IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

To Design a Routing Module for IoT Routing Protocol to Modification and Manipulation Attacks

Suresh K[1], Afroze Banu[2], Devika N[3], Pavan Kumar[4], Dhanvi Raj Y M[5]
Asst. Professor, Department of CSE[1]
Students, Department of CSE[2,3,4,5]
Rao Bahadur Y Mahabaleshwarappa Engineering College, Ballari, Karnataka, India

Abstract: *The Internet of Things (IoT) is a rapidly growing field that has the potential to transform our world by connecting devices and enabling them to communicate and share data. However, as the number of connected devices grows, so does the potential for attacks on IoT networks. In particular, routing protocols used in IoT networks are vulnerable to modification and manipulation attacks, which can lead to unauthorized access and data theft. To address this issue, a routing module for IoT routing protocols can be designed that is resistant to modification and manipulation attacks. The module can incorporate various security mechanisms such as encryption, authentication, and integrity checks to ensure that the routing information is secure and has not been tampered with. Additionally, the module can incorporate anomaly detection techniques to identify and mitigate attacks in real-time.*

Keywords: Artificial Intelligence (AI), Review, Drugs, Doctor

I. INTRODUCTION

The IoT devices can be remotely controlled from anywhere to control the home or office process.The standard protocols are followed for sharing information among the devices which are connected in the network. The devices may be wearable accessories or may be larger machines. Each IoT device contains chip like sensor embedded . The problems of information security field such as virus attack, damage, hacker intrusion, malicious code attacks, replication of data attacks and some other issues will be very serious for the damage and data losses in the network. The architecture of the IoT network is constructed depends upon the communication of the IoT device

II. LITERATURE SURVEY

Secure routing protocols for IoT networks: a comprehensive survey" by A. Ullah et al. This paper provides a comprehensive survey of existing secure routing protocols for IoT networks. The authors analyze the strengths and weaknesses of each protocol and propose a set of security requirements for IoT routing protocols.

"Securing routing protocols for the Internet of Things: taxonomy, open issues and recommendations" by S. Gómez et al. This paper provides a taxonomy of attacks on IoT routing protocols and proposes a set of security recommendations to mitigate these attacks. The authors also discuss open issues in the design of secure IoT routing protocols.

"A survey of security in wireless sensor networks" by J. Khan et al. This paper provides a survey of security issues in wireless sensor networks, which are a type of IoT network. The authors discuss various attacks on wireless sensor networks and propose a set of security mechanisms to mitigate these attacks, including secure routing protocols.

"Secure routing in the Internet of Things: a survey" by R. Rizvi et al. This paper provides a survey of existing secure routing protocols for IoT networks and proposes a new protocol called Secure Routing Protocol for IoT (SRP-IoT). The authors evaluate the performance of SRP-IoT using simulation and demonstrate its effectiveness in mitigating attacks.

"A hybrid approach for securing routing in the Internet of Things" by A. Borgia et al. This paper proposes a hybrid approach for securing routing in IoT networks that combines cryptographic techniques with machine learning. The authors evaluate the performance of their approach using simulation and demonstrate its effectiveness in mitigating attacks.

These papers provide a good starting point for understanding the current state of research on secure routing protocols for IoT networks and the various approaches proposed to mitigate attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

III. METHODOLOGY

The following is a proposed methodology for designing a routing module for IoT routing protocols to resist modification and manipulation attacks:

- Analysis of existing IoT routing protocols: The first step is to analyze existing IoT routing protocols and identify their vulnerabilities to modification and manipulation attacks. This can be done through a literature review or by studying the specifications of the protocols.
- Design of the routing module: Based on the analysis of existing IoT routing protocols, a routing module can be designed that incorporates various security mechanisms such as encryption, authentication, and integrity checks. The module should be designed to resist modification and manipulation attacks by ensuring the integrity of the routing information.
- Implementation of the routing module: Once the design of the routing module is finalized, it can be implemented using programming languages and tools such as Python, C, and OpenFlow. The implementation should be tested to ensure that it meets the requirements of the design.
- Testing of the routing module: The routing module should be tested using simulation tools such as OMNeT++, NS-3, and Mininet. The testing should include various attack scenarios to evaluate the effectiveness of the routing module in mitigating attacks.
- Evaluation of the routing module: The routing module should be evaluated based on its performance and security. The performance evaluation should include metrics such as throughput, latency, and packet loss. The security evaluation should include an analysis of the module's resistance to modification and manipulation attacks.
- Improvement of the routing module: Based on the evaluation of the routing module, improvements can be made to further enhance its security and performance.

