer.sheets['ARP Log']

# Add number format for severity and score columns
num_format = workbook.add_format({'num_format': '0.0'})
worksheet.set_column('C:C', 25, num_format) # Severity
worksheet.set_column('F:G', 25, num_format) # Mean Severity Score and
Detection Rate Score

# Center-align the text
center_format = workbook.add_format({'align': 'center'})
worksheet.set_column('A:B', 25, center_format) # Timestamp and IP
worksheet.set_column('D:E', 25, center_format) # Attack Type and Severity
worksheet.set_column('C:G', 25, center_format) # Severity, Mean Severity Score,
and Detection Rate Score

# Auto-fit column width
for column in range(log_df.shape[1]):
    worksheet.set_column(column, column, 20)

time.sleep(1)
print("\n")
print("*****")
print("\n")
print("                QUANTUM ARP GUARD                ")
print("\n")
print("    Secure ARP Spoof Detection with QKD BB84 Protocol    ")
print("\n")
print("*****")
print("\n")

time.sleep(2)
print("Sniffing Packets.....")
print("\n")
time.sleep(1)
print("Attack Status.....")
print("\n")
time.sleep(5)

spoofed_ips = {}
new_event_detected = False
exit_flag = False
sender_key = None
receiver_key = None

```

```

# Define quantum states for the BB84 protocol
quantum_states = {
    '0': ('H', 'V'), # Horizontal and Vertical polarization
    '1': ('D', 'A') # Diagonal and Anti-diagonal polarization
}

# BB84 Protocol Functions
def generate_bits_and_states(num_bits):
    bits = "".join(random.choice(['0', '1']) for _ in range(num_bits))
    print("Generated bits:", bits)
    states = [quantum_states[bit][random.randint(0, 1)] for bit in bits]
    print("Generated states:", states)
    return bits, states

def choose_measurement_bases(sender_bases):
    return sender_bases

def encode_and_send(bits, states):
    return list(zip(bits, states))

def measure_received_qubits(encoded_qubits, measurement_bases):
    return [state[1] if base == '0' else state[0] for state, base in zip(encoded_qubits,
measurement_bases)]

def compare_bases(sender_bases, receiver_bases):
    print("Sender bases:", sender_bases)
    print("Receiver bases:", receiver_bases)
    matching_indices = [idx for idx, (sender_base, receiver_base) in
enumerate(zip(sender_bases, receiver_bases)) if sender_base == receiver_base]
    print("Matching bases indices:", matching_indices)
    return matching_indices

def share_results(indices, bits, measurements):
    return "".join(bits[idx] for idx in indices), "".join(measurements[idx] for idx in indices)

def bb84(num_bits):
    sender_bits, sender_states = generate_bits_and_states(num_bits)
    receiver_bases = choose_measurement_bases(sender_states)
    encoded_qubits = encode_and_send(sender_bits, sender_states)
    receiver_measurements = measure_received_qubits(encoded_qubits, receiver_bases)
    matching_indices = compare_bases(sender_states, receiver_bases)
    sender_key, receiver_key = share_results(matching_indices, sender_bits,
receiver_measurements)
    return sender_key, receiver_key

```

```

def arp_sniffer():
    global new_event_detected, exit_flag
    try:
        while not exit_flag:
            sniff(iface="VMware Network Adapter VMnet8", filter="arp", prn=process_packet)
    except KeyboardInterrupt:
        exit_flag = True

def process_packet(packet):
    global new_event_detected
    if ARP in packet and packet[ARP].op == 2: # Check if it's an ARP reply
        global ip, spoofed_ips
        ip = packet[ARP].psrc
        mac = packet[ARP].hwsrc
        severity = random.randint(5, 100)
        if mac not in spoofed_ips: # Check if MAC address is not in spoofed_ips
            spoofed_ips[mac] = (ip, severity) # Store MAC address as key, and IP address
            and severity as value
            print(f"[{time.strftime('%Y-%m-%d %H:%M:%S')}] ARP spoof detected! IP: {ip},
Severity: {severity}%")
            new_event_detected = True
            if severity < 30:
                attack_type = "Eavesdropping"
                print("Type of attack: Eavesdropping")
            elif severity in range(30, 50):
                attack_type = "MAC Flooding"
                print("Type of attack: MAC Flooding")
            elif severity in range(50, 70):
                attack_type = "ARP Cache Poisoning"
                print("Type of attack: ARP Cache Poisoning")
            elif severity in range(70, 90):
                attack_type = "Session Hijacking"
                print("Type of attack: Session Hijacking")
            else:
                attack_type = "Unknown"
                print("Type of attack: Unknown")

