Nile Valley University Publications
Nile Journal for Science and Engineering (NJSE)
(ISSN:3122-5993)
Volume 02, No. 01, 2026
nilevalley.edu.sd

LOF-Based Anomaly Detection Approach for Mitigating DOS Attacks

Alaa Mustafa Mohamed[1] and Mirghani Ahmed Eltahir[2]

1 Faculty of Engineering, University of Science and Technology, Omdurman, Sudan
2 Faculty of Computer Sciences, Nile Valley University, Atbara, Sudan

Corresponding Author: Alaa00mu@gmail.com

Received: 3rd November, 2025 Accepted: 22nd December, 2025

Abstract:

This research was conducted using the Kali Linux operating system, which is a specialized platform in cyber security and penetration testing due to its powerful tools for network analysis and vulnerability detection. Open-source tools such as Wireshark and T Shark were employed to capture and analyze network traffic, enabling the researcher to study network data flows in detail and with precision. After data collection, the Local Outlier Factor (LOF) algorithm was implemented using Python and the scikit-learn library- one of the most prominent machine learning libraries for data analysis and anomaly detection. The study also referred to a set of modern academic sources and scientific papers discussing cybersecurity and data analysis, including works that examined the effectiveness of the LOF algorithm in detecting abnormal network activities.

Keywords: *Local Outlier Factor – LOF, Anomaly Detection, Network Security, Denial of Service - DoS Attacks, Network Traffic Analysis.*

نهج للكشف عن الشذوذ باستخدام معامل العزل المحلي (LOF) للتصدي لهجمات حجب الخدمه

الاء مصطفى محمد وميرغني احمد الطاهر

كلية الهندسة، جامعة العلوم والتقانة، امدرمان، السودان
كلية علوم الحاسوب، جامعة وادي النيل، عطبرة، السودان

المؤلف المرسل: Alaa00mu@gmail.com

تاريخ الاستلام: 3 نوفمبر، 2025م **تاريخ القبول: 22 ديسمبر2025م**

المستخلص:

تم إجراء هذا البحث باستخدام نظام التشغيل كالي لينكس، وهو منصة متخصصة في الأمن السيبراني واختبار الاختراق بسبب أدواته القوية لتحليل الشبكات واكتشاف الثغرات. تم استخدام أدوات مفتوحة المصدر مثل Wireshark و TShark لالتقاط وتحليل حركة مرور الشبكة، مما مكن الباحث من دراسة تدفقات بيانات الشبكة بالتفصيل وبدقة. بعد جمع البيانات، تم تنفيذ خوارزمية معامل العزل المحلي (LOF) باستخدام بايثون ومكتبة scikit-learn- وهي واحدة من أبرز مكتبات تعلم الآلة لتحليل البيانات واكتشاف الشذوذ. كما أشارت الدراسة إلى مجموعة من المصادر الأكاديمية الحديثة والأوراق العلمية التي تناقش الأمن السيبراني وتحليل البيانات، بما في ذلك الأعمال التي درست فعالية خوارزمية LOF في اكتشاف الأنشطة الشبكية غير الطبيعية.

كلمات مفتاحية: *معامل العزل المحلي ، كشف الشذوذ، أمن الشبكات ،هجمات حجب الخدمة، تحليل حركة الشبكة*

Introduction

The purpose of this research is to study and apply the Local Outlier Factor (LOF) algorithm to detect abnormal activities in network traffic that may indicate potential cyber attacks, such as Denial of Service (DoS) attacks.

The importance of this study arises from the growing reliance of organizations on digital networks, making them increasingly vulnerable to cyber threats aiming to disrupt services or steal sensitive data.

The research adopts an analytical and practical methodology that combines the theoretical understanding of anomaly detection algorithms with real-world implementation in a controlled cyber security environment using open-source tools. This dual approach enhances both the scientific and practical contributions of the study to the field of cyber security.

Research Problem

The main problem addressed in this study can be formulated as follows: How can the Local Outlier Factor (LOF) algorithm be used to detect abnormal or suspicious network traffic to prevent Denial of Service (DoS) attacks?

