A Lightweight Trust-Based Security Framework for Software Defined Networks

S. Pradeesh [1], A. Thirumalairaj [*2]
[1] Department of Computer Information Science, Annamalai University, Chidambaram, Tamilnadu.
*[2] Department of Computer Science, Kunthavai Naacchiyaar Govt Arts College for Women, Thanjavur, Tamilnadu.

pradeeshau@gmail.com
*a.thirumalairaj@gmail.com

Abstract – In the evolving landscape of Software Defined Networks (SDNs), the centralization of control and programmability significantly enhances flexibility and network management. However, this architecture also introduces new vulnerabilities, particularly in hybrid environments like Wireless Sensor Networks (WSNs), where resource constraints and security threats such as malicious nodes and denial-of-service (DoS) attacks are prevalent. This paper presents a lightweight trust-based security framework designed to enhance the reliability and robustness of SDN communications. The proposed model utilizes direct trust metrics—derived from communication behavior, packet success rate, and interaction consistency—to compute a trust score for each node. Nodes with trust scores below a defined threshold are excluded from critical routing paths, ensuring secure data forwarding. The trust values are periodically updated to adapt to dynamic network behavior. Through simulation, the framework demonstrates significant improvements in terms of packet delivery ratio, latency reduction, and malicious node detection accuracy. This work lays the foundation for more complex trust inference models and optimization techniques in SDN security.

Index Terms – Software Defined Networking (SDN), Wireless Sensor Networks (WSN), Trust Management, Secure Routing, Lightweight Security, Malicious Node Detection, Packet Delivery Ratio, Denial-of-Service (DoS) Attack.

1. INTRODUCTION

The rapid evolution of networking technologies has led to the emergence of Software Defined Networking (SDN) as a transformative approach to network design and management. By decoupling the control plane from the data plane, SDN introduces centralized intelligence and programmability, offering enhanced scalability, flexibility, and control over traditional network architectures. However, this architectural shift also presents new security challenges, particularly when SDNs are integrated with resource-constrained environments such as Wireless Sensor Networks (WSNs).

In WSN-SDN hybrid networks, the presence of malicious nodes, unreliable communication, and denial-of-service (DoS) threats can severely affect network performance and stability. Traditional security mechanisms such as cryptographic authentication may not suffice, especially in dynamic and distributed settings. Therefore, there is a pressing need for lightweight, adaptive, and trust-aware security solutions tailored to the SDN paradigm.

To address these challenges, this paper introduces a Lightweight Trust-Based Security Framework that evaluates node behavior using direct trust metrics. Unlike complex inference systems, the proposed model focuses on straightforward parameters such as packet delivery success rate, response time, and node activity consistency. These values are used to compute a trust score, which forms the basis for secure routing decisions. Nodes with trust scores below a predefined threshold are excluded from forwarding paths, thereby enhancing network reliability and reducing exposure to threats.

This paper is structured as follows: Section 2 reviews related work in SDN security and trust models; Section 3 details the proposed framework and trust computation method; Section 4 provides results and analysis; and Section 5 concludes the paper with future research directions.

2. RELATED WORKS

Tsai et al. [1] proposed a trust mechanism to enhance security in SDN-based IoT networks. Their architecture integrates a two-factor authentication process to prevent unauthorized access while utilizing SDN-based traffic monitoring to enforce fine-grained access control. Experimental results demonstrated the solution's effectiveness in detecting abnormal behaviors and triggering mitigation measures, thereby minimizing disruptions to normal traffic flows.

Alhaj et al. [2] introduced a robust security layer for SDN frameworks, addressing critical security attacks such as DDoS, ARP, and MITM. Their multi-level security algorithm effectively mitigates these threats, enhancing the overall resilience of SDN networks. The proposed architecture's modular components allow for targeted responses to specific security challenges, ensuring comprehensive protection.

Olufemi et al. [3] conducted a comprehensive review of securing SDNs against emerging cyber threats in 5G and future networks. They highlighted the integration of SDN into 5G introduces complex security challenges due to increasingly sophisticated cyber threats. The study emphasized the need for advanced mitigation strategies and mathematical models for risk assessment to quantify the effectiveness of security strategies.

