World Journal of Information Technology
ISSN: 2959-9911
DOI: https://doi.org/10.61784/wjit3007

A BLOCKCHAIN-DRIVEN ALGORITHM FOR ANOMALY DETECTION IN IPV6 NETWORK TRAFFIC

YuXin Li
Jiangxi Normal University (JIANGXI NORMAL UNIVERSITY), Nanchang 330022, Jiangxi,China.
Corresponding Email: Liyuxin202411@163.com

Abstract: As the deployment of IPv6 networks continues to expand, managing security threats becomes increasingly intricate due to the protocol's extensive address space and dynamic traffic patterns. This paper presents a novel blockchain-driven decentralized anomaly detection algorithm designed explicitly for IPv6 networks. By leveraging the inherent properties of blockchain—immutability, transparency, and decentralization—our approach enhances security monitoring capabilities. Integrating traffic analysis with a distributed ledger facilitates improved accuracy in anomaly detection and robust resilience against distributed denial-of-service (DDoS) attacks and other threats. Experimental evaluations conducted in a simulated IPv6 environment demonstrate that the proposed methodology outperforms traditional centralized detection systems, significantly improving detection accuracy, attack mitigation, and data integrity.

Keywords: IPv6 networks; Blockchain-driven security; Anomaly detection algorithm; Decentralized monitoring; DDoS attack resilience

1 INTRODUCTION

The global shift towards IPv6 adoption is driven by the need for a larger address space and enhanced functionalities for IoT and other networked devices. However, IPv6 networks face unique security challenges due to structural differences and a larger address pool, complicating traffic analysis and anomaly detection [1,2]. Existing centralized anomaly detection systems struggle with issues such as single points of failure and vulnerability to interception, making them less effective in distributed IPv6 environments [3,4]. Furthermore, centralized designs can lead to data integrity concerns and increased latency under high-volume attacks, such as DDoS [5].

Recent studies have highlighted the increasing sophistication of attacks targeting IPv6 networks, necessitating more advanced detection mechanisms [6]. Traditional methods often rely on fixed thresholds and known attack signatures, which are inadequate against novel and evolving threats. This underscores the need for adaptive systems that can learn from traffic patterns and anomalies to enhance their detection capabilities. Such adaptability not only aids in recognizing traditional attack methods but also enables effective responses to dynamically changing attack techniques. For instance, incorporating machine learning technologies may allow systems to adjust their detection algorithms in real time within a constantly changing environment, improving their ability to respond to unknown threats.

Moreover, with the proliferation of IoT devices, the volume and variety of traffic in IPv6 networks are set to increase, requiring solutions that can efficiently scale while maintaining high detection accuracy. The expansion will also introduce significant traffic access, resulting in more complex interactions within the network that further complicate traffic analysis and anomaly detection. Therefore, the primary challenges to be addressed include:

- Decentralization: Developing a system that eliminates single points of failure and enhances resilience against attacks.
- Real-time Processing: Implementing mechanisms that can analyze traffic in real-time to detect and respond to anomalies without introducing significant latency.
- Data Integrity: Ensuring that the data collected for anomaly detection is secure from tampering and unauthorized access.

This study proposes a blockchain-integrated algorithm for IPv6 traffic analysis that improves detection accuracy, transparency, and resilience by securely logging network activities and using a consensus-driven approach to ensure consistency [7].

The remainder of this paper is organized as follows: Section 2 reviews related work in anomaly detection and blockchain applications in network security. Section 3 details the proposed methodology, including architecture design and algorithm development. Section 4 presents the experimental setup and results, highlighting the proposed method's performance compared to traditional systems. Finally, Section 5 concludes the paper and discusses future research directions.