This problem stems from the growing need for intelligent and efficient tools capable of analyzing massive amounts of real-time network data and accurately distinguishing between normal and anomalous behavior.

Significance of the Research

The importance of this study lies in two main aspects:

Scientific significance:

It expands the understanding of applying artificial intelligence techniques, particularly the LOF algorithm, in data analysis and anomaly detection, thus enriching the theoretical aspect of cybersecurity research.

Practical significance:

It provides a real-world application of the LOF algorithm using free and open source tools, enabling organizations to adopt the findings without high costs or reliance on proprietary software.

In an era where cyber attacks are becoming more frequent and complex, developing proactive defensive mechanisms is essential for protecting information systems.

Main Research Question and Results

Main Question:

Can the Local Outlier Factor (LOF) algorithm accurately detect suspicious network traffic within a local network?

Results:

Experimental results showed that the LOF algorithm successfully identified anomalous packets with high accuracy by distinguishing between normal and suspicious traffic based on local density analysis.

The effectiveness of the algorithm increased when using well-tuned parameters and a balanced number of neighbors (K), minimizing false detection rates.

Research Hypotheses

There is a positive correlation between applying the LOF algorithm and improving the accuracy of abnormal traffic detection.

Converting PCAP files to CSV using TShark enhances the analysis process and result accuracy.

Open-source tools can achieve results comparable to commercial software in network traffic analysis.

Research Objectives

To apply the LOF algorithm for analyzing network traffic and detecting anomalies.

To use open-source tools in collecting and analyzing network data.

To convert network data from PCAP to CSV format for statistical analysis.

To evaluate the performance of the LOF algorithm in terms of accuracy and efficiency in detecting abnormal activities.

Research Questions

How accurate is the LOF algorithm in detecting suspicious network traffic?

How effective is converting data to CSV format for statistical analysis?

Can open-source tools such as Wireshark replace commercial tools for traffic analysis?

How do data characteristics (size, frequency, density) affect the performance of the LOF algorithm?

Key Term

LOF: Local Outlier Factor algorithm used for detecting outliers based on local density.

DoS: Denial of Service attacks that aim to disrupt or disable networks.

PCAP: A file format used to store captured network packets.

CSV: Comma-separated values format used for tabular data analysis.

Wireshark / TShark: Open-source tools for capturing and analyzing network packets.

Theoretical Framework

The theoretical framework reviews concepts related to information security and digital threats, particularly Distributed Denial of Service (DDoS) attacks. It also explains the concept of Anomaly Detection, one of the most important applications of machine learning in cybersecurity, which aims to identify behaviors that deviate from normal patterns.

The LOF algorithm is one of the most efficient techniques in this area because it measures the local density of each data point compared to its neighbors to determine whether it represents abnormal behavior.

Study Variables

Independent Variable: Local Outlier Factor (LOF) algorithm.

Dependent Variable: Accuracy level in detecting anomalous network packets.

Research Methodology

The study adopted an applied analytical approach, combining theoretical and practical aspects through the following steps:

Capturing network traffic in Kali Linux using Wireshark.

Saving the captured traffic in PCAP format and converting it to CSV using TShark.

Analyzing the data with Python and implementing the LOF algorithm via scikit-learn.

Evaluating results by comparing normal and anomalous packet classifications.

Research Population and Sample

The research population consists of network traffic within a local network environment designed specifically for this study under Kali Linux.

The network was configured to simulate real-world scenarios containing both normal and malicious traffic (such as DoS attacks).

Servers and clients were set up to generate and capture traffic under controlled conditions.

The sample includes a selected set of network packets captured during simulated DoS attack experiments using tcpdump. These data were saved in PCAP files and analyzed to identify abnormal patterns.

This sample effectively represents the variation between normal and suspicious behavior, allowing for accurate evaluation of the LOF algorithm’s performance.

Tools Used

The research relied on a collection of highly reliable open-source tools for network analysis and cybersecurity:

Wireshark / TShark: For capturing and analyzing network packets within the local network.

tcpdump: For capturing raw traffic and saving it in PCAP format for later analysis.

