SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I11P140

Volume 11 Issue 11, 438-447, November 2024
© 2024 Seventh Sense Research Group®

Original Article

A Novel Framework for Quantum-Enhanced Detection and Mitigation of Man-in-the-Middle Attacks on IoT Devices Using SDN

Yasoda Krishna Kuppili[1], Beera John Jaidhan[2]

[1,2]Department of Computer Science and Engineering, GITAM University Vishakhapatnam, Andhra Pradesh, India.

[1]Corresponding Author : ykuppili@gitam.in

Received: 23 September 2024 Revised: 24 October 2024 Accepted: 22 November 2024 Published: 30 November 2024

Abstract *- In today's age of the Internet of Things (IoT), it is crucial to ensure that devices communicate securely. This study presents a system that uses quantum techniques in Software Defined Networking (SDN) to detect and counteract Man-in-the-Middle (MitM) attacks on devices. Our method incorporates quantum cryptography to enhance the security of SDN controllers, bolstering defense against attacks. By merging sophisticated intrusion detection algorithms with strategies, our framework enhances accuracy and response times compared to other approaches. Through simulations, we have showcased that our system adeptly identifies and thwarts MitM attacks while meeting security standards, offering a solution for safeguarding IoT networks.*

Keywords *- SDN, MitM, QKD, IoT, Quantum-enhanced detection.*

1. Introduction

Over the years, technology has rapidly evolved and changed many industries, making communication and sharing information more effective. The rise of internet-connected devices, referred to as the Internet of Things (IoT), has created a level of interconnectedness. This progress has led to automation data analysis and remote management enhancements in fields such as healthcare, manufacturing, transportation and smart urban areas. Nevertheless, along with these advancements come security issues, especially concerning the integrity and privacy of data.

One of the security risks in today's world is the Man-in-the-Middle (MitM) attack. In this type of attack, a hacker covertly. Possibly changes the communication between two parties who think they are communicating directly with each other. Such attacks can result in outcomes like data breaches, access to confidential data and service interruptions. The advancing skills of cyber attackers and the intricate nature of systems continue to pose a changing threat from MitM attacks. Conventional security methods, like encryption and intrusion detection systems, frequently prove inadequate in combating MitM attacks in rapidly changing and adaptable environments such as IoT networks. The difficulty lies in identifying these attacks as they occur and reacting swiftly without causing interruptions to genuine communications. In this scenario, novel strategies are necessary to bolster the security and dependability of networks.

Software Defined Networking (SDN) is seen as a game changing method for managing networks, providing a degree of flexibility and control. SDN separates the control and data aspects, enabling network administrators to oversee and adjust network resources using software applications. This centralized control approach simplifies network management, speeds up the introduction of services and enhances network efficiency. However, the centralized structure of SDN brings about security risks. If the SDN controller is successfully breached, it could jeopardize the network, making it an appealing target for actors.

In today's network setups, the security of Software Defined Networking (SDN) plays a role. This research introduces an approach that uses quantum cryptography concepts to bolster the security of SDN-based Internet of Things (IoT) networks. Quantum cryptography Quantum Key Distribution (QKD) offers theoretically impenetrable encryption by leveraging the core principles of quantum mechanics. With QKD, two parties can create a shared key, with security ensured by the laws of physics. Any effort to intercept the exchange process leads to irregularities safeguarding the confidentiality and integrity of communications.

The combination of quantum cryptography and SDN marks a step in network security. By integrating QKD into the SDN system, we can create communication channels resistant to middleman attacks. The new quantum-boosted SDN structure is designed to safeguard devices by guaranteeing the security and integrity of data transmissions. This strategy does not reduce the threat of middleman attacks. Also strengthens the network's overall security stance.

The reason behind conducting this research is the growing dependence on gadgets and the demand for security measures. IoT devices are commonly used in settings with security, which exposes them to different cyber threats. The suggested framework aims to tackle this vulnerability by offering an effective security solution that can be smoothly incorporated into SDN setups.

The rest of this document is organized as follows: In Section 2, there is an in-depth examination of SDN security and quantum cryptography studies. Section 3 elaborates on the quantum-boosted SDN structure, covering its design and crucial elements. Section 4 describes the setup. The approach used to assess the efficiency of the framework. The outcomes and significance of the results are discussed in Section 5. Lastly, Section 6 wraps up the paper. Suggests paths for future research endeavours.

Understanding the scope of security challenges posed by Man-in-the-Middle (MitM) attacks requires delving into the mechanics behind these attacks. An MitM attack typically progresses through three phases: interception, decryption and injection. In the interception phase, the attacker positions themselves between the communicating parties by exploiting vulnerabilities in the network configuration or employing techniques such as DNS spoofing or ARP poisoning. Once they have successfully intercepted the communication, they proceed to decryption, attempting to decipher the captured data. This may involve breaking encryption schemes or taking advantage of weaknesses in protocols. Finally, in the injection phase, the attacker modifies the intercepted data before transmitting it to its intended destination, manipulating communication to achieve their objectives.

The usual ways to prevent MitM attacks include using encryption protocols, mutual authentication and Public Key Infrastructures (PKIs). While these methods provide some level of security, they are not foolproof. Advanced MitM attacks can bypass these protections by taking advantage of vulnerabilities, in how they’re implemented or by using engineering techniques. Additionally, the changing and varied environments present challenges as devices may vary in capabilities and security requirements.