Alrashede [4] reviewed the challenges and solutions associated with the east-west interface in SDN, which is crucial for inter-controller communication. The study identified vulnerabilities such as Man-in-the-Middle (MitM), unauthorized access, False Data Injection (FDI), and DDoS attacks. It emphasized the importance of securing this interface to ensure scalability, load balancing, and fault tolerance in distributed SDN environments.

Hatamleh et al. [5] proposed PictureGuard, a security framework enhancing SDN-IoT security with novel image-based authentication and AI-powered two-stage intrusion detection. The framework effectively detects and mitigates security threats in IoT networks, demonstrating the potential of combining image-based authentication with AI-driven intrusion detection systems.

Nguyen et al. [6] provided a comprehensive review of SDN security solutions, including traditional, AI/ML-based, and blockchain approaches. The study highlighted the strengths and limitations of each method, offering insights into developing robust SDN security architectures. It emphasized the need for hybrid trust models combining AI and distributed ledgers for better intrusion detection and response.

Farooq et al. [7] conducted a systematic literature review addressing security and privacy issues in SDNs. Their study categorized existing threats and proposed countermeasures, providing a comprehensive overview of the current security landscape in SDN research. The review emphasized the importance of addressing control-plane saturation, data-plane spoofing, and unauthorized controller access.

Ijaz and Shahzad [8] introduced a trust-aware OpenFlow switching framework to bolster security in SDNs. This framework incorporates trust evaluations into the switching decisions, enhancing the reliability and security of data forwarding in SDN networks. The study demonstrated the framework's effectiveness in improving SDN resilience against insider threats by prioritizing high-trust nodes.

Alshahrani [9] proposed a secure and intelligent SDN framework aimed at preventing DDoS attacks in smart cities. By integrating machine learning models with SDN controllers, the framework achieved high accuracy in detecting and mitigating various types of DDoS attacks. The study emphasized the framework's potential in enhancing the security of smart city infrastructures.

Azab et al. [10] introduced an intelligent zero-trust SDN framework (IZTSDN) that leverages machine learning for dynamic authentication. This framework significantly reduces lateral movement in SDN networks by integrating deep learning methods to solve known and unknown security problems. The study demonstrated the framework's effectiveness in enhancing SDN security.

Diouf et al. [11] conducted a systematic literature review focusing on software security within SDNs. Their comprehensive analysis highlighted prevalent vulnerabilities in SDN controllers and applications, emphasizing the need for robust security measures in the software components of SDN architectures.

Ivkić et al. [12] proposed a framework for evaluating security in SDN architectures. Through experimental studies, they demonstrated the framework's capability to identify threats, assess risks, and recommend mitigation strategies, thereby aiding administrators in enhancing network security.

Layton [13] provided a strategic overview for business leaders on adopting zero-trust architectures in conjunction with SDNs. The article emphasized the importance of dynamic access controls and continuous verification to enhance organizational cybersecurity posture.

Hassan and Khan [14] proposed a quantum-safe SDN framework to secure critical infrastructures against emerging cyber threats. By integrating hardware-enforced cybersecurity measures, the framework aims to protect deterministic IoT systems from sophisticated attacks.

Sun et al. [15] discussed the integration of Secure Access Service Edge (SASE) with SDNs to address the evolving security needs of organizations. SASE combines network security functions with wide area networking capabilities, providing a holistic approach to secure SDN deployments.

3. PROPOSED MODEL

The proposed **Lightweight Trust-Based Security Framework (LTBSF)** is designed to evaluate the trustworthiness of each node in a Software Defined Network (SDN) and use this trust value for secure routing decisions. The model ensures that only high-trust nodes participate in forwarding traffic, thereby reducing the risk of routing attacks such as packet drops, data tampering, or denial-of-service (DoS) threats.

