Robustness of Federated Malware Detection Under Byzantine Attacks in IoT Networks

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 9 peer-reviewed papers addressing the following research question: How do different aggregation algorithms (FedAvg, FedProx, FedNova) affect the robustness of federated malware detection systems against Byzantine attacks on IoT networks when measured by model. This work investigates the possibilities enabled by federated learning concerning IoT malware detection and studies security issues inherent to this new learning paradigm. In this context, a framework that uses federated learning to detect malware affecting IoT devices is. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 6.5/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Federated Learning for Malware Detection in IoT Devices. Research question: How do different aggregation algorithms (FedAvg, FedProx, FedNova) affect the robustness of federated malware detection systems against Byzantine attacks on IoT networks when measured by model accuracy degradation?.

2 Methodology

Systematic literature search across multiple databases yielded 9 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 6.5/10.

3 Results

9 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 6.5/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

References

- http://arxiv.org/abs/2104.09994v3
- http://arxiv.org/abs/2006.16545v1
- http://arxiv.org/abs/2506.01989v2