Workgroup:	Network Working Group
Internet-Draft:	draft-wu-mten-taxonomy-00
Published:	19 September 2022
Intended Status:	Informational
Expires:	23 March 2023
Authors:	Q. Wu	J. Wu	Q. Ma
---	---	---	---
	Huawei	*Huawei*	*Huawei*

Network Management of Encrypted Traffic: Detect it don't decrypt it

Abstract

Increased use of encryption at the transport, network, or application layer impacts how networks are operated, managed, and secured, especially existing traffic management practices. This position paper analyzes impacts on network management protocols and functionalities,encrypted traffic identification process and a collection of encryption techniques and Internet traffic categorization in the existing traffic management. Encrypted traffic identification processes appear to be hard since Application-layer and transport-layer encryption make the traffic class estimation more complex and less accurate and therefore might be not effective as input information to the queue management. To make network management in support traffic encryption, the various metadata information exchange and storage appears to be useful, especially size and time related data. These data will be more effective to be used in the flow based traffic identification and classification, which can detect the traffic class without decryption. This position paper also discuss the future direction, in order to support modern data driven traffic management at the network layer, more coordination between the management plane and data plane or between application layer and network layer is required to support more fine granularity network control on various different application traffic.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 March 2023.

Copyright Notice

Table of Contents

1. Introduction

Identifying the type of a network flow or a specific application is important for the network performance monitoring, it also helps resolve the network usage issues that impact the security of the applications running on the network. However it becomes more and more difficult in recent years due to widely deployment of encryption and increased usage of VPN and TOR, e.g., more and more internet traffic is encrypted using QUIC, TLS 1.3 and DOT, etc, VPN and TOR are

used to keep user identity anonymous. This poses great challenges for the network traffic monitoring, e.g., identify various different types of network flow within VPN or HTTP connection and extracting statistical features from each traffic flow. In addition, pervasive monitoring was blamed as an attack in [RFC7285] and revisiting the security and privacy properties of our IETF standards had been recommended.

In 2015, IAB joined with GSMA to organize a workshop on "The Managing Radio Networks in an Encrypted World" (MaRNEW). The focus is to manage mobile network under the assumption that much of internet traffic is or will be encrypted, investigate which network management function is impacted, which is not but have to be done differently in more encrypted environment. One important outcome of this IAB workshop is [RFC8404] which discusses pervasive encryption effect on operators and the evolution of mobile networks. Both Encryption in Hosting and Application SP Environments and Encryption for Enterprises has been investigated in [RFC8404].

This documents starts with a few typical encrypted traffic monitoring use cases and example monitoring framework and analyzes impacts on network management protocols and functionalities, encrypted traffic identification process and a collection of encryption techniques and Internet traffic categorization in the existing traffic management. To make network management in support traffic encryption, the various metadata information exchange and storage appears to be useful, especially size and time related data. These data will be more effective to be used in the flow based traffic identification and classification, which can detect the traffic without decryption. This position paper also discuss the future directions.

2. Encrypted Traffic Classification and Identifications Use Cases

In the network traffic monitoring,traffic classification and identifications are used to select packets or flow belonging to a specific application or service in a traffic stream based on the content of the packet header or metadata information of the data packet. Encrypted traffic can be identified gradually based on attributes such as protocols, applications, and services, and finally realize protocol identification, application identification, abnormal traffic identification, and content essence identification. In this section, we provide 3 typical use cases for encrypted traffic classification and identification.

2.1. High Priority traffic QoS guarantee

Alice at the home network is downloading a video file from youtube website in the meanwhile, she receives a call on Wechat application. The most of bandwidth is used for file transfer application which incur delay for the call on Wechat application. When more and more bandwidth is consumed by file transfer application, the call is unable to continue. To provide QoS guarantee for the call application, the management system needs to detect the call traffic within other network traffic, and prioritize the call traffic over other traffic.

2.2. Malware traffic detection

TLS based Encryption enhances the privacy of end users using IoT Devices. In the meanwhile, malware authors also can use TLS based encryption to escape network based analysis. A malicious IoT device might use DOH to avoid detection by malware DNS filtering service or uses privacy enhancing technologies such as Tor or evasion techniques such as client hello randomization. To detect malware running on the IoT devices, TLS profile [I-D.ietf-opsawg-mud-tls] can be created to check any discrepancies in the TLS message sent from the IoT device in comparison with legitimate flow.