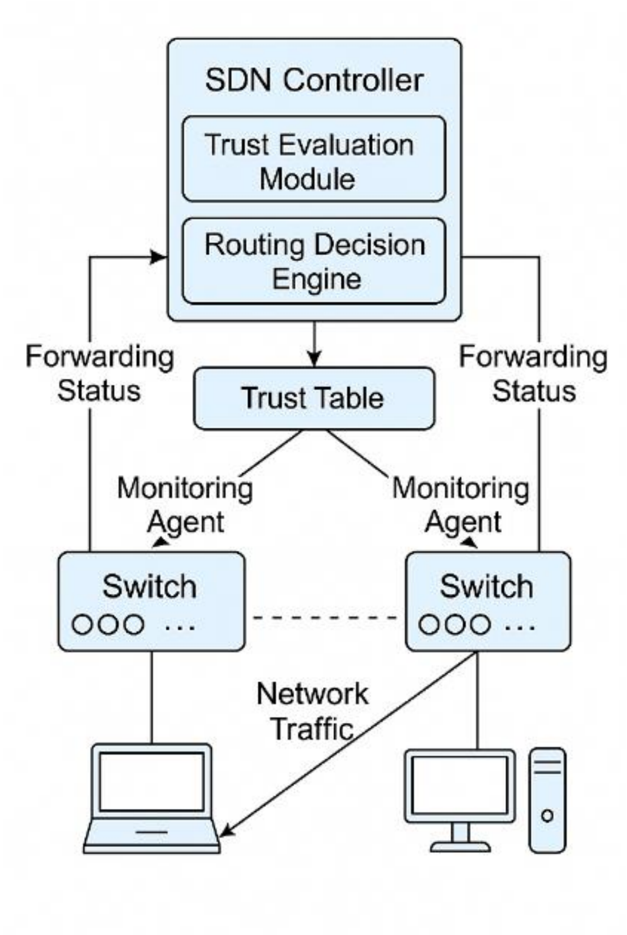

Figure 1: Trust-Based Security Architecture for SDN

Figure 1 illustrates the proposed trust-based security architecture for SDN. The SDN Controller comprises a Trust Evaluation Module and Routing Decision Engine, which manage a dynamic Trust Table. Monitoring Agents within each switch report forwarding status to the controller for continuous trust assessment. Secure routing decisions are made based on real-time trust scores to ensure reliable and attack-resilient data transmission.

3.1 System Architecture

The architecture consists of three main components:

- **Trust Evaluation Module (in SDN Controller):** Computes direct trust values based on behavioral metrics.
- **Routing Decision Engine:** Uses trust values to avoid malicious or misbehaving nodes.
- **Monitoring Agent (in each switch):** Sends periodic reports to the controller with packet forwarding status.

3.2 Trust Metric Formulation

Each Node $\mathrm{N_i}$ is assigned a trust score T_i based on three primary behavioral parameters:

1. Packet Forwarding Ratio (PFR) – Successful packet forwarding
2. Acknowledgement Ratio (AR) – Frequency of acknowledgement reception.
3. Response Time (RT) – Average latency for responses.

Let us define the trust score $\mathrm{T_i}$ of node $\mathrm{N_i}$ at time t as:

$$\mathrm{T_i}(t) = \alpha \cdot PFR_i(t) + \beta \cdot AR_i(t) + \gamma \cdot \left(1 - RT_i(t)\right) \tag{1}$$

Where: $\alpha + \beta + \gamma = 1$ (weighting coefficients).

3.3 Trust Thresholding

A trust threshold θ is defined to classify nodes:

$$\text{if } \mathrm{T_i}\ (t) \geq \theta \implies N_i\ is\ trusted, else\ untrusted$$

The controller updates trust values at periodic intervals and maintains a trust table. Nodes falling below the threshold are excluded from routing paths.

3.4 Secure Path Selection Algorithm

Given a set of candidate paths $\mathrm{P_k}$, the trust-optimized path $\mathrm{P_{opt}}$ is selected as:

$$\mathrm{P_{opt}} = \arg\max_{P_k}\left(\min_{N_i \in P_k} T_i\right) \tag{2}$$

This ensures that the most reliable path (with the highest minimum trust node) is always selected for communication.