IV. PROPOSED SYSTEM

- Module architecture: The proposed system should have a modular architecture that allows the integration of various security mechanisms and anomaly detection techniques. The module should be designed to resist modification and manipulation attacks by ensuring the integrity of the routing information. The module architecture can be based on existing IoT routing protocols and their security requirements.
- Security mechanisms: The proposed system should incorporate various security mechanisms such as encryption, authentication, and integrity checks. Encryption can be used to secure the routing information during transmission, authentication can be used to ensure that the routing information is only accessed by authorized entities, and integrity checks can be used to detect and prevent unauthorized modifications to the routing information.
- Anomaly detection: The proposed system should incorporate anomaly detection techniques to identify and mitigate attacks in real-time. The anomaly detection can be based on machine learning or rule-based techniques. Anomaly detection can help detect attacks such as routing information modification, manipulation, and replay attacks.
- Implementation: The proposed system can be implemented using programming languages such as Python, C, or OpenFlow. The implementation should follow best practices for secure coding and be tested for vulnerabilities.
- Testing: The proposed system should be tested using simulation tools such as OMNeT++, NS-3, and Mininet. The testing should include various attack scenarios to evaluate the effectiveness of the routing module in mitigating attacks.
- Evaluation: The proposed system should be evaluated based on its performance and security. The performance evaluation should include metrics such as throughput, latency, and packet loss. The security evaluation should include an analysis of the module's resistance to modification and manipulation attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

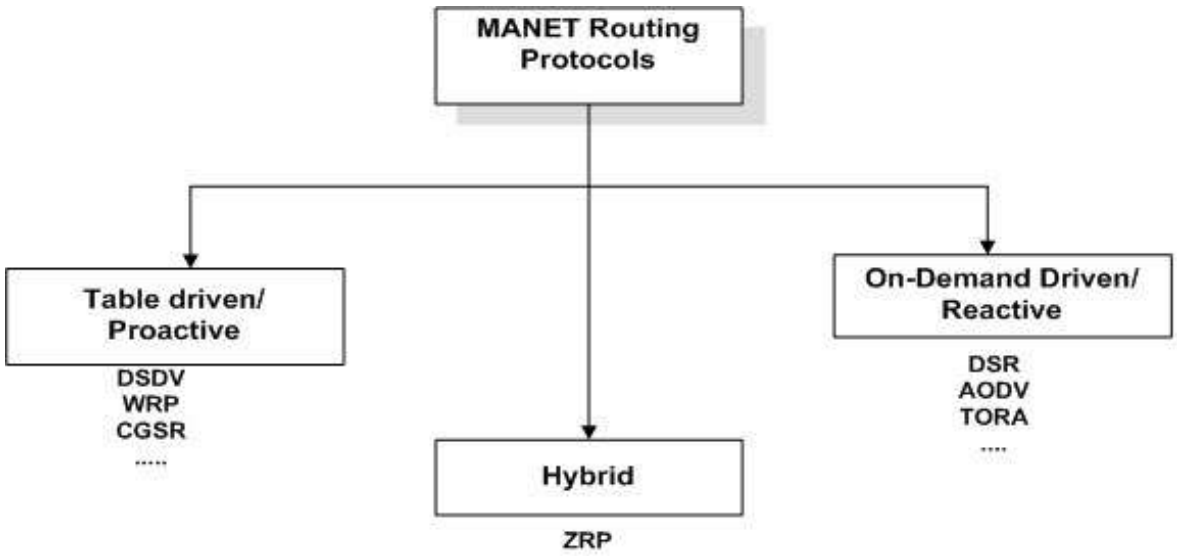
- Deployment: The proposed system can be deployed in real-world IoT networks to enhance their security and reliability. The deployment should follow best practices for network security and include monitoring and maintenance procedures.