2 RELATED WORK

2.1 Anomaly Detection in IPv6 Networks

Anomaly detection in IPv6 networks typically employs two primary methodologies: signature-based and behavior-based approaches. Signature-based methods rely on predefined patterns or signatures of known attacks. At the same time, behavior-based techniques analyze the expected behavior of network traffic to identify deviations that may indicate potential threats. However, both methodologies exhibit significant limitations when applied in large-scale environments due to scalability and adaptability concerns [8]. In particular, the unique characteristics of IPv6, including its expansive address space and diverse traffic patterns, pose substantial challenges in processing the high volumes of data traffic generated. This can adversely affect detection speed and accuracy, increasing the risk of undetected anomalies and successful attacks [9]. Consequently, there is a pressing need for more effective and adaptable detection mechanisms to maintain performance levels in the face of increasing network complexity and traffic volume.

2.2 Blockchain Applications in Network Security

Blockchain technology has opened new avenues for enhancing network security, extending applications to secure data management, access control, and tamper-resistant logging [7]. The decentralized nature of blockchain offers a robust solution to many traditional security challenges by providing a secure and immutable ledger that records all transactions and interactions within a network. While its application in anomaly detection is still nascent, preliminary research indicates significant potential for leveraging distributed ledgers to bolster data authenticity, improve transparency, and enhance resilience against tampering [10]. Integrating blockchain with existing security frameworks may thus facilitate a paradigm shift in how anomaly detection is approached, particularly in the context of IPv6 networks where conventional methods are often inadequate.

2.3 Contributions

This paper introduces a novel block-chain-enhanced anomaly detection model tailored explicitly for IPv6 traffic, effectively addressing the common vulnerabilities associated with centralized detection systems. The proposed model incorporates a hybrid detection framework that utilizes smart contracts and consensus protocols to automate and decentralize the anomaly detection process, thereby increasing system resilience and reducing reliance on single points of failure. The approach also emphasizes secure, real-time traffic monitoring, crucial for promptly identifying and responding to threats in dynamic network environments. These contributions represent a significant advancement in network security, providing a comprehensive solution that improves detection accuracy and enhances overall network integrity and trustworthiness.

3 METHOD

3.1 Definitions and Theorems

The proposed architecture integrates three core modules: a traffic feature extraction module, an intelligent contract-based anomaly detection module, and a consensus mechanism to ensure data integrity, as shown in Figure 1.

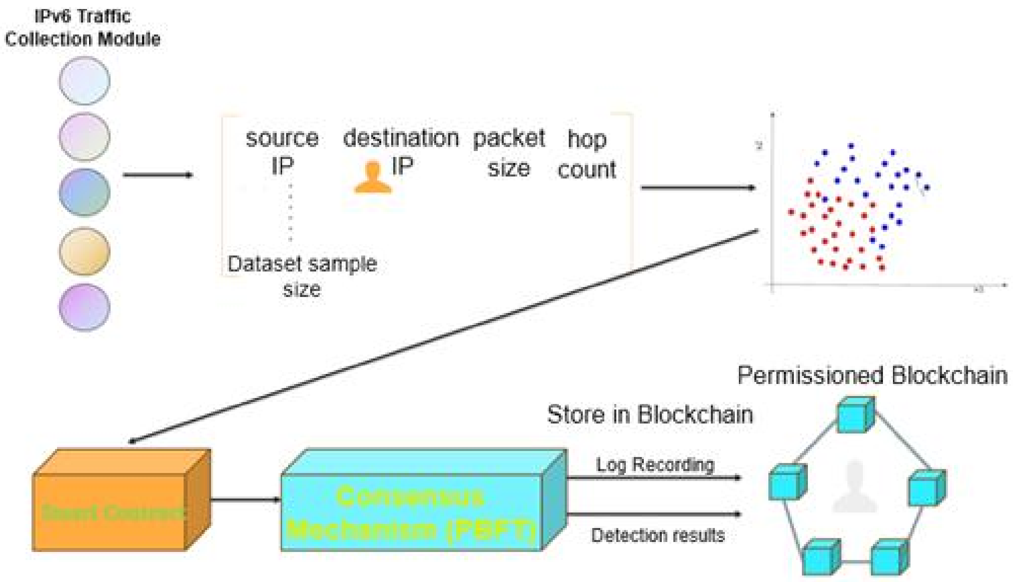

Figure 1 Architecture Overview of Traffic Anomaly Detection System

Traffic Feature Extraction: The extraction module gathers IPv6 traffic data, including source and destination IPs, packet sizes, and hop limits, forming a feature matrix ***X***. A dimensionality reduction technique is applied using PCA to improve computational efficiency:

$$X_{PCA} = W \cdot X \tag{1}$$

Where ***W*** represents the transformation matrix for PCA. This helps reduce the data's dimensionality while maintaining its essential features for further analysis, as shown in Figure 1.

Smart Contract Module: The anomaly detection rules are implemented via smart contracts. An alert is triggered when the sum of feature values exceeds the threshold θ:

$$if \sum(feature\ values) > \theta, then\ Trigger\ Alert \tag{2}$$

3.2 Enhanced Anomaly Detection Algorithm

The proposed algorithm uses a combination of clustering and classification to identify anomalies.
Clustering Analysis: Initial clustering is conducted with a density-based clustering algorithm to define the boundaries of normal traffic clusters. The anomaly degree ϵ for any data point $\boldsymbol{X_a}$ is computed as:

$$\epsilon = \frac{1}{k}\sum_{j=1}^{k} \parallel \mathbf{X}_a - \mathbf{C}_j \parallel \tag{3}$$

Classification Model: We use a Support Vector Machine (SVM) to classify further traffic, refining detection between normal and anomalous patterns. The SVM objective function is:

$$\mathcal{L} = \frac{1}{2} \parallel \mathbf{w} \parallel^2 + C\sum_{i=1}^{n} \xi_i \tag{4}$$

Where ξ_i are slack variables, and C is the regularization parameter.

4 EXPERIMENT

4.1 Experimental Setup

To rigorously evaluate our blockchain-driven anomaly detection model, we created a controlled IPv6 simulation environment that closely replicates realistic network conditions and challenges in modern IPv6 networks. This high-fidelity test setup maintained a data flow rate of 10 Gbps, with packet sizes ranging from 64 to 1500 bytes, emulating the diverse traffic commonly observed in enterprise systems. The simulation included various traffic types, such as HTTP, DNS, and ICMP, to ensure a realistic distribution of network activities. Virtualized nodes within the environment generated attack scenarios like Distributed Denial-of-Service (DDoS), probing, and network scanning attacks, each targeting common IPv6 vulnerabilities to test the model's response under diverse malicious conditions. To further enhance reliability, we used the CICIDS2017 dataset, adapted for IPv6 patterns, which provides a wide range of labeled benign and malicious activities essential for validating anomaly detection accuracy.
To assess the model's performance, we conducted a comparative analysis against three base-line systems: a traditional intrusion detection system (IDS) based on a centralized signature database, a signature-based IDS specifically configured for IPv6 patterns, and a behavior-based IDS that detects deviations using statistical baselines. We evaluated each model using key performance metrics: Detection Accuracy (the rate of correctly identified anomalies), Latency (average time from detection to alert generation, essential for real-time responsiveness), Attack Resilience (system stability and reliability under high-stress attack scenarios), and Data Integrity (ensuring log immutability and tamper resistance). This rigorous testing framework allowed us to capture the strengths and limitations of each model, particularly in handling the unique demands of IPv6 networks.

4.2 Experimental Results

Our blockchain-driven approach showed no-table improvements across all performance metrics, as illustrated in Table 1.