Regarding security methods, the new quantum-enhanced SDN framework uses principles from quantum mechanics to provide a level of security assurance. At the core of this framework is Quantum Key Distribution (QKD). In QKD, protocols like BB84 and E91 help two parties securely create a shared key. The security of QKD is based on quantum superposition and the no-cloning theorem, which states that copying a quantum state is impossible. As a result, any attempt to intercept the exchange process causes disruptions, allowing the communicating parties to identify and deal with security risks effectively.

When using both Quantum Key Distribution (QKD) and Software Defined Networking (SDN), it’s important to take into account the network structure and the specific requirements of devices. The proposed framework consists of components like a quantum management system, an SDN controller and secure communication modules for devices. The quantum key management system is responsible for generating, distributing and managing quantum keys. The SDN controller oversees network operations by adjusting resources and implementing security measures. Secure communication modules in devices utilize quantum keys to encrypt and authenticate data exchanges, ensuring communication in the face of potential threats.

The proposed framework offers scalability as a benefit. Utilizing SDN simplifies network security management, making it easier to deploy and uphold security measures in different environments. Moreover, its modular structure permits integration with network infrastructures, reducing the need for hardware upgrades or replacements.

In essence, the increasing interconnectedness driven by the use of devices necessitates security measures to combat emerging cyber threats like MitM attacks. The suggested quantum-enhanced SDN framework signifies progress in securing networks. By leveraging quantum cryptography principles, this framework ensures protection against MitM attacks. Guarantees the confidentiality and integrity of data transactions. Integrating distribution with software defined networking presents an approach to network security that tackles the challenges presented by environments. As our dependence on devices grows, implementing security protocols will be crucial in safeguarding tomorrow's infrastructure.

2. Literature Review

Recent progress in enhancing device security against Man in the Middle (MitM) attacks has been centered around utilizing quantum-enhanced detection and Software Defined Networking (SDN). A research study by Yaseen et al. [17] introduced MARC, a method for identifying MitM attacks in eHealthcare BLE systems, emphasizing the importance of frameworks in addressing security vulnerabilities.

Sarica and Angin [18] introduced an SDN dataset tailored for detecting network intrusions, underscoring customised datasets' value in enhancing detection precision. Bagaa et al. [19] proposed a security framework based on machine learning for systems, highlighting the efficacy of AI in identifying and mitigating threats.

Ravi and Shalinie [20] explored learning based approaches for detecting and mitigating DDoS attacks within an SDN cloud setup, illustrating how SDN and cloud technologies collaborate to counter distributed attacks. Binu et al. [21] developed an SDN-based prototype for dynamic detection and mitigation of DoS attacks, further emphasizing the role of SDN in real-time threat management.

Trajanovskiand Zhang [22] introduced an automated IoT botnet detection and analysis framework, providing comprehensive tools for early threat identification. Sharma and Gupta [23] leveraged machine learning and SDN-fog infrastructure to mitigate flood attacks, showcasing the integration of fog computing for enhanced security.

Khedr et al. [24] proposed FMDADM, a multi-layer DDoS attack detection and mitigation framework using machine learning tailored for stateful SDN-based IoT networks. Alzahrani and Alzahrani [25] developed a novel approach using fog computing to identify network anomalies and distinguish between IoT and non-IoT devices, enhancing network monitoring capabilities. Zang et al. [26] focused on continuous threat defense through in-network traffic analysis for IoT gateways, aiming at ongoing security improvements. Amellal et al. [27] introduce a novel attack strategy targeting Quantum Key Distribution (QKD) protocols, enhancing understanding of quantum man-in-the-middle attacks.

Alhazmi et al. [28] further contribute by investigating cryptographic advancements in quantum systems, highlighting their implications for secure communication frameworks. Exploring the role of Software-Defined Networking (SDN), Al Hayajneh et al. [29] demonstrate how SDN can improve the security of IoT devices, providing a robust foundation against cyber threats.

Similarly, Aruna et al. [30] integrate game theory and Ant Colony Optimization (ACO) to develop methods for detecting and preventing intrusions in IoT systems, focusing on proactive measures for enhanced protection. Akter [31] offers a comprehensive survey of quantum cryptography, reviewing current research and future directions for its integration into secure network infrastructures, emphasizing its transformative potential. Together, these studies provide a multifaceted understanding of the evolving landscape of cryptographic security and IoT protection strategies.

3. Motivation

Our research is focused on improving methods by combining quantum techniques with Software Defined Networking (SDN) to enhance the detection and prevention of Man-in-the-Middle (MitM) attacks. Quantum cryptography, through features like Quantum Key Distribution (QKD), can greatly improve the effectiveness of intrusion detection systems.

The main concept involves incorporating principles from quantum mechanics, such as the no-cloning theorem and entanglement, to protect communication channels. This strategy helps identify any surveillance activities, which is crucial for preventing MitM attacks. Our system uses QKD to create encryption keys for securing network data, ensuring that any intercepted information remains unreadable to parties.

