

Evaluating Cross-Layer Security and Trustworthiness in Modern Network Architectures

Student Name: Redhwan Murshed Hamood Moqbel

Course Code: Research Methodology in Computer Science (A1800)

Lecturer: Dr. Mohammed Anbar

Contents

Contents	I
Abstract	II
Chapter 1: Introduction	1
1.1 Background	2
1.2 Problem Statement	2
1.3 Research Objectives	2
1.4 Research Scope	3
Chapter 2: Literature Review	4
2.1 Studies:	5
2.2 Comparative Summary of Related Studies	8
3.1 Methodology Overview	10
3.2 Expected Outcomes	10
3.3 Project Timeline (Gantt Chart)	10
References	11

Abstract

This research tackles the growing security problems in Internet of Things (IoT) and wireless networks. Right now, traditional security models just don't work well for small, battery-powered devices. This study suggests a "cross-layer" approach to figure out if a network node is trustworthy. Instead of using heavy encryption, we look at statistical features from the lower network layers (like signal strength). By using a method called Change point Detection (CPD), the goal is to tell the difference between actual cyberattacks—like sinkholes—and normal wireless interference. The end goal is to create a lightweight security system that cuts down on false alarms without draining device batteries.

Chapter 1: Introduction

1.1 Background

The IoT has completely changed how we connect, bringing billions of devices into areas like healthcare, smart homes, and factories. To save battery life and run smoothly, these networks use lightweight protocols like MQTT and CoAP. But there's a catch: being "lightweight" usually means sacrificing security. The standard TCP/IP security methods we use on regular computers are simply too heavy for small IoT sensors. If we try to use them, the devices run out of battery or processing power very quickly, which leaves a massive gap in how we protect wireless networks.

1.2 Problem Statement

The main issue in IoT security today is a frustrating trade-off. Standard encryption (like TLS/SSL) drains too much power, while traditional Intrusion Detection Systems (IDS) make too many mistakes in wireless setups. Most current defenses rely on fixed rules or "static thresholds." The problem with this is that they can't tell if a dropped signal is caused by a hacker or just natural wireless noise, which leads to a ton of false alarms. On top of that, internal routing attacks—like sinkholes—can easily sneak past perimeter defenses by acting like normal devices. We really need a dynamic, cross-layer system that measures network "trust" based on real-time behavior rather than strict, outdated rules.

1.3 Research Objectives

To figure out exactly where the performance bottlenecks are when we try to secure standard IoT protocols like MQTT and CoAP.

To pinpoint specific Quality of Service (QoS) signs—like signal drops at the physical layer—that act as red flags for internal routing attacks.

To build a trustworthiness model using Changepoint Detection (CPD) that adapts to natural wireless fluctuations instead of relying on fixed rules.

To test how well this new model spots sinkhole attacks compared to older, single-layer security methods, focusing heavily on both accuracy and battery use.

1.4 Research Scope

This study focuses specifically on wireless IoT devices running on the IEEE 802.15.4 standard. We are only looking at internal routing attacks (specifically sinkholes) and cross-layer anomalies. The research will not cover physical damage to the devices or massive external DDoS attacks.

Chapter 2: Literature Review

2.1 Studies:

Hmissi & Ouni (2022):

This research compared the largest IoT application protocol layers (MQTT, CoAP, DDS and AMQP) from an efficiency, security, interoperability and Quality of Service perspective. They showed that the use of lightweight protocols will help to enhance communication performance for constrained devices. However, security and interoperability challenges remain unresolved and more effective cross-layer solution development is required.

Jahangeer et al. (2023):

An overview of the network layer security of Internet of Things (IoT) devices and the relevant attacks connected to the Routing Protocol for Low Power and Lossy Networks (RPL). The study looks specifically at four types of RPL protocol attacks; Sinkholes, Wormholes, Sybils, and Blackholes. Additionally, existing detection and prevention mechanisms are examined. This includes Machine Learning-based solutions. The conclusion drawn is that while the current solutions available increase the level of security, there is still a need for lightweight, efficient mechanisms that are appropriate for use in resource-constrained IoT settings.

Anani and Ouda (2024):

The goal of the research was to create a reliable but lightweight wireless M-Bus (Meter Bus) communication system using the Noise Protocol Framework (NPF). The protocol combines the NX and XX handshake(s) from NPF to provide greater security without draining batteries. Performance comparisons with TLS showed that, compared to TLS, the proposed wireless M-Bus protocol had a lower memory footprint, smaller messages, faster handshakes, and a significantly longer lifetime (up to 9.51 years for NX on a single battery) making it very suitable for resource-constrained environments such as smart metering and IoT (Internet of Things) applications.

