Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Informatik und Medien

Untersuchung des Potentials von Netzwerkverkehrsanalysemethoden zur automatischen Inventarisierung von Systemen in Krankenhäusern

Veit Kilian Siebert

Masterarbeit • Studiengang Informatik • Fachbereich Informatik und Medien • 19.02.2026

Einleitung

Trotz der Wichtigkeit von Netzwerkinventaren mangelt es an öffentlicher Forschung zu ihrer Automatisierung in der Gesundheitsversorgung. In dieser Arbeit wird ein Proof of Concept für eine Geräteklassifikation in medizinischen Netzwerken über eine Reproduktion der Forschungsarbeit [1] implementiert. Das Proof of Concept wird auf öffentlichen Geräteerkennungs- (DI-) Datensätzen überprüft und auf einem öffentlichen, medizinischen Datensatz sowie einem neuen Datensatz aus einem echten Labornetzwerk angewendet.

Öffentliche Datensätze

Es werden die öffentlichen DI-Datensätze IoTSentinel [2] und UNSW-IoTDevID [1], [3], [4], [5] sowie der harmlose Teil vom medizinischen CICIoMT2024 [6] Angriffsdatensatz verwendet.

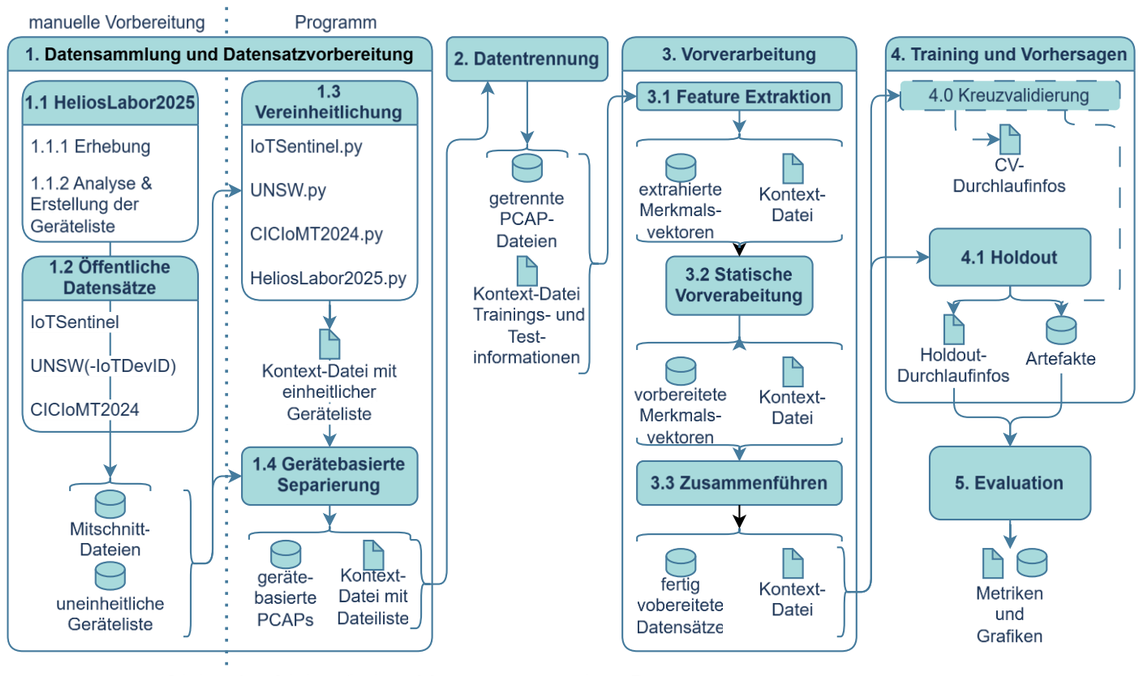

Abb. 1: Ablauf der Umsetzung des Programms

Konzept und Implementierung

Es wird eine paketbasierte Geräteklassifikation auf der Basis von passiv aufgezeichnetem Netzwerkverkehr und überwachtem maschinellem Lernen durchgeführt. Das Proof of Concept verwendet den Ablauf in Abb. 1.
Es wird der neue HeliosLabor2025 Datensatz mit der Helios Kliniken Gruppe erstellt. Dafür wird der über SPAN-Ports gespiegelte Netzwerkverkehr eines Labors aufgezeichnet und analysiert (1.1). Es werden dieser und die öffentlichen Datensätze für die Verarbeitung vorbereitet (1.2-1.4).
Die Mitschnittdateien der Datensätze werden in einen Trainings- und Testteil getrennt (2.). Für die DI-Datensätze wurde die Datentrennung aus [1] reproduziert. Für den CICIoMT2024, HeliosLabor2025 und IoTSentinel Datensatz wurde ein eigenes, stratifiziertes Holdout verwendet.
Im 3. Schritt werden paketbasierte Merkmale nach [1] aus den Mitschnittdateien parallel extrahiert und vorbereitet. In Schritt 4 werden verschiedene Entscheidungsbaum- und Random Forest Modelle (mit Hyperparametern aus [1] und [7]) trainiert und die Vorhersagen erstellt. In Schritt 5 werden übliche Metriken für die Evaluation berechnet. Es werden die Aggregationen der Vorhersagen aus [1] angewendet. Es wird der Macro-Durchschnitt des F1-Scores aufgrund der unausgeglichenen Datensätze verwendet.