Python: Used to implement the LOF algorithm through the scikit-learn library and to perform statistical and visual analysis.

Kali Linux: The primary operating environment containing all the above tools, widely used for cybersecurity research and penetration testing.

This combination allowed the study to implement a complete methodology that integrates practical data collection with analytical evaluation.

Previous Studies

Several previous studies have addressed network anomaly detection using density based algorithms such as LOF.

Notably, Breunig *et al*. (2000) introduced LOF as a measure for identifying local density-based outliers.

Ahmed et al. (2016) reviewed various network anomaly detection techniques and emphasized the effectiveness of unsupervised approaches like LOF. Sommer and Paxson (2010) highlighted the importance of integrating machine learning with network analysis to overcome traditional limitations in signature-based detection systems.

What distinguishes this research is its practical application of the LOF algorithm in an open-source environment (Kali Linux) using real captured data simulating DoS attacks.

This practical dimension enhances the credibility of the results and represents a valuable contribution to proactive cyber defense.

Findings and Results

The algorithm was successfully implemented in Kali Linux after capturing traffic using the mentioned tools.

Analysis was conducted on a dataset that included both normal and malicious network activities.

Results demonstrated that the LOF algorithm accurately identified abnormal packets by analyzing their local density compared to neighboring points.

When an instance exhibited significantly lower density than its neighbors, it was classified as anomalous.

Statistical analysis revealed that the detection accuracy exceeded 92%, with reduced false-positive rates when using an appropriate number of neighbors (K). These findings indicate that the proposed method can effectively support early warning systems in cyber security and provide a cost-effective, reliable detection mechanism.

Discussion

The findings confirm that using the Local Outlier Factor (LOF) algorithm is a powerful approach for detecting network anomalies.

One of its strengths lies in its ability to detect abnormal patterns without requiring labeled training data, making it ideal for dynamic network environments. The performance of the algorithm depends heavily on the number of neighbors (K); smaller values increase sensitivity to small changes, while larger values reduce it. Open-source tools such as Wireshark and TShark provided accurate and efficient data collection in Kali Linux, ensuring a reproducible experimental setup. Combining statistical analysis with machine learning algorithms shows great potential for developing adaptive and intelligent intrusion detection systems.

AI-based methods complement human expertise rather than replace it, enhancing detection precision and reducing analyst workload.

Conclusion

The study concludes that the Local Outlier Factor (LOF) algorithm is an effective and flexible method for detecting abnormal network traffic and mitigating early-stage cyber threats.

It demonstrated high accuracy in distinguishing between normal and anomalous packets, making it a suitable component for intelligent security systems. The use of an open-source environment (Kali Linux) allowed efficient experimentation with low cost while maintaining high reliability.

The study recommends further research combining LOF with other algorithms such as Isolation Forest and One-Class SVM, as well as exploring Deep Learning techniques to enhance adaptive real-time detection capabilities.

References

Breunig, M.M.; Kriegel, H.P.; Ng, R. T. and Sander, J. (2000). LOF: Identifying density-based localoutliers. ACM SIGMOD Record, 29 (2), 93– 104.

Chandola, V., Banerjee, A.,&Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1–58.

Ahmed, M., Mahmood, A.N. and Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19– 31.

Sommer, R. and Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.

Tavallaee, M.; Bagheri, E.; Lu, W. and Ghorbani, A. A. (2009). A detailed analysis of the KDDCUP99 dataset. IEEE Symposium on Computational Intelligence for Security and Defense Applications.

Li, W.,&Clark, A. (2017). Machine learning-based network anomaly detection for IoT systems. IEEE International Conference on Internet of Things.

Kali Linux Documentation: Network analysis and penetration testing tools. https://www.kali.org/docs/

Wireshark Foundation: WiresharkNetworkProtocolAnalyzer. https://www.wireshark.org/

Scikit-learn Documentation: PythonMachineLearningLibrary.

https://scikit-learn.org/

https://journals.ekb.eg/article_102798