Iqbal et al. (2021)

The approach of this research proposed ALAM, an Anonymous Lightweight Authentication Mechanism, to Software-Defined Networking (SDN)-based smart homes; This combines lightweight cryptographic functions such as hashing, exclusive OR (XOR), and symmetric keys with SDN technology to develop a mutual anonymous authentication for Internet of Things (IoT) that have limited resources. Through the formal verification of the design using both BAN Logic and ProVerif as well as conducting performance evaluations, ALAM was determined to provide anonymity, provide resistance to replay attacks, support secure key exchange, and have lower execution time (0.1236 millisecond) than existing solutions resulting in being a viable option for protecting intelligent home networks.

Aslan & Aslan (2023)

This study examined IoT protocols through the OSI model and the TCP/IP model, as well as their ability to interoperate, and how to map at the protocol level. We researched several different IoT protocols including 6LoWPAN, ZigBee, Bluetooth, LoRaWAN, Z-Wave, NFC and Sigfox and compared their architecture layers, communication distance/frequency, and data rates. The results of our study indicate that the five-layer IoT architecture provides much greater overall coverage than a standard architecture and that the selection of a protocol depends on several factors including application distance requirements, power efficiency and the amount of data required for transmission.

Yuan et al. (2022)

The objective of this research is to provide a new way of classifying malware targeting Internet-of-Things (IoT) devices by creating a lightweight Convolutional Neural Network (LCNN) for classifying malware using multidimensional Markov Images (MMIs) from the executables of malicious software instead of conventional feature extraction. The architecture of the trained model is composed of depthwise convolutional layers followed by channel shuffling to achieve a lower model complexity than the size of the dataset used (approximately 1 MB). Experimentation on several separate datasets demonstrates that the proposed method can achieve more than 95% accuracy; in fact, some implementations of the LCNN provided classifying accuracy above 99.356%. This is an improvement in performance when compared to using a heavier Deep Neural Network (DNNs) such as VGG16 and ResNet50. Furthermore, the results of this study indicate that this classification method is accurate and capable of being used on IoT resources that have limited processing power.

Khan et al. (2021)

The purpose of this survey was to identify lightweight cryptography protocols suitable for use on resource-constrained Internet of Things (IoT) devices. It identified strengths, weaknesses and vulnerabilities of these protocols as applicable to the four different layers of an IoT ecosystem—device, edge node, fog node, and cloud. The survey found that many existing lightweight solutions improve security efficiency but are unable to account for the fact that different IoT systems may have access to varying levels of resources and therefore, more adaptive and elastic cryptography protocols will be required to ensure secure and scalable cross-layer IoT protection.

Karoliny et al. (2025)

A trustworthiness computation framework for wireless networks has been developed that utilizes Quality of Service (QoS) attributes from the network layers and Change-point Detection (CPD) is used to identify differences between normal behavior, different types of attacks, and failures within the system itself. A trustworthiness model that includes three steps was tested in IEEE 802.11 environments and demonstrated that the framework effectively identified attacks, malfunctioning nodes, as well as communication anomalies which supports its claims to provide cross-layer trustworthiness evaluations in Internet of Things (IoT) and/or wireless devices.

Khan and Hasan (2017)

The potential significance of this study is to offer an updated overview of the various types of network threats, cyber attacks, and security countermeasures available today using a classification scheme for attack types that includes both passive and active types of attacks such as phishing, hijacking, malware, and denial of service. The research illustrated that traditional defensive strategies like firewalls, anti-virus programs, and signature-based intrusion detection systems continue to play an important role; however, the shortcomings of traditional static rules-based methodology when confronted with changing patterns of malicious behaviour means other more agile or adaptable forms of defence are required.

Murkomen (2024)

A thorough examination of TCP/IP application layer protocol performance, security, and privacy was conducted in this study. The protocol types studied included: HTTP, HTTPS, FTP, SMTP, DNS and DHCP; and the research found many challenges with regards to performance and security, including but not limited to latency, bandwidth limitations, session hijacking, DNS attacks, and a lack of privacy protection within the protocols studied. The results from this research illustrate that current strategies must be improved through developing stronger protocol protection methods, using adaptive protection methods, as well as utilizing new technologies (e.g., IoT and machine learning) to enhance both security and efficiency for all forms of communication.