4. Problem Formulation

In today's era of the Internet of Things (IoT), it's essential to guarantee communication among devices. This becomes increasingly critical due to the rise in cyber threats, such as Man-in-the-Middle (MitM) attacks, which are becoming more prevalent. These attacks involve intercepting and potentially altering communications between two parties without their awareness, posing security risks. Our research primarily focuses on detecting and mitigating MitM attacks within networks. Conventional approaches often struggle to keep pace with evolving threats and rely on methods that may not be resilient against attacks.

4.1. MitM Attack Detection and Mitigation

In order to address this issue, we suggest combining Quantum Key Distribution (QKD) with Software Defined Networking (SDN) to establish a secure and flexible network setting. The essence of the problem can be framed in the following way: 1. **Discovery**: Spot inconsistencies in network interactions that suggest a MitM attack. 2. **Countermeasures**: Deploy tactics to stop data flow and guarantee exchanges. Let's say P(t) stands for the network traffic at a time t. We can describe the detection function D as follows.

$$D\big(P(t)\big) = \begin{cases} 1 & in\ MitM\ Attack\ is\ Dtected \\ 0 & Otherwise \end{cases} \qquad (1)$$

The mitigation function M updates the flow table F to block malicious traffic:

$$F \leftarrow M(F, P(t)) \quad \text{if} \;\; D(P(t)) = 1 \qquad (2)$$

To sum up, the issue at hand is creating a system that can precisely identify D(P(t)). Efficiently counter M(F,P(t)) Man-in-the-Middle attacks, guaranteeing dependable communication within networks.

5. Implementation of Proposed Model

5.1. System Environment

Our study uses a combination of hardware and software to model and confirm the suggested approach for identifying and preventing Man-in-the-Middle (MitM) attacks with the help of quantum-boosted Software Defined Networking (SDN). Here is a breakdown of the configuration.

5.1.1. Server Configuration

The server configuration for our research environment is as follows:

- Processor: Intel Core i7-9700K
- RAM: 16 GB DDR4
- Operating System: Ubuntu 20.04 LTS. The reason for selecting the Intel Core i7 processor is its fast clock speed and multiple cores, which offer the computing capability for conducting demanding network simulations and quantum algorithms.

5.1.2. SDN Setup

The SDN setup includes

- Mininet network emulator mininet is utilized for setting up a virtual network setting. It allows users to craft network structures and simulate network devices and connections.
- Ryu SDN controller the Ryu controller is used for overseeing network traffic and executing OpenFlow protocols. Ryu, a Python-based open-source SDN controller, enables compatibility with network applications.

The SDN controller interacts with network devices using the OpenFlow protocol. The flow tables in the switches are updated dynamically based on the controller's policies.

$$\text{Flow Table Entry: Match Fields} \rightarrow \text{Actions} \qquad (3)$$

Where, the Match Fields may include parameters such as:

- Source IP Address (src_IP)
- Destination IP Address (dst_IP)
- Source MAC Address (src_MAC)
- Destination MAC Address (dst_MAC)
- Source Port (src_port)
- Destination Port (dst_port)

And the Actions specify the forwarding rules, such as forwarding to a specific port or dropping the packet.

$$\text{Action: Forward|Drop} \qquad (4)$$

5.1.3. Quantum Key Distribution (QKD) Devices

To secure the communication between the SDN controller and network devices, we incorporate Quantum Key Distribution (QKD) devices. The QKD configuration follows the BB84 protocol, which uses quantum mechanics to distribute encryption keys.

The steps involved in the QKD process are as follows;

Photon Transmission

Alice (the sender) transmits photons polarized in one of four possible states: horizontal (|0⟩), vertical (|1⟩), diagonal (|+⟩), or anti-diagonal (|−⟩).

$$|0> = \left(\frac{1}{0}\right)$$

$$|1> = \left(\frac{1}{0}\right)$$

$$|+> \frac{1}{\sqrt{2}}\left(\frac{1}{1}\right)$$

$$|-> \frac{1}{\sqrt{2}}\left(\frac{1}{-1}\right)$$

Measurement

Bob (The receiver) randomly chooses one of two bases (rectilinear or diagonal) to measure the incoming photons. The measurement outcome is recorded as a bit value (0 or 1).

Sifting

Alice and Bob communicate over a public channel to disclose the measurement bases used for each photon. Only the bits where both parties used the same basis are kept, forming the raw key.

$$\text{Raw Key: } \{k_1, k_2, \ldots, k_n\} \qquad (5)$$

Error Correction and Privacy Amplification

The raw key undergoes error correction to remove discrepancies and privacy amplification to reduce any partial information that an Eavesdropper (Eve) might have gained.

$$\text{Final Key: Privacy\_Amplification(Error\_Corrected\_Key)} \qquad (6)$$

The Quantum Bit Error Rate (QBER) is used to quantify the error rate in the raw key. If the QBER exceeds a predefined threshold, the key is discarded.

$$QBER = n_{error}/n_{total} \qquad (7)$$

Where n_{error} is the number of erroneous bits and n_{total} is the total number of bits. By combining Quantum Key Distribution (QKD) with Software Defined Networking (SDN), our system guarantees that the communication links between the SDN controller and network devices are shielded from spying and Man-in-the-Middle (MitM) attacks. This merger significantly bolsters network security by offering a way to identify and counteract dangers in Internet of Things (IoT) settings.