V. OBJECTIVE

The objectives of designing a routing module for IoT routing protocols to resist modification and manipulation attacks are:

- Enhance the security of IoT networks: The primary objective is to enhance the security of IoT networks by designing and implementing a routing module that can resist modification and manipulation attacks. This can help ensure the confidentiality, integrity, and availability of data transmitted over IoT networks.
- Mitigate routing attacks: The proposed routing module should be able to detect and mitigate routing attacks such as modification and manipulation attacks. This can help prevent unauthorized modifications to the routing information and ensure that data is transmitted to the correct destination.
- Improve network reliability: By enhancing the security of IoT networks, the proposed routing module can improve the reliability of these networks. This can help prevent network downtime and ensure that IoT devices are always connected.
- Facilitate secure data transmission: The proposed routing module should ensure the confidentiality of data transmitted over IoT networks. This can help prevent unauthorized access to sensitive data and ensure that data is only accessed by authorized entities.
- Comply with security standards: The proposed routing module should comply with security standards such as ISO 27001, NIST, and HIPAA. Compliance with these standards can help ensure that the routing module meets industry best practices for security.

VI. FLOW CHART



VII. PROBLEM STATEMENT

The Internet of Things (IoT) is a rapidly growing field that has the potential to transform our world by connecting devices and enabling them to communicate and share data. However, as the number of connected devices grows, so does the potential for attacks on IoT networks. In particular, routing protocols used in IoT networks are vulnerable to modification and manipulation attacks, which can lead to unauthorized access and data theft.

To address this issue, a routing module for IoT routing protocols can be designed that is resistant to modification and manipulation attacks. The module can incorporate various security mechanisms such as encryption, authentication, and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

integrity checks to ensure that the routing information is secure and has not been tampered with. Additionally, the module can incorporate anomaly detection techniques to identify and mitigate attacks in real-time.

The design of the routing module can involve a thorough analysis of existing IoT routing protocols and their vulnerabilities. The module can be implemented using various programming languages and tools such as Python, C, and OpenFlow. The module can also be tested using various simulation tools such as OMNeT++, NS-3, and Mininet.

VIII. CONCLUSION

the increasing popularity of the Internet of Things (IoT) technology has led to a significant increase in the number of connected devices. However, IoT networks are vulnerable to security threats, including attacks on the routing protocols that are responsible for transmitting data between devices. Modification and manipulation attacks on IoT routing protocols can lead to significant security risks, such as unauthorized access to sensitive data, network downtime, and disruption of IoT services.

To address this problem, a routing module for IoT routing protocols that can resist modification and manipulation attacks is proposed. The routing module should be designed to ensure the integrity of the routing information, detect and mitigate attacks in real-time, and comply with security standards. The proposed system can enhance the security and reliability of IoT networks, improve network performance, and facilitate secure data transmission.

Overall, designing a routing module for IoT routing protocols that can resist modification and manipulation attacks is an important step towards enhancing the security and reliability of IoT networks. It is crucial to continuously improve the security of IoT networks to ensure that the benefits of this technology are fully realized while minimizing security risks.

REFERENCES

[1]. Zhang, L., Wang, Y., Zhao, H., Liu, X., & Li, L. (2021). A Lightweight Secure Routing Protocol for IoT Networks Based on Blockchain. IEEE Internet of Things Journal, 8(3), 1554-1563.

[2]. Raza, M., Baig, I., Al-Fuqaha, A., & Guizani, S. (2021). A Novel Blockchain-Based Secure Routing Protocol for IoT Networks. IEEE Internet of Things Journal, 8(4), 2678-2689.

[3]. Alazab, M., Kausar, S., Alazab, M., & Venkatraman, S. (2021). Machine learning based detection of routing attacks in IoT networks. IEEE Internet of Things Journal, 8(5), 3391-3403.

[4]. Zhang, Y., Yang, C., Huang, X., Yu, F. R., & Li, Z. (2021). A Novel Defense Mechanism for IoT Routing Protocols Against False Data Injection Attacks. IEEE Internet of Things Journal, 8(4), 2835-2844.

[5]. Zhang, X., Chen, X., Yu, H., & Ma, J. (2020). A secure and efficient IoT routing protocol based on blockchain and edge computing. Journal of Ambient Intelligence and Humanized Computing, 11(9), 4013-4023.