2.3. Traffic Flow Billing

Mobile services are playing an increasingly important role in our daily lives. The mobile data consumption per subscriber has grown rapidly with the increasing use of 4G and 5G technologies. We see more and more mobile users want to subscribe additional mobile data service. The operators can offer on demand mobile data service to subscribers and distinguish data service traffic from other network traffic. Bandwidth on data service traffic is charged on a Pay As You Go basis, and it is calculated on the actual bandwidth usage (GB) in your last month multiplied by bandwidth charges rate per month.

3. Issues with Encrypted Traffic Management

3.1. New Emerging Encryption Protocols Identification

With the emergence and popularization of new encryption protocols, such as the TLS1.3 protocol, only a few fields in the data packet are not encrypted, and the certificate and domain name information will be encrypted. During the TLS1.3 handshake, the encrypted traffic identification algorithm for some plaintext fields will fail.

3.2. User Privacy Exposure in the Measurement Protocol

When the client uses encryption to protect the sensitive information from disclosure to the malicious attacker and enhance the user privacy, during the communication between the client and server, the client can also take measurement of data with individual identity information from the end system and share them with the server which might be misused by the server and represent a threat to the user privacy.

3.3. The impact of Encryption on network QoS management

QoS classification refers to the process of classifying the type of IP packets or traffic. When VPN software or TOR software is used to encrypt whole IP packets, QoS classification component in the traffic management has no way of knowing what kind of packet was inside the tunnel, therefore it only classifies according to the outer header. Suppose the DSCP field in the inner packet is copied into the outer header, there is potential risk to violate privacy issue.

3.4. The Impact of Encryption on Network Access Control Management

Enabling controlling access to encrypted traffic, data and networks,resource using predetermined or customized permissions based on the user's role, identity attributes or risk factors improves security and flexibility but also imposes challenges to traditional network access management, which is usually controlled through a combination of mechanisms such as maintaining separate static VLAN/IP subnet assignments per organization, applying Access Control Lists (ACLs) on VLANs and/or IP subnets. IP address-based policies (such as forwarding, routing, QoS and security policies) may not be sufficient enough to accommodate users in motion. If a web transaction is performed over encrypted HTTPS (typically port 443), the URL filtering policy inspects the Server Name Indication (SNI) field within the TLS Client Hello handshake. And then the firewall can be configured to lookup and enforce policy, when TLS Encrypted Client Hello [I-D.draft-ietf-tls-esni] is applied, the URL filtering policy will fail for Encrypted HTTPS web transactions.

3.5. The Impact of Encryption Flow Traffic Collection and Analyzer

IPFIX enables generation of exhaustive flow data based on subnet, IP address, port number, or any number of other network traffic attributes which can be exploited for detecting abnormal in network behavior ('anomaly detection'). IPFIX flow records also provide various performance statistics associated with IP traffic, such as RTT (Round Trip Time), Delay, Jitter, Sequence of Packet Lengths and Times, packet data from the first packet of a flow such as HTTP URL, DNS hostname/address. When TLS Encrypted Client Hello [I-D.draft-ietf-tls-esni] is applied, acquiring unencrypted metadata such as cipher suites, TLS versions, and the client's public key length become a challenge.

3.6. Multiple Flow based Traffic Identification

When multiple flows are carried in the same connection, e.g., VPN or QUIC, it became difficult to identify various different types of a network flow within VPN or HTTP connection and extract statistical features from each traffic flow since these flows might share the same context information, e.g., originating from the same source IP address within a 5 minute window.

3.7. Distinguishing Malware traffic from Legitimate Traffic

Encryption is an important means of protecting privacy, protecting our data from prying eyes and preventing criminals from stealing our credit card information, app usage habits or passwords. On the other hand, encryption is a double-edged sword that protects privacy while also giving criminals an opportunity. Encryption hides malware like other information, leading to a range of worms (as well as Trojans and viruses). When more and more encryption techniques are used, it became a big challenge to distinguish malware traffic from legitimate traffic or anomaly traffic.

3.8. Encrypted Traffic Tagging

Most of the work on encrypted traffic monitoring now focuses on supervised machine learning, which requires a lot of labeled data during training. However, since privacy protection and traffic tagging tools such as deep packet analysis tools cannot handle encrypted traffic, it is difficult to legally collect and accurately label encrypted traffic datasets in a short time and at low cost. This situation get even worse when lacking tools to automatically extract and select features.

3.9. Encrypted Traffic Distribution

In the real network environment, when encrypted traffic is categorized into several classes, each class might have different number of sample data. Class imbalance is also an important problem in encrypted traffic classification, which will directly affect the classification accuracy. This situation can be aggravated when features in the sampled data prone to failure.

4. Encrypted Traffic Measurement Framework

In this section, we provide an overview of the whole Measurement System. The main components of a Measurement System are Measurement agent, collector, Data Analysis tool, Controller.