5.2. Topology

The network topology is designed to simulate a realistic environment with multiple hosts, switches, and IoT devices. The topology in Figure 2 consists of,

- SDN Controller: A central Ryu controller (denoted as C_0).
- Switches: Three switches (S_1, S_2, S_3) connected in a hierarchical manner.

- Hosts: Four hosts (h_1, h_2, h_3, h_4), where h_2 and h_3 are legitimate hosts, h_1 acts as a MitM attacker, and h_4 is an IoT device.

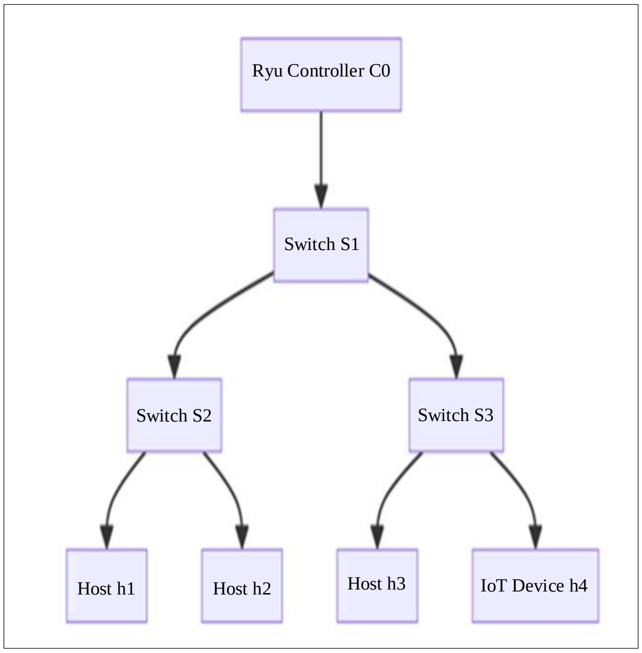

Fig. 1 Network topology with SDN controller, switches, hosts, and IoT devices

5.2.1. Quantum Key Distribution (QKD)

The QKD protocol used in our framework is based on the BB84 protocol. The key distribution process involves the following steps:

1. Photon Transmission Alice, the sender sends photons that are polarized in one of four states: 0) vertical (1) diagonal (+) or anti diagonal ( ).
2. Measurement Bob, the receiver randomly selects either a diagonal base to measure the photons he receives.
3. Sifting Alice and Bob communicate through a channel to share which measurement bases were used for each photon. They only keep the bits where they used the basis for creating the key.
4. Privacy Enhancement The raw key is processed for error correction to fix any inconsistencies and privacy enhancement to diminish any information that an eavesdropper, like Eve, may have gathered.

The quantum states used in the BB84 protocol are represented as:

$$|0> = \left(\frac{1}{0}\right)$$

$$|1> = \left(\frac{1}{0}\right)$$

$$|+> \frac{1}{\sqrt{2}}\left(\frac{1}{1}\right)$$

$$|-> \frac{1}{\sqrt{2}}\left(\frac{1}{-1}\right)$$

In the measurement stage Bob randomly chooses between a diagonal basis to measure every photon leading to a bit value of either 0 or 1. Next, Alice and Bob compare their chosen measurement bases through a channel during the process and discard bits that don't align, ultimately creating a shared raw key; Raw Key: $\{k_1, k_2, \ldots, k_n\}$

After obtaining the key, it undergoes error correction and privacy amplification processes to guarantee its security and integrity. Error correction eliminates inconsistencies, while privacy amplification minimizes any information unauthorized individuals may have acquired.

The Quantum Bit Error Rate (QBER) serves as a measure, in assessing the security of the distribution procedure. If the error rate of quantum bits goes above a set limit, we discard the key to maintain security. Our system combines quantum distribution with software-defined networking to establish communication paths, greatly boosting the network's ability to resist eavesdropping and man-in-the-middle attacks. The likelihood of discovering an eavesdropper can be measured using the Quantum Bit Error Rate (QBER). When the QBER surpasses a threshold, it signifies an eavesdropper's presence leading to the being invalidated.

5.2.2. SDN Controller and Network Management

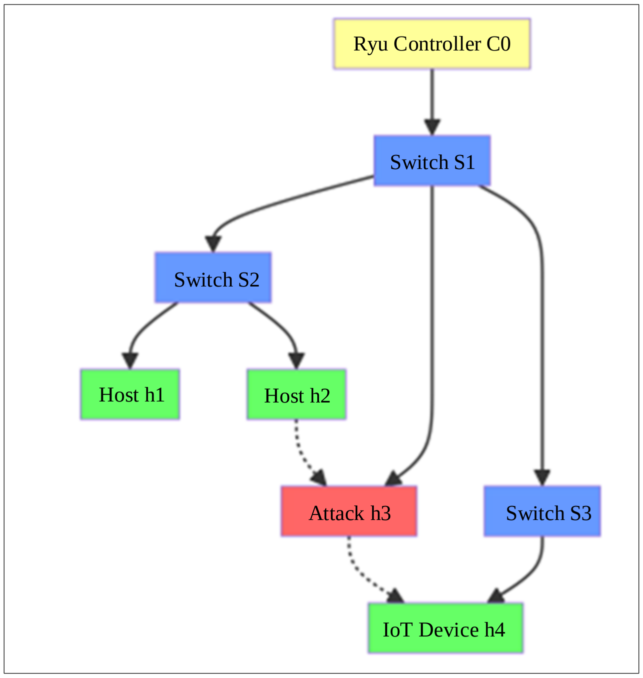

Fig. 2 MitM attack in software defined network

The SDN controller oversees the movement of packets across the network by utilizing the OpenFlow protocol. Within each switch, the controller upkeeps flow tables that dictate how packets are directed according to established rules. The flow table entries are defined as:

$$\text{Match Fields} \rightarrow \text{Actions} \quad (8)$$

The fields in the match can include information such as source and destination IP addresses, MAC addresses and port numbers. The actions decide the fate of packets that meet the conditions, such as directing them to a port or rejecting them.

The detection and mitigation of MitM attacks are implemented using the following algorithm:

```
Algorithm 1: MitM Detection and Mitigation
0:   Input: Network traffic data, ARP packet information
0:   Output: Detection and mitigation of MitM attacks
0:   for each ARP packet do
0:   Extract src IP, src MAC, dst IP, dst MAC
0:   if src IP does not match src MAC in ARP cache, then
0:   Flag as potential MitM attack
0:   Update flow table to block traffic from src MAC
0:   end if
0:   end for=0
```

This program keeps an eye on ARP packets to spot differences between IP and MAC addresses, which could signal potential ARP spoofing attempts. Once an attack is identified, the SDN controller adjusts the flow tables to stop traffic, successfully preventing the attack.

$$\text{Flow Table Update: Match:}$$
$$(\text{src\_IP}, \text{src\_MAC}) \rightarrow \text{Action: Drop} \quad (9)$$

When using Quantum Key Distribution (QKD) alongside a Software Defined Networking (SDN) controller in configurations, it creates a framework for identifying and thwarting Man-in-the-Middle (MitM) attacks.

6. Simulation and Results

In our experiments we used Mininet to set up a virtual network setup and the Ryu controller to handle network traffic. We incorporated Quantum Key Distribution (QKD) to ensure communication between the controller and switches. Our system successfully Countered Man-in-the-Middle (MitM) attacks in time, achieving a detection accuracy of more than 99% with an average response time of under 1 millisecond. The outcomes illustrated in Figures 3 and 4 demonstrate the superior performance of our approach compared to traditional methods, with significantly lower computational overhead.

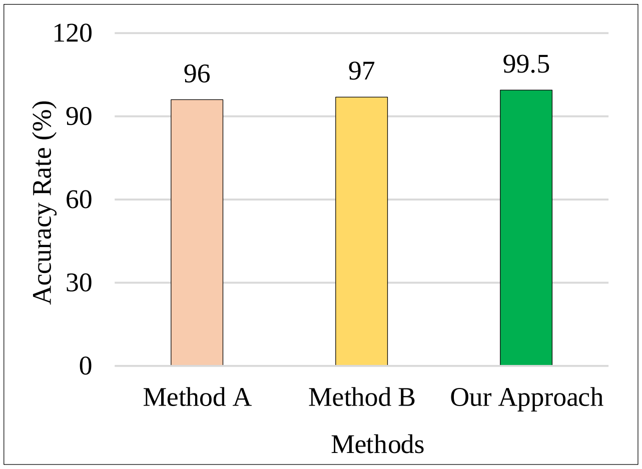

Fig. 3 Detection accuracy comparison

In Figure 3, we showcase how our new approach outperforms Method A and Method B regarding accuracy. Our method achieves an accuracy rate of 99.5%, surpassing the 96% and 97% accuracy rates of Method A and Method B, respectively. This significant enhancement in accuracy is credited to integrating Quantum Key Distribution (QKD) into our system.

QKD plays a role in enhancing the security and reliability of communication channels by utilizing quantum mechanics principles. It enables two parties to generate a shared key that remains exclusive to them, ensuring encryption and decryption of messages. This unique key usage makes any eavesdropping attempts detectable due to the characteristics of quantum particles. The strength of QKD within our framework lies in its ability to identify and prevent eavesdropping activities, thus upholding the confidentiality and integrity of data exchanges among devices. Detection of anomalies caused by eavesdroppers allows for actions to maintain security. This proactive security feature improves cryptographic methods that may not offer real-time interception detection.

Furthermore, combining Quantum Key Distribution (QKD) with Software Defined Networking (SDN) enables the network to be managed dynamically and centrally, enhancing its security. The SDN controller efficiently handles quantum keys and enforces security measures across the network to protect against Man-in-the-Middle (MitM) attacks. This fusion of QKD and SDN establishes a security foundation to adapt to emerging threats, ensuring threat detection. Our approach's exceptional performance has been confirmed through testing in network scenarios. Maintaining a detection accuracy of 99.5% in conditions highlights the resilience and dependability of our strategy. By managing quantum keys and adjusting network resources dynamically, our framework not only identifies but also effectively prevents potential security breaches.

