Submission Overview

Initial Submission

This manuscript has been submitted to the editorial office for review. Changes cannot be made during editorial review, but you can view the information and files you submitted, below.

Download Reviewer PDF

Article Type

Research Article

Title

Confidence-Based Model Fusion for Robust Adversarial Detection in Multi-Controller SDNs

Manuscript Files

Name	Type of File	Size
CBMF IEEE Final .docx	Main Document - MS Word	1.6 MB

Abstract

Machine Learning (ML)-based Network Intrusion Detection Systems (NIDS) are increasingly deployed in Software-Defined Networks (SDNs) to detect anomalous traffic. However, adversarial poisoning attacks such as Random Label Manipulation (RLM) can compromise model integrity, especially in Multi-Controller SDN (MSDN) environments. The Trans-controller Adversarial Perturbation Detection (TAPD) framework addresses this by transferring models across controllers and using voting to identify compromised nodes. Yet TAPD treats all controller votes equally, ignoring model reliability. In this paper, we propose Confidence-Based Model Fusion (CBMF), a novel enhancement to TAPD that weights each controller's vote by its confidence score derived from self-evaluation error. CBMF improves detection accuracy by reducing the influence of compromised controllers. We validate CBMF on the UNR-IDD dataset and demonstrate significant improvements in detection precision, recall, and robustness under varying attack intensities.

Authors

Name	Email	Country/Location
M.V.Balaganesh BTech [1] Corresponding Author Submitting Author 0009-0007-6265-4965	balaganeshmv@gmail.com	India
Shinmaya K.B [1]	shriassociates.com_bit27@mepcoeng.ac.in	India
Shree Harini [1]	anitha.karhikeyan1_bit27@mepcoeng.ac.in	India
Varsha G. A [1]	1515arunkumar_bit27@mepcoeng.ac.in	India

Affiliations

1. Department of Information Technology

We will use the best match from our database to determine if your manuscript is eligible for special benefits. Matched organizations are for internal purposes and will not be published.

Matched organization
Mepco Schlenk Engineering College Department of Information Technology
SIVAKASI, India

Additional Information

Funders

No funding was received for this manuscript

Keywords

- Communication Security
- Information Security
- Privacy

Subject Area

Information Security

Is this submission for a special issue?

No, this is not for a special issue

Has this manuscript been submitted previously to this journal?

No, it wasn't submitted previously

Has a version of this manuscript previously been made available elsewhere online, as a preprint or other format?

No, it is not available

Would you like to make your research publicly available as a preprint?

No, I do not want to preprint my manuscript

Cover letter / Comments

No, I don't have additional comments

History

Submitted On	1 November 2025 by Bala Ganesh Mv
	Show this version history
Submission Started	1 November 2025 by Bala Ganesh Mv