## ABSTRACT

The detection of anomalies within network traffic has been a hot topic in the network security research community for the last decades. The immense growth of the internet and the ever-deeper reaching integration in our lives have emphasized the importance of network security. Significant effort has been put into the research of unsupervised anomaly detection due to the ever-changing threat landscape. However, despite the many proposed solutions, they are rarely adopted by the industry.

Network anomaly detection faces many different obstacles, such as lack of representative datasets, high cost of error, and the ever-changing nature of the traffic itself. While the last years have seen a surge of new public available datasets, the question of how to adapt to the dynamic nature of network traffic and security threats is rarely answered. This thesis explores the possible application of a dynamic sketching algorithm, the Robust Random Cut Forest, on current network traffic data. This unsupervised anomaly detection algorithm does not need prior training and can adapt to concept drifts within the data. With the utilization of hyperparameter-optimization, we investigate the detection capabilities in an emulated real-world scenario. The algorithm shows promising detection performance as it was overall capable of distinguishing between anomalies and normal instances and outperformed a comparable static model. However, the long runtimes and many false alarms restrict the application as a standalone solution. To tackle these issues we provide an outlook on possible adaptions where the dynamic anomaly detection capabilities can be utilized in the context of network anomaly detection.

# ZUSAMMENFASSUNG

Die Erkennung von Anomalien im Netzwerkverkehr war in den letzten Jahrzehnten ein heißes Thema in der Forschungsgemeinschaft für Netzwerksicherheit. Das immense Wachstum des Internets und die immer tiefer greifende Integration in unser Leben haben die Bedeutung der Netzwerksicherheit unterstrichen. Aufgrund der sich ständig verändernden Bedrohungslandschaft wurden beträchtliche Anstrengungen in die Forschung zur unbeaufsichtigten Erkennung von Anomalien unternommen. Trotz der vielen Lösungsvorschläge werden sie jedoch nur selten von der Industrie übernommen. Die Erkennung von Netzwerkanomalien stößt auf viele verschiedene Hindernisse, wie z.B. den Mangel an repräsentativen Datensätzen, hohe Fehlerkosten und die sich ständig ändernde Natur des Datenverkehrs selbst. Während in den letzten Jahren eine Flut neuer öffentlich verfügbarer Datensätze zu verzeichnen war, wird die Frage, wie man sich an die dynamische Natur des Netzwerkverkehrs und die Sicherheitsbedrohungen anpassen kann, nur selten beantwortet.
In dieser Arbeit wird die mögliche Anwendung eines dynamischen Skizzenalgorithmus, des Robust Random Cut Forest, auf aktuelle Netzwerkverkehrsdaten untersucht. Dieser Algorithmus zur Erkennung unbeaufsichtigter Anomalien erfordert kein vorheriges Training und kann sich an Konzeptabweichungen innerhalb der Daten anpassen. Mit Hilfe der Hyperparameter-Optimierung untersuchen wir die Erkennungsfähigkeiten in einem emulierten Realwelt-Szenario. Der Algorithmus zeigt eine vielversprechende Erkennungsleistung, da er insgesamt in der Lage war, zwischen Anomalien und normalen Instanzen zu unterscheiden und ein vergleichbares statisches Modell übertraf. Die langen Laufzeiten und viele Fehlalarme schränken jedoch die Anwendung als Standalone-Lösung ein. Für diese Probleme, bieten wir alternative Lösungen an, da wir glauben, dass die intrinsischen Eigenschaften des Algorithmus im Zusammenhang mit der Erkennung von Netzwerkanomalien eine wertvolle Hilfe sein können.