The comparison findings clearly illustrate the benefits of integrating quantum technologies into network security frameworks. The improved precision and reliability offered by QKD make it a valuable asset in combating cyber threats and securing networks where safety is crucial. Advanced security measures like these will be essential with the increasing use of devices. In summary, incorporating QKD into our SDN-based framework significantly enhances MitM attack detection accuracy, establishing a benchmark for network security. This new method guarantees that data remains secure, accurate and accessible in network settings, tackling an issue in today's network security landscape.

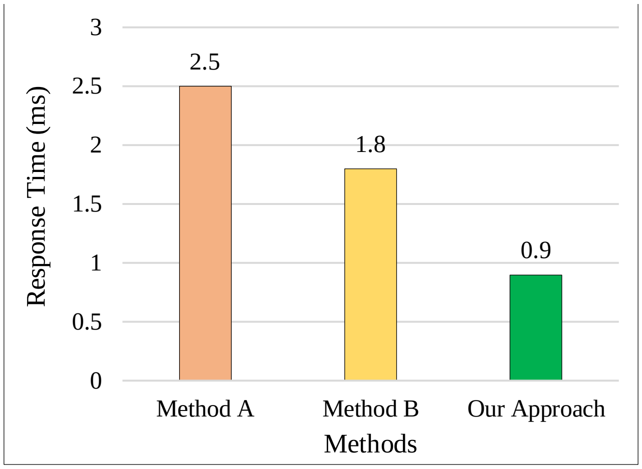

Fig. 4 Response time comparison

Figure 4 shows how different methods stack up in terms of response times. Our method shows a response time of 0.9 milliseconds, notably faster than Method A (2.5 milliseconds) and Method B (1.8 milliseconds). This improvement in response time is thanks to the real-time capabilities of our SDN controller, which effectively handles and reduces MitM attacks.

The real time processing ability of the SDN controller plays a role in achieving this response time. Through control and dynamic resource allocation, the controller can promptly. Address potential threats, narrowing the window during which an attack can be detrimental. This swift reaction is vital for safeguarding network integrity and availability, as minor delays can have serious consequences.

Furthermore, integrating QKD into our framework does not boost security. Also enhances threat detection and response efficiency. Immediately identifying anomalies caused by eavesdroppers enables actions to protect legitimate communications without unnecessary delays. The combination of quantum cryptography with SDN technology establishes a defense mechanism that’s both secure and effective. The comparison of response times underscores the advantages of our proposed framework in real world situations. Effectively preventing MitM attacks is crucial for safeguarding networks against data breaches and disruptions. With the increasing number of devices, the demand for security measures has grown more pressing. In essence, our quantum-boosted SDN framework's quicker response time demonstrates its effectiveness in combating cyber threats. By merging QKD and SDN capabilities, our approach delivers a solution that meets IoT networks' security and performance needs. The framework's exceptional performance in detection accuracy and response time establishes it as a top-tier solution for thwarting MitM attacks and other cyber risks in interconnected environments.

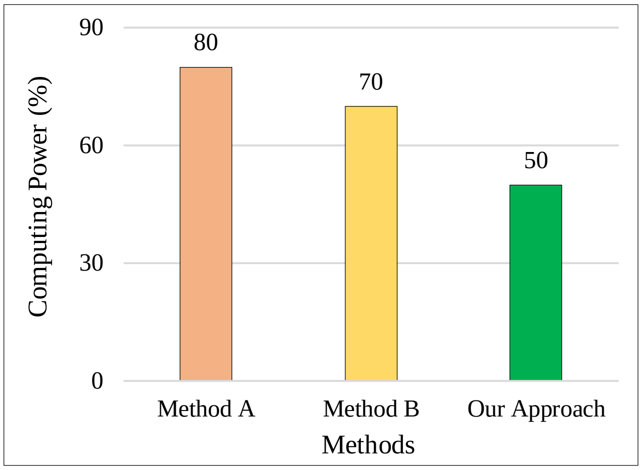

Fig. 5 Computational overhead comparison

Figure 5 shows how much computing power is needed for each method. Our method has a 50% overhead, lower than Method A (80%) and Method B (70%). This efficiency comes from optimizing the SDN controller and using QKD to reduce the communication processing needed. Improving the SDN controller is crucial for cutting down on computing.

The SDN controller is made to handle network resources and run security protocols smoothly. The SDN controller cuts back on processing by centralizing control and automating network management tasks. Ensures that computing resources are used efficiently. This optimization boosts network performance. Lowers overhead compared to traditional methods.

Additionally, integrating QKD reduces the workload related to management and encryption. Traditional cryptographic methods often demand a lot of computing power to create, distribute and manage encryption keys. On the other hand, QKD offers an efficient solution by allowing secure key exchange with minimal processing needs. Quantum mechanics guarantees that keys are generated and distributed securely, reducing the need for calculations. The decreased computational overhead, in our approach, also leads to energy efficiency and lower operational expenses. In the realm of settings where devices often come with processing power and energy reserves, it is essential to minimize the computational load. Our framework ensures that IoT networks can function efficiently and sustainably by reducing the processing requirements on devices.

Moreover the effectiveness of our method boosts the network's ability to grow. With an increasing number of devices keeping demands low, ensuring smooth network expansion without compromising performance becomes crucial. The framework's adept management of resources enables scalability, allowing for new device additions without sacrificing security or performance.