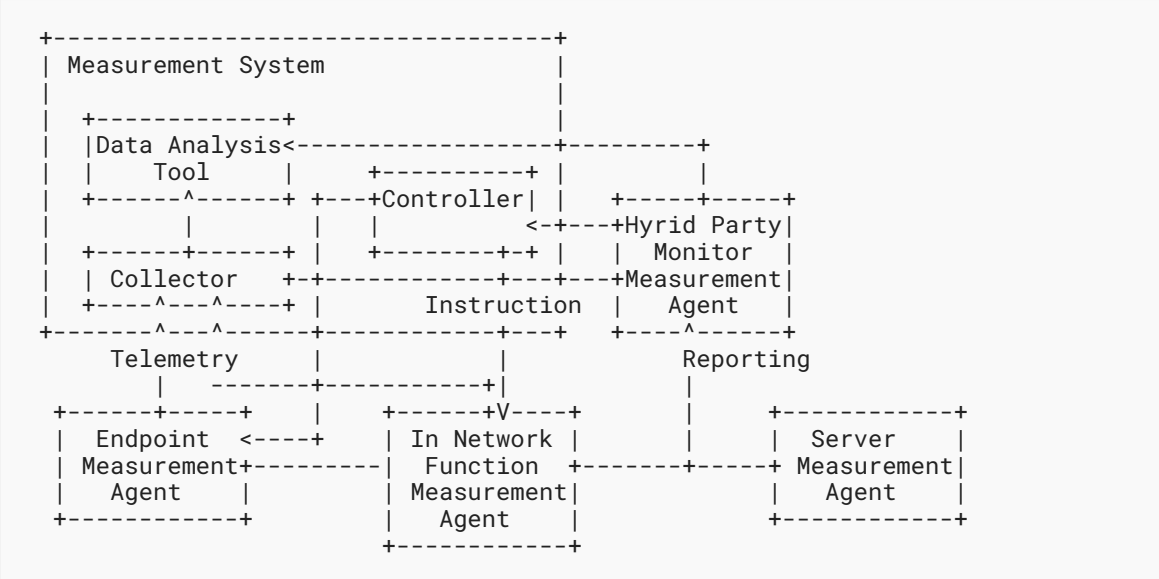
The measurement agent performs measurement tasks and extract statistical features from encrypted traffic flow. The management agent can be collocated with the traffic management functionalities such as traffic classifier, traffic marking, traffic shaping, queue management. The end system that runs an application program that sends or receives data traffic, an intermediate system that forwards data packets to end devices, or a third party that observes the data traffic but does not make itself visible to the Session participants can play the role of the measurement agent within the Encrypted traffic monitoring framework. The MAs are pieces of code that can be executed in specialized hardware (hardware probe) or on a general-purpose device (like a PC or mobile phone).

The Controller manages an Measurement agent through use of the Control Protocol, which transfers the Instruction to the measurement agent. This instruction describes the Measurement Tasks the Measurement agent should perform and when. For example the Controller may instruct an Measurement Agent at a Edge gateway: "Count the number of bytes that the server sent".

The Collector accepts a Report from a Measurement Agent with the Measurement results or Measurement metadata information from its Measurement Tasks. It then provides the Results to a data analysis tool.

The data analysis tool is responsible for the process of feature selection, to eliminate irrelevant feature and then use deep learning, supervised learning, unsupervised learning to identify the flow category and the application in use. In addition, Data analysis tool may interact with controller to adjust resource allocation or enforce security policy on the network devices.

The data analysis tool can be collocated with measurement agent in the same device which classify the traffic flow and provides on path traffic management if needed.