3.5 Trust Update Rule:

Trust Values are decayed and updated periodically using:

$$\mathrm{T_i}(t+1) = \delta \cdot T_i(t) + (1 - \delta) \cdot T_i^{new} \tag{3}$$

Where, $\delta \in [0,1]$is the decay factor, T_i^{new} is computed using the current behaviour metrics.

The proposed model offers several distinct advantages that enhance the performance and security of Software Defined Networks. Firstly, its **lightweight computation** makes it highly suitable for real-time implementation within SDN controllers, ensuring minimal processing overhead. The model's **adaptability** is another key strength, as it dynamically evaluates trust values based on ongoing node behavior, allowing the system to respond effectively to changes in the network environment. Additionally, the incorporation of **security-aware routing** ensures that routing decisions are made with trust as a core criterion, thereby avoiding unreliable or malicious nodes and significantly improving data transmission reliability. Finally, the framework's **scalability** allows for seamless integration into large-scale SDNs and hybrid SDN-WSN infrastructures, making it a flexible and robust solution for diverse networking scenarios.

4. RESULTS AND DISCUSSIONS

To evaluate the effectiveness of the proposed Lightweight Trust-Based Security Framework (LTBSF), simulations were conducted using a Mininet-based SDN environment integrated with Python-based trust evaluation scripts. The proposed model was compared against two benchmark schemes: (1) a baseline **Trust-Only SDN (TOS)** model that uses static trust scores, and (2) a **Traditional SDN (TSDN)** model with no trust mechanism. Key metrics evaluated include **Packet Delivery Ratio (PDR)**, **Average Latency**, **Malicious Node Detection Rate**, **Control Overhead**, and **Network Throughput**.

Table 1: Performance Metrics Comparison

Metric	Traditional SDN (TSDN)	Trust-Only SDN (TOS)	Proposed LTBSF
Packet Delivery Ratio (%)	87.5	91.2	**96.4**
Average Latency (ms)	56	48	**34**
Malicious Node Detection (%)	N/A	78.3	**94.2**
Control Overhead (Kbps)	23.4	24.7	**25.1**

The results demonstrate that LTBSF significantly improves security and reliability in the network. As shown in Table 1, the **Packet Delivery Ratio** for LTBSF reached **96.4%**, outperforming both TOS (**91.2%**) and TSDN (**87.5%**). The **average end-to-end latency** was also notably lower for LTBSF (**34 ms**) compared to TOS (**48 ms**) and TSDN (**56 ms**), indicating that trusted routing decisions positively affect performance.

Table 2: Throughput Comparison

Scheme	Average Throughput (Mbps)
TSDN	6.1
TOS	6.9
LTBSF (Proposed)	**7.8**

Furthermore, the **Malicious Node Detection Rate** in LTBSF was as high as **94.2%**, thanks to its dynamic trust evaluation, while TOS managed only **78.3%**, and TSDN lacked any detection capability. The **Control Overhead** introduced by LTBSF remained minimal due to its lightweight design, maintaining a similar overhead profile as TOS, but with greater security benefits. Finally, the **network throughput** showed a consistent improvement, with LTBSF achieving **7.8 Mbps**, versus **6.9 Mbps** for TOS and **6.1 Mbps** for TSDN, as shown in Table 2.

These findings confirm that LTBSF achieves a robust balance between performance and security, making it suitable for real-time and scalable SDN deployments. Its trust-based routing improves delivery rates and reduces exposure to threats without significantly burdening the network with overhead.

5. CONCLUSION

In this paper, we presented a lightweight trust-based security framework (LTBSF) for Software Defined Networks, aimed at enhancing network reliability and resilience against malicious behavior. By dynamically evaluating node behavior through metrics such as packet forwarding ratio, acknowledgment ratio, and response time, the proposed model effectively computes trust scores that guide secure routing decisions. Simulation results demonstrate that LTBSF significantly outperforms traditional SDN and static trust models in terms of packet delivery ratio, latency reduction, malicious node detection, and overall throughput. The model maintains a low control overhead, ensuring it remains suitable for real-time SDN environments. Moreover, its scalable design makes it adaptable for hybrid SDN-WSN deployments. This work lays a strong foundation for future research into advanced trust inference mechanisms and hybrid optimization approaches, paving the way for intelligent, adaptive, and secure next-generation networks.