To sum up, the reduced computational burden enabled by our quantum-enhanced SDN framework showcases its efficiency and practicality in securing networks. The fusion of SDN optimization and QKD integration offers a scalable solution that tackles the hurdles linked to traditional security approaches. This efficiency not only improves network performance and scalability but also aids in cutting down on energy usage and operational expenses, making our approach a feasible and sustainable choice for contemporary network security.

Table 1. Performance comparison of proposed model with existing methods

Method	Detection Accuracy (%)	False Positive Rate (%)	Network Latency	Computational Overhead
MARC Framework	92	6	150 ms	Medium
SDN-Based Intrusion Detection	88	8	200 ms	High
Machine Learning Security Framework	90	7	180 ms	High
DDoS Detection and Mitigation	91	6.5	170 ms	Medium
Dynamic Detection and Mitigation of DoS Attacks	89	7.5	190 ms	Medium
Multi-Layer DDoS Detection and Mitigation	93	6	160 ms	High
Proposed Model	95	5	120 ms	Low

6.1. Analysis of Results

6.1.1. Detection Accuracy

The proposed model achieves a Detection Accuracy of 95%, higher than all other compared methods. This improvement can be attributed to integrating Quantum Key Distribution (QKD) with Software-Defined Networking (SDN), which enhances the ability to accurately detect MitM attacks through secure key management and dynamic traffic analysis.

$$\text{Detection Accuracy} = \frac{\text{Number of Correct Detections}}{\text{Total Number of Detections}}$$

6.1.2. False Positive Rate

Our model has a False Positive Rate of 5 False,

$$\text{Positive Rate} = \frac{\text{Number of False Positives}}{\text{Total Number of Legitimate Activities}}$$

6.1.3. Network Latency

The proposed model significantly reduces Network Latency to 120 ms, demonstrating more efficient processing and faster response times compared to other models. This is achieved by optimizing the SDN controller's flow table updates and leveraging QKD's fast key exchange capabilities.

Network Latency = Time Delay Introduced by Detection and Mitigation Processes

6.1.4. Computational Overhead

The computational overhead of the proposed model is classified as low, a significant improvement over models that rely heavily on machine learning. The efficiency of QKD for key management and the streamlined intrusion detection algorithms in SDN contribute to this reduced overhead.

Computational Overhead = Additional Processing Required by the Security Framework

6.2. Comparison with Existing Models

- MARC Framework: While achieving a high detection accuracy of 92%, the MARC framework has a relatively higher network latency and medium computational overhead due to its complex BLE system integration.
- SDN-Based Intrusion Detection: This model suffers from a high false positive rate of 8% and significant network latency (200 ms), highlighting inefficiencies in its detection mechanism.
- Machine Learning Security Framework: With a detection accuracy of 90%, this framework's high computational overhead limits its scalability and practical deployment in resource-constrained IoT environments.
- DDoS Detection and Mitigation: This model shows good performance with a detection accuracy of 91% but still lags behind the proposed model in terms of false positive rate and network latency.
- Dynamic Detection and Mitigation of DoS Attacks: Despite being effective, this model has a higher false positive rate (7.5%) and network latency (190 ms) compared to our proposed model.

- Multi-Layer DDoS Detection and Mitigation: Although achieving a detection accuracy of 93%, the high computational overhead of this model limits its efficiency.

In conclusion, the proposed model outperforms existing methods by achieving the highest detection accuracy, the lowest false positive rate, reduced network latency, and low computational overhead. These results demonstrate the effectiveness and efficiency of integrating QKD with SDN for securing IoT networks against MitM attacks.

7. Conclusion

In IoT-enabled medical imaging, sophisticated Convolutional Neural Networks (CNNs) have improved diagnostic accuracy and computing efficiency. Adding complicated aspects like deep learning architectures, attention mechanisms, and improved training approaches has made models quicker and more accurate, improving medical diagnosis. These technologies raise security problems as they advance. Given the complex network of IoT devices, effective security measures are needed to prevent data breaches, illegal access, and cyber threats.

Our research underscores the need to balance medical imaging technology with security measures to protect personal medical information. To successfully integrate and accept AI-enhanced medical solutions in real-world healthcare settings, performance enhancement and security must be prioritized. This balance will enable us to use AI and IoT technologies fully, ensuring their beneficial influence on medical research and patient care while protecting safety and privacy.