Betreuung Prof. Dr. Michael Pilgermann • Dipl.-Inform. Ingo Boersch
• Technische Hochschule Brandenburg

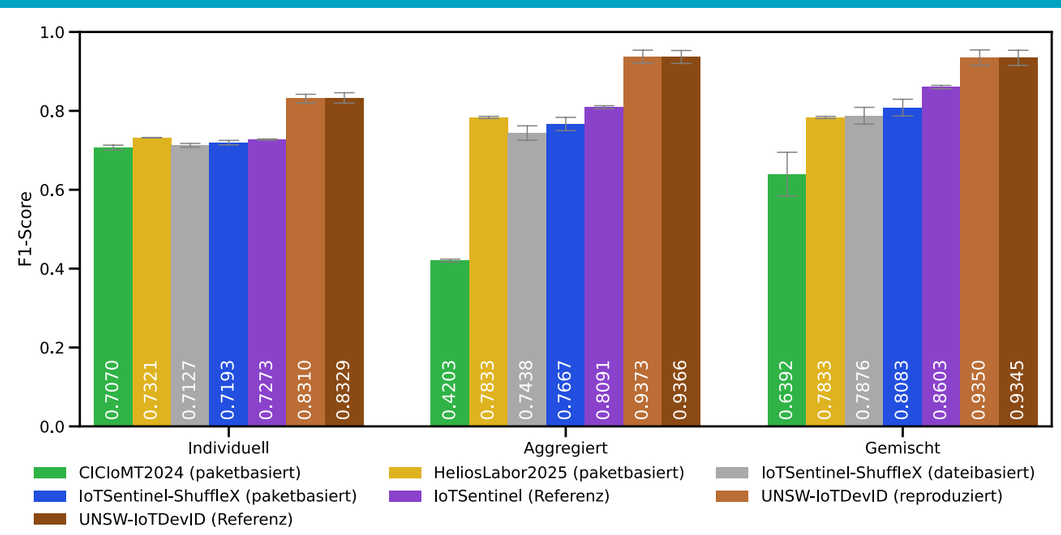

Abb. 2: Ausschnitt der gemessenen, durchschnittlichen Leistungen. Die Referenz-Leistung entstammt dem Online-Repository von [1].

Ergebnisse

Um die Reproduktion zu verifizieren, wird ihre Leistung auf dem IoTSentinel und UNSW-IoTDevID Datensatz mit der originalen Leistung verglichen unter der Nutzung gleicher Modelle. Die Leistungen werden anschließend mit denen der besten Modelle auf den medizinischen Datensätzen verglichen. Ein Teil der Leistungen auf dem Testteil ist in Abb. 2 dargestellt.
Die Reproduktion liefert auf dem IoTSentinel Datensatz schlechtere Ergebnisse. Verantwortlich sind vermutlich in der Arbeit beschriebene Unterschiede in der Reproduktion. Bei dem UNSW-IoTDevID Datensatz ist die Leistung sehr ähnlich.
Die Leistung auf dem CICIoMT2024 Datensatz ist schlechter, wurde aber für die individuellen Vorhersagen als akzeptabel angesehen. Für die schlechtere Leistung sind vermutlich die simulierten Geräte verantwortlich. Die Leistung auf dem HeliosLabor2025 Datensatz ist bei den individuellen Vorhersagen besser als auf dem IoTSentinel Datensatz und bei den Aggregationen schlechter. Dabei wurden einige schlecht erkannte Geräte identifiziert.
Die Reproduktion wird somit als erfolgreich und die Leistung auf den medizinischen Daten als vielversprechend angesehen.

Fazit

In dieser Arbeit wurde gezeigt, dass eine existierende Technik der Geräteerkennung auf einem Netzwerk des Gesundheits-wesens anwendbar ist und ähnlich gute Ergebnisse liefern kann wie in anderen Netzwerken. Die Anwendung zur Unterstützung eines automatischen Inventars ist somit plausibel.

Quellen und Verweise

[1] K. Kostas, M. Just, und M. A. Lones, „IoTDevID: A Behavior-Based Device Identification Method for the IoT“, *IEEE Internet of Things Journal*, Bd. 9, Nr. 23, S. 23741–23749, Dez. 2022, doi: 10.1109/JIOT.2022.3191951.
[2] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, und S. Tarkoma, „IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT“, in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Juni 2017, S. 2177–2184. doi: 10.1109/ICDCS.2017.283.
[3] A. Hamza, H. H. Gharakheili, T. A. Benson, und V. Sivaraman, „Detecting Volumetric Attacks on IoT Devices via SDN-Based Monitoring of MUD Activity“, in *Proceedings of the 2019 ACM Symposium on SDN Research*, in SOSR '19. San Jose CA USA: Association for Computing Machinery, Apr. 2019, S. 36–48. doi: 10.1145/3314148.3314352.
[4] A. Sivanathan *u. a.*, „Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics“, *IEEE Trans. on Mobile Comput.*, Bd. 18, Nr. 8, S. 1745–1759, Aug. 2019, doi: 10.1109/TMC.2018.2866249.
[5] A. Sivanathan *u. a.*, „Characterizing and classifying IoT traffic in smart cities and campuses“, in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Mai 2017, S. 559–564. doi: 10.1109/INFCOMW.2017.8116438.
[6] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, und A. A. Ghorbani, „CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT“, *Internet of Things*, Bd. 28, S. 101351, Dez. 2024, doi: 10.1016/j.iot.2024.101351.
[7] K. Kostas, R. Y. Kostas, M. Just, und M. A. Lones, „GeMID: Generalizable Models for IoT Device Identification“, 2. Juli 2025, *arXiv*: arXiv:2411.14441v2. doi: 10.48550/arXiv.2411.14441.

* Der Inhalt dieses Posters entstammt der Masterarbeit. Die Informationen, Quellen und Abbildungen wurden für dieses Poster zusammengefasst oder angefertigt. Die vollständigen Quellenangaben befinden sich in der Masterarbeit.