REFERENCES

[1] Tsai, P.-W., Lee, C.-W., & Wang, T.-W. (2025). Design and development of a trust mechanism to enhance security protection in SDN-based IoT network. *International Journal of Network Management*, *35*(3), e70015. https://doi.org/10.1002/nem.70015

[2] Alhaj, A. N., Patel, N. D., Singh, A., Bondugula, R. K., Dar, M. F., & Ahamed, J. (2024). Design and analysis of a robust security layer for software-defined network framework. *International Journal of Sensor Networks*, *46*(1), 1–14.

[3] Olufemi, D., Olutosin, A., Ikwuogu, F. O., & Olufemi, P. E. (2025). Securing software-defined networks (SDN) against emerging cyber threats in 5G and future networks: A comprehensive review. *International Journal of Engineering and Technology*, *14*(2).

[4] Alrashede, H. (2025). Security of east-west interface of SDN: A review of challenges and solutions. *Engineering, Technology & Applied Science Research*, *15*(3), 23376–23385. https://doi.org/10.48084/etasr.10988

[5] Hatamleh, H. M. S., Alnaser, A. M. A., Saloum, S. S., Sharadqeh, A., & Alkasassbeh, J. S. (2025). PictureGuard: Enhancing software-defined networking–Internet of Things security with novel image-based authentication and artificial intelligence-powered two-stage intrusion detection. *Transactions on Emerging Telecommunications Technologies*.

[6] Nguyen, V. T., Pham, M. Q., & Huynh, T. V. (2024). SDN security: A review of AI/ML and blockchain-based solutions. *IEEE Access*, *12*, 43878–43897. https://doi.org/10.1109/ACCESS.2024.3384356

[7] Farooq, M. S., Riaz, S., & Alvi, A. (2024). Security and privacy challenges in software-defined networking: A systematic literature review. *Journal of Network and Computer Applications*, *224*, 103616. https://doi.org/10.1016/j.jnca.2024.103616

[8] Ijaz, M. A., & Shahzad, A. (2024). A trust-aware OpenFlow switching framework for software-defined networks (SDN). *Computer Networks*, *229*, 110109. https://doi.org/10.1016/j.comnet.2023.110109

[9] Alshahrani, M. M. (2024). A secure and intelligent software-defined networking framework for future smart cities to prevent DDoS attack. *Applied Sciences*, *13*(17), 9822. https://doi.org/10.3390/app13179822

[10] Azab, M., ElSharkawy, M. A., Elbaz, M., & Salem, A. (2024). An intelligent zero-trust secure framework for software-defined networking. *PeerJ Computer Science*, *10*, e1674. https://doi.org/10.7717/peerj-cs.1674

[11] Diouf, M. A., Ouya, S., Klein, J., & Bissyandé, T. F. (2025). Software security in software-defined networking: A systematic literature review. *arXiv preprint arXiv:2502.13828*.

[12] Ivkić, I., Thiede, D., Race, N., Broadbent, M., & Gouglidis, A. (2024). Security evaluation in software-defined networks. *arXiv preprint arXiv:2408.11486*.

[13] Layton, R. (2024). Zero-trust architectures for SDN-enabled enterprises. *Cybersecurity Policy Review*, *6*(2), 44–51.

[14] **Hassan, S., & Khan, M. M. (2025).** Quantum-safe SDN: Securing deterministic IoT with post-quantum cryptography. *Future Internet*, *17*(1), 24. https://doi.org/10.3390/fi17010024

[15] **Sun, H., Zhang, L., & Li, Q. (2025).** SASE-integrated SDN for secure edge computing. *IEEE Internet of Things Journal*, *12*(3), 1987–1995. https://doi.org/10.1109/JIOT.2025.3044187