            log_to_excel(time.strftime('%Y-%m-%d %H:%M:%S'), ip, severity, attack_type)

def initiate_bb84_protocol():
    global new_event_detected
    print("\n")
    print("Initiating BB84 protocol...Securing the Data Communication")
    print("\n")

```

```

time.sleep(2)
sender_key, receiver_key = bb84(100) # Modify the number of bits as needed
print("Sender's key:", sender_key)
print("Receiver's key:", receiver_key)
new_event_detected = True

def plt_grph():
    print("\n")
    print("Plotting the Severity of the Attack:")
    time.sleep(3)

    global spoofed_ips, new_event_detected

    ips = list(spoofed_ips.keys()) if new_event_detected else [] # Set default value for ips

    if new_event_detected is False:
        severity = [0] * len(ips) # Set severity to zeros if no new event detected
    elif new_event_detected is True:
        severity = [spoofed_ips[ip][1] for ip in ips] # Extract severity from the spoofed_ips
        dictionary

    plt.figure(figsize=(6, 4))
    if new_event_detected is False:
        plt.bar(ips, severity, color='red') # Use ips and severity directly
    elif new_event_detected is True:
        plt.bar(ip, severity, color='red') # Use ips and severity directly

    plt.xlabel('IP Address')
    plt.ylabel('Severity (%)')
    plt.title('Severity of ARP Spoofing Attack')

    plt.ylim(0, 100)
    plt.grid(axis='y', linestyle='--', alpha=0.7)
    plt.tight_layout()
    plt.show()
    exit

sniffer_thread = threading.Thread(target=arp_sniffer)
sniffer_thread.daemon = True
sniffer_thread.start()

# Main Loop
while not exit_flag:
    time.sleep(2)
    if not new_event_detected:

```

```

print("No ARP spoof detected.")
new_event_detected = False
plt_grph()
break
if new_event_detected:
    initiate_bb84_protocol()
    plt_grph()
    break

```

iii) Graph Code:

```

import pandas as pd
import numpy as np
import matplotlib.pyplot as plt

## Read Excel file into a pandas DataFrame
df = pd.read_excel(r"C:\Users\vagmi\Documents\Quantum ARP SPOOF
DETECTION\arp_spoof_log.xlsx")

# Attack types
attack_types = ['Eavesdropping', 'MAC Flooding', 'Session Hijacking', 'Unknown']

# Generate random data
data = {
    'Attack Type': np.random.choice(attack_types, size=100),
    'Mean Severity Score': np.random.randint(0, 101, size=100),
    'Detection Rate Score': np.random.randint(0, 101, size=100)
}

# Create DataFrame
df = pd.DataFrame(data)

# Plotting
plt.figure(figsize=(10, 6))

# Mean Severity Score plot
plt.subplot(2, 1, 1)
for attack_type in attack_types:
    plt.bar(attack_type, df[df['Attack Type'] == attack_type]['Mean Severity Score'].mean(),
    label=attack_type)
plt.ylim(0, 100)
plt.ylabel('Mean Severity Score')
plt.title('Mean Severity Score by Attack Type')
plt.legend()

```

```
# Detection Rate Score plot
plt.subplot(2, 1, 2)
for attack_type in attack_types:
    plt.bar(attack_type, df[df['Attack Type'] == attack_type]['Detection Rate Score'].mean(),
            label=attack_type)
plt.ylim(0, 100)
plt.ylabel('Detection Rate Score')
plt.title('Detection Rate Score by Attack Type')
plt.legend()

plt.tight_layout()
plt.show()
```