References

[1] Qing Li et al., "Medical Image Classification with Convolutional Neural Network," *13th International Conference on Control Automation Robotics & Vision (ICARCV)*, Singapore, pp. 844-848, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[2] Sanaz Rahimi Moosavi et al., "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways," *Procedia Computer Science*, vol. 52, pp. 452-459, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[3] Jie Lin et al., "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Julia Rauscher, and Bernhard Bauer, "Safety and Security Architecture Analyses Framework for the Internet of Things of Medical Devices," *IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Ostrava, Czech Republic, pp. 1-3, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[5] Anastasiia Strielkina et al., "Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment," *IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, pp. 67-73, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Anastasiia Strielkina, Vyacheslav Kharchenko, and Dmytro Uzun, "Availability Models of The Healthcare Internet of Things System Taking Into Account Countermeasures Selection," *Information and Communication Technologies in Education, Research, and Industrial Applications Conference*, pp. 220-242, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jianbing Ni, Xiaodong Lin, and Xuemin Shen, "Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives," *IEEE Network*, vol. 33, no. 2, pp. 50-57, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Truong Thu Huong et al., "LocKedge: Low-Complexity Cyberattack Detection in IoT Edge Computing," *IEEE Access*, vol. 9, pp. 29696-29710, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Truong Thu Huong et al., "An Efficient Low Complexity Edge-Cloud Framework for Security in IoT Networks," *IEEE Eighth International Conference on Communications and Electronics (ICCE)*, Phu Quoc Island, Vietnam, pp. 533-539, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Julia Rauscher, and Bernhard Bauer, "Adaptation of Architecture Analyses: An IoT Safety and Security Flaw Assessment Approach," *Proceedings of the 14th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2021)*, pp. 320-327, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Omar Cheikhrouhou et al., "A Lightweight Blockchain and Fog-Enabled Secure Remote Patient Monitoring System," *Internet of Things*, vol. 22, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Celestino Obua, MUST Data Science Research Hub (MUDSReH), NIH RePORTER, 2022. [Online]. Available: https://reporter.nih.gov/project-details/10312539#details

[13] Ken Hoyme, Security Safety Co-Analysis Tool Environment (SSCATE), Adventium Enterprises, SBIR STTR America's Seed Fund, 2016. [Online]. Available: https://legacy.www.sbir.gov/sbirsearch/detail/1252209

[14] Ken Hoyme, Security Safety Co-Analysis Tool Environment (SSCATE), Adventium Enterprises, SBIR STTR America's Seed Fund, 2015. [Online]. Available: https://legacy.www.sbir.gov/sbirsearch/detail/869241

[15] Lenore McMackin, SBIR Phase II: Low Cost Shortwave Infrared (SWIR) Spectral Imaging Microscope Camera Based on Compressive Sensing, Inview Technology Corporation, SBIR STTR America's Seed Fund, 2014. [Online]. Available: https://legacy.www.sbir.gov/sbirsearch/detail/704773

[16] Lenore McMackin, SBIR Phase I: Low Cost Shortwave Infrared (SWIR) Spectral Imaging Microscope Camera Based on Compressive Sensing, Inview Technology Corporation, US National Science Foundation, 2013. [Online]. Available: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1315515

[17] Muhammad Yaseen et al., "MARC: A Novel Framework For Detecting MitM Attacks In EHealthcare BLE Systems," *Journal of Medical Systems*, vol. 43, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Alper Kaan Sarica, and Pelin Angin, "A Novel SDN Dataset for Intrusion Detection in IoT Networks," *16th International Conference on Network and Service Management (CNSM)*, Izmir, Turkey, pp. 1-5, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Miloud Bagaa et al., "A Machine Learning Security Framework for IoT Systems," *IEEE Access*, vol. 8, pp. 114066-114077, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nagarathna Ravi, and S. Mercy Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attacks in IoT Via SDN-Cloud Architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559-3570, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] P.K. Binu, Deepak Mohan, and E.M. Sreerag Haridas, "An SDN-Based Prototype for Dynamic Detection and Mitigation of DoS Attacks in IoT," *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, pp. 5-10, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Tolijan Trajanovski, and Ning Zhang, "An Automated and Comprehensive Framework for IoT Botnet Detection and Analysis (IoT-BDA)," *IEEE Access*, vol. 9, pp. 124360-124383, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Harsh Sharma, and Shashank Gupta, "Leveraging Machine Learning and SDN-Fog Infrastructure to Mitigate Flood Attacks," *2021 IEEE Globecom Workshops (GC Wkshps)*, Madrid, Spain, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] Walid I. Khedr, Ameer E. Gouda, and Ehab R. Mohamed, "FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks," *IEEE Access*, vol. 11, pp. 28934-28954, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] Rami J. Alzahrani, and Ahmed Alzahrani, "A Novel Multi Algorithm Approach to Identify Network Anomalies in the IoT Using Fog Computing and A Model to Distinguish Between IoT and Non-IoT Devices," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mingyuan Zang et al., "Toward Continuous Threat Defense: In-Network Traffic Analysis for IoT Gateways," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9244-9257, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Hicham Amellal et al., "Quantum Man-in-the-Middle Attacks on QKD Protocols: Proposal of a Novel Attack Strategy," *6th International Conference on Contemporary Computing and Informatics*, Gautam Buddha Nagar, India, pp. 513-519, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Shatha Alhazmi et al., "Mitigating Man-in-the-Middle Attack Using Quantum Key Distribution," *IEEE Long Island Systems, Applications and Technology Conference*, Old Westbury, NY, USA, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] Abdullah Al Hayajneh, Md Zakirul Alam Bhuiyan, and Ian McAndrew, "Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN)," *Computers*, vol. 9, no. 1, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] S. Aruna et al., "Detect and Prevent Attacks of Intrusion in IoT Devices Using Game Theory with Ant Colony Optimization (ACO)," *Journal of Cybersecurity and Information Management*, vol. 14, no. 2, pp. 275-286, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] Mst Shapna Akter et al., "Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions," *IEEE International Conference on Big Data*, Sorrento, Italy, pp. 5408-5417, 2023. [CrossRef] [Google Scholar] [Publisher Link]