APPLICATION AWARENESS

DEEP PACKET INSPECTION POWERED BY MACHINE LEARNING AND DEEP LEARNING

ENCRYPTED TRAFFIC INTELLIGENCE FOR NETWORK TRAFFIC ANALYSIS

Encryption greatly enhances the security and privacy of data. However, it introduces new challenges in terms of network monitoring and security, as it gives networks only limited visibility into the underlying traffic flows. To reinstate traffic awareness across IP networks, ipoque has enhanced its OEM deep packet inspection (DPI) technology with encrypted traffic intelligence (ETI) for accurate and highly reliable, real-time analysis of encrypted traffic. By leveraging advanced machine learning (ML) and deep learning (DL) techniques and high-dimensional data analysis, ETI complements ipoque's market-leading traffic identification and classification methodologies and metadata extraction to deliver granular visibility for protocols, applications and services that are encrypted.

ML and DL techniques for encrypted traffic intelligence

ETI combines multiple ML algorithms, including k-nearest neighbors (k-NN) and decision tree learning, as well as multiple DL algorithms, including convolutional neural networks (CNN), recurrent neural networks (RNN) and long short-term memory (LSTM) networks, to maximize the accuracy of traffic identification and classification results. With over 1000 features, including statistical, time series and packet-level features, ipoque's ML/DL capabilities boast the ability and the capacity to learn extremely complex patterns and DL automatically identifies the features to be used in such algorithms.

Visibility for encrypted, anonymized and obfuscated traffic

ML and DL techniques combined with the behavioral and statistical/heuristic analysis provided by ipoque's DPI technology deliver fine-grained traffic analysis into not only encrypted traffic but also traffic delivered via VPNs/proxies and traffic obfuscated by randomization, tunneling, domain fronting and mimicry. Insights delivered by ETI enable ipoque's DPI technology to support a wide range of networking solutions such as routers, network packet brokers, policy control engines, IP probes and security tools, including next-gen firewalls, DDoS prevention systems and cloud access security brokers.

DPI engines: R&S®PACE 2 and R&S®vPACE

ETI is incorporated into ipoque's scalar and vector packet processing-based DPI software R&S®PACE 2 and R&S®vPACE. It enables IP traffic awareness in both traditional and cloud computing environments. This way, encrypted traffic visibility is extended for networking and cybersecurity solutions deployed not only as proprietary appliances but also as CNFs and VNFs.

Key characteristics

- Built-in ETI methodologies, without performance and memory penalties
- Over 1000 features, including statistical, time series and packet-level features
- High-dimensional data analysis
- Highly optimized ML algorithms such as k-NN and decision tree models
- State-of-the-art DL algorithms optimized for market-leading classification accurracy and reliability

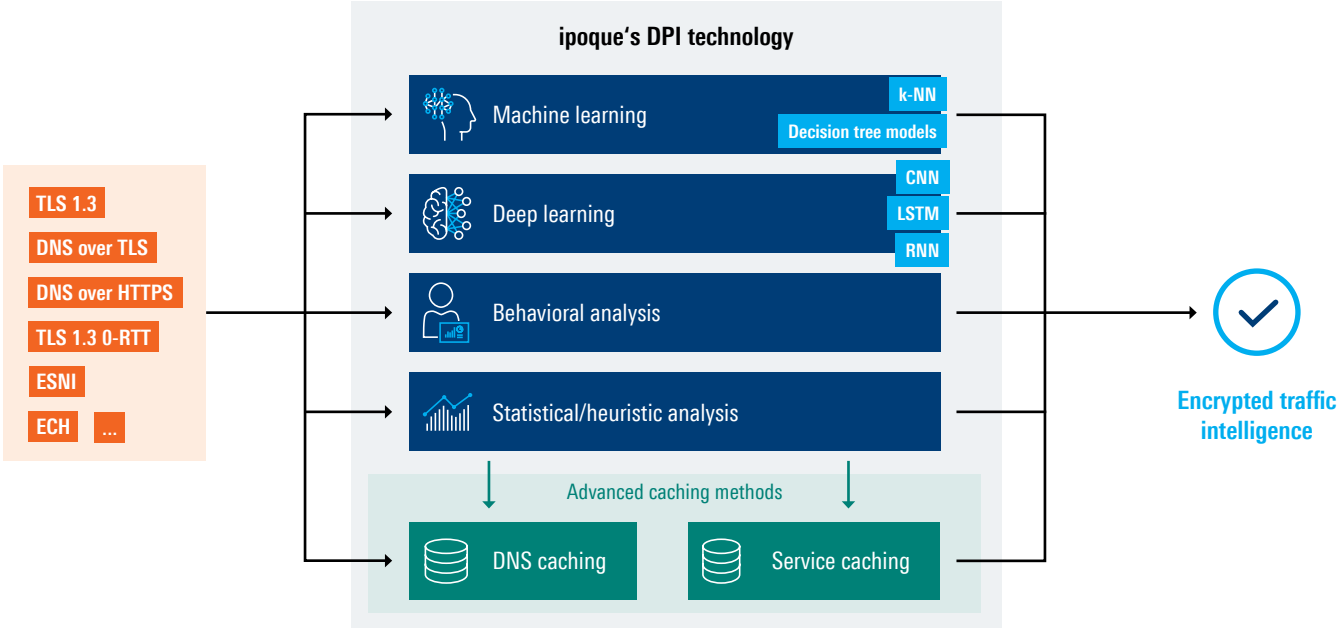
Use cases

ETI is pivotal to many use cases involving encrypted traffic, e.g. OTT video apps such as Netflix or Amazon Prime. Traffic from these platforms is encrypted which limits the visibility of traditional DPI methods to ascertain whether a user is downloading a video or streaming a movie on demand. With ETI, operators can identify the underlying service, allowing them to apply the right policy control and traffic steering rules. They can prioritize video streaming over download packets by delivering the former via priority routes. They can also implement compression for an on-demand stream to avoid content buffering, especially during congestion where speeds are compromised.

This is similar in the case of services from Apple, Google or Meta. Applications by Meta, such as Facebook, Facebook Messenger or Facebook Video, are encrypted over TLS 1.3, making it virtually impossible for network operators to tell these services apart. With ETI, operators can classify each of these applications and their services in real time, allowing the implementation of differentiated policies. For example, video content from Facebook Video that is accessed multiple times may be cached, while packets from a Messenger application can be run through additional filtering to identify security threats hidden in file attachments.

Key benefits

- **Future-proof deep packet inspection**
  ETI caters not only for existing encryption protocols such as TLS 1.3, TLS 1.3 0-RTT, ESNI, ECH, DNS over HTTPs and DNS over TLS but also for newer and more complex protocols that are being released
- **Enables advanced functionalities and services in network functions**
  ETI allows network functions to enrich their existing capabilities, leveraging real-time insights on encrypted applications and services
- **Easily integrated**
  As a software module, the DPI technology can be integrated into any device, in any part of the network from the edge to the core and in any environment, including virtualized and cloud-native networks
- **High performance and reliability**
  Weekly signature updates combined with continuous performance and reliability testing
- **Enables additional monetization streams**
  Real-time traffic visibility enables operators to roll out and enforce new plans and services effectively



ipoque GmbH
A Rohde & Schwarz Company
Augustusplatz 9, 04109 Leipzig
Info: +49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 3683.7454.32 | Version 01.01 | April 2022
Encrypted traffic intelligence for network traffic analysis
Data without tolerance limits is not binding | Subject to change

3683745432

3683.7454.32 01.01 PDP 1 en