Table 1 Performance Comparison of Anomaly Detection Methods

Method	Accuracy (%)	Latency (ms)	Attack Resilience	Data Integrity
Traditional IDS	83.4	52	Medium	Low
Signature-Based IDS	85.2	49	Low	Medium
Behavior-Based IDS	87.8	47	Medium	Low
Blockchain-Driven (Our Method)	96.2	42	High	High

The results in Table 1 indicate a marked improvement in performance for our block-chain-driven approach over traditional methods. Our model achieved a detection accuracy of 96.2%, surpassing signature-based and behavior-based IDS approaches, scoring 85.2% and 87.8%, respectively. This improvement is attributed to the adaptive nature of the blockchain-based model, which enables learning from network traffic patterns and swiftly responding to novel threats, even those lacking known signatures.
Regarding latency, our method maintained the lowest delay at 42 ms, a significant improvement over traditional IDS systems, which suffered from higher latencies due to centralized processing constraints. The reduction in latency

demonstrates the advantage of the decentralized blockchain model, which distributes processing tasks and mitigates bottlenecks.

4.3 Discussion of Results

Our blockchain-driven model outperformed conventional IDS approaches in detection accuracy and real-time performance. The decentralized ledger system reduces latency and reinforces the reliability and resilience of the anomaly detection process under high-stress conditions like DDoS attacks. These improvements underscore the potential of blockchain integration in anomaly detection for IPv6 networks by:

1) Enhancing Scalability and Fault Tolerance: Unlike traditional IDS systems, our model distributes computational tasks across nodes, eliminating the vulnerabilities of a single-point failure and enhancing system stability during peak traffic loads.

2) Improving Anomaly Detection Through Adaptability: By combining blockchain with machine learning, our system adapts to new traffic patterns and identifies anomalous behavior in real time, outperforming static rule-based systems.

3) Ensuring Robust Data Integrity: The blockchain's immutable nature provides a reliable audit trail, preserving the authenticity and integrity of anomaly detection data, which is indispensable for forensic analysis in post-incident investigations.

5 CONCLUSION

This paper introduced a blockchain-enabled anomaly detection framework that addresses the scalability and security limitations of traditional centralized IPv6 traffic monitoring systems. Our approach leverages tamper-resistant, automated detection through a decentralized ledger and smart contracts, achieving superior detection accuracy and attack resilience.

Integrating blockchain technology enhances the transparency and robustness of IPv6 network defenses against increasingly sophisticated cyber threats. Future work could focus on optimizing the consensus mechanism and exploring the use of machine learning models for enhanced anomaly prediction. Additionally, deploying advanced algorithms in real-world scenarios will further validate the effectiveness and scalability of the proposed approach.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Zhang Y, Kasahara S, Shen Y, et al. Smart Contract-Based Access Control for the Internet of Things. IEEE IoT Journal, 2018, 6(2): 1594-1605.

[2] Lee I, Lee K. Internet of Things (IoT) Security: Threats and Solutions. IEEE Access, 2020, 8: 25786-25805.

[3] Mirkin B. Clustering for Data Mining: A Data Recovery Approach. Chapman and Hall/CRC, 2005.

[4] Chen Y, Zhang Z, Lin Y. Security and Privacy Issues of the Internet of Things: A Survey. IEEE Internet of Things Journal, 2020, 7(4): 2951-2969.

[5] He S, Zhang Y, Yang L. Advanced Anomaly Detection for IPv6 Traffic. IEEE Transactions on Information Forensics and Security, 2021, 16: 2744-2757.

[6] Patel D, Mistry K, Patel P. IPv6 Network Traffic Analysis: A Survey. International Journal of Computer Applications, 2019, 975, 8887.

[7] Krawczyk H, Bellare M. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, 1997.

[8] Yang S, et al. Blockchain-based Network Intrusion Detection System in IPv6 Networks. Journal of Information Security and Applications, 2019, 45: 87-97.

[9] Sharafaldin I, Lashkari A H, Ghor-bani A A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 2018: 108-116.

[10] Zhou H, Xiong Y, Zhang Y. Blockchain-Based Security Management in IoT: A Survey. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1242-1265.