2.2 Comparative Summary of Related Studies

Study	Focus	Method/Approach	Key Findings	Gap / Limitation
Jahangeer et al. (2023)	IoT network security	ML-based detection, RPL attack review	Attack detection improvement	High computation overhead
Khan & Hasan (2017)	Network threats / IDS	Rule-based security review	Traditional IDS limitations	Static defense models
Hmissi & Ouni (2022)	IoT protocols (MQTT, CoAP)	Protocol survey	Efficiency vs security trade-off	Weak built-in security
Karoliny et al. (2025)	Trustworthiness computation	CPD + QoS features	98.7% attack/noise detection	Limited integrated frameworks
Aslan & Aslan (2023)	Cross-layer IoT protocols	Architecture comparison	Protocol diversity challenges	No unified security standard
Anani & Ouda (2024)	Lightweight secure communication	Noise Protocol Framework	Energy-efficient secure protocol	Focused on specific protocol
Nanda et al. (ALAM) (2020)	Lightweight authentication	SDN + lightweight crypto	Low-cost secure authentication	Smart home focused
Nyangaresi et al. (2020)	Lightweight cryptography	Survey / comparative analysis	Adaptive crypto need	Limited elastic solutions
Yuan et al. (2021)	IoT malware detection	Lightweight CNN	High accuracy, low complexity	Malware classification scope
Murkomen (2024)	TCP/IP app-layer security	Security/privacy survey	Protocol vulnerabilities identified	Broad survey, no unified model

Chapter 3: Research Methodology

3.1 Methodology Overview

The project will follow a straightforward, four-step testing process:

1. Simulation: We will use network simulators (like Cooja or NS-3) to build a controlled wireless environment.
2. Data Collection: We'll gather network health metrics (like RSSI and Packet Delivery Ratio) while the network is running normally, and again while simulating a Sinkhole attack.
3. Algorithm Implementation: We will apply the CPD mathematical model to the data to calculate a real-time "Trustworthiness Index."
4. Testing and Comparison: Finally, we'll compare our model's speed and accuracy against standard, threshold-based security systems to see how it performs.

3.2 Expected Outcomes

- A working cross-layer framework that actually protects IoT devices in real-time.
- A massive drop in false alarms caused by everyday wireless noise.
- A lightweight security algorithm that runs comfortably on devices with very little RAM (under 128KB).

3.3 Project Timeline (Gantt Chart)

Project Phase	Month 1	Month 2	Month 3	Month 4
Literature review and identifying gaps				
Setting up simulation and collecting data				
Building and testing the trust algorithm				
Analyzing results and final thesis writing				

References

- [1] Aslan, F. Y., & Aslan, B. (2023). Comparison of IoT protocols with OSI and TCP/IP architecture. *International Journal of Engineering Research and Development*, 15(1), 333–343. <https://dergipark.org.tr/en/pub/umagd/article/1063036>
- [2] Anani, W., & Ouda, A. (2024). A secure lightweight wireless M-Bus protocol for IoT: Leveraging the noise protocol framework. *IEEE Access*.
<https://ieeexplore.ieee.org/document/10705901>
- [3] Hmissi, F., & Ouni, S. (2022). A survey on application layer protocols for IoT networks. *International Journal on Advances in Telecommunications*, 15(1–2), 11–20.
<https://arxiv.org/abs/2405.15901>
- [4] Jahangeer, A., Bazai, S. U., Aslam, S., Marjan, S., Anas, M., & Hashemi, S. H. (2023). A review on the security of IoT networks: From network layer's perspective. *IEEE Access*.
<https://ieeexplore.ieee.org/document/10047861>
- [5] Karoliny, J., Etzlinger, B., Khanzadeh, R., Springer, A., & Bernhard, H.-P. (2025). Network support layers trustworthiness computation for wireless networks. *IEEE Transactions on Communications*, 73(3), 1879–1894. <https://ieeexplore.ieee.org/document/10663457>
- [6] Khan, R., & Hasan, M. (2017). Network threats, attacks and security measures: A review. *International Journal of Advanced Research in Computer Science*, 8(8), 116–120.
https://www.researchgate.net/publication/322665241_NETWORK_THREATS_ATTACKS_AND_SECURITY_MEASURES_A_REVIEW
- [7] Murkomen, T. (2024). Performance, privacy, and security issues of TCP/IP at the application layer: A comprehensive survey. *GSC Advanced Research and Reviews*, 18(3), 234–264. <https://gsconlinepress.com/journals/gscarr/content/performance-privacy-and-security-issues-tcpip-application-layer-comprehensive-survey>
- [8] Nanda, A., Puthal, D., Rodrigues, J. J. P. C., & Kozlov, S. (2020). ALAM: Anonymous lightweight authentication mechanism for SDN-enabled smart homes. *IEEE Internet of Things Journal*. <https://ieeexplore.ieee.org/document/9197651>
- [9] Nyangaresi, V. O., Abdullah, M. T., & Hassan, R. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. *IEEE Access*, 8, 205580–205606.
<https://ieeexplore.ieee.org/document/9205259>
- [10] Yuan, B., Wang, J., Wu, P., & Qing, X. (2021). IoT malware classification based on lightweight convolutional neural networks. *IEEE Transactions on Emerging Topics in Computational Intelligence*. <https://ieeexplore.ieee.org/document/9496689>