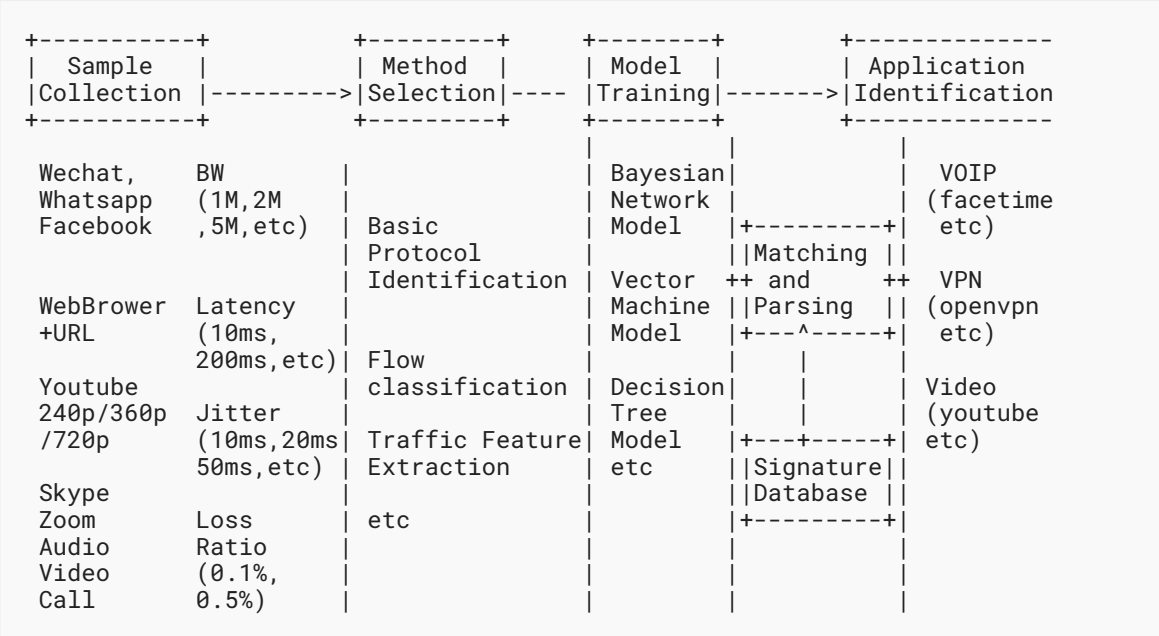
4.1. Measurement Point Placement

There are several possible locations from which encrypted network traffic can be monitored. These include end systems that terminate sessions, intermediate systems that are an active part of a session, and third-party devices that passively monitor a session.

The performance metrics collected by Measurement Agent can be divided into end-system metrics, application-level metrics, and transport-level metrics. Some of these metrics may be specific to the measurement point or may depend on where the measurement agent are located in the network, while others are more general and can be collected in any monitoring location.

The measurement agent can also collect metadata information from encrypted network traffic. The metadata information can be captured from packet header, e.g., the sequence of packet lengths and inter- arrival times, it also can be captured from the outsider of the packet, e.g., inter-arrival time, throughput and burst times.

4.2. Work flow of Encrypted Traffic Classification and Identification



Through the analysis of live network data monitoring, it is found that different service flows have some traffic statistics and protocol context information in common, some encrypted application (for example, VoIP application) has some of the typical characteristics, for example:

- The packet size is somewhat constant;
- The packet size would fall into a specific range;
- The inter packet arrival time is somewhat constant;

For application identification, the sample data should be collected and fed into hardware acceleration component , the hardware acceleration component selects appropriate traffic identification methods such as basic protocol identification, flow characteristics extraction, traffic feature identification (e.g., packet length, transmission direction) for feature construction and select appropriate model training methods such as Bayesian network model to create and update Statistical feature identification signature database. Based on the base signature database, the pattern matching and parsing task can be performed to identify applications.

4.3. Encryption Technique Classification

In the encryption environment, various different encryption techniques can be used to offer a secure connection over the internet. These techniques can be classified into three main categories:

- VPN encryption
- TOR encryption

- Non-VPN encryption

4.3.1. VPN Encryption

VPN encryption protocol outlines how a VPN will create a secure tunnel between your device and the target server. VPN providers use different encryption protocols to secure the network connection and data traffic. The VPN encryption protocols vary in speeds, security standards, mobility, and general performance. Here are some of the most commonly used VPN encryption protocols in the industry:

- IKEv2/IPSec: Secure, stable, and very fast;
- OpenVPN: Best-in-class. Very secure, stable, and fairly fast;
- WireGuard: is a recent addition to the VPN industry, and it offers a good balance of security, reliability, and fast speeds;
- SoftEther: is a recent addition to the VPN industry and is considered secure, stable, fast;

[RFC4301] provide a security architecture at IP layer through the use of a combination of cryptographic and protocol security mechanisms:

- Security Protocols -- Authentication Header (AH) [RFC4302] and Encapsulating Security Payload (ESP) [RFC4303];
- Security Associations -- what they are and how they work, how they are managed, associated processing ;
- Key Management -- manual and automated (The Internet Key Exchange (IKE)) [RFC4306];
- Cryptographic algorithms for authentication and encryption [RFC4305][RFC4307];

[RFC4303] introduce Traffic Flow confidential capability which can be used to obscure the size and frequency of IP traffic using a fixed-sized, constant-send-rate IPsec tunnel. [I-D.ietf-ipsecme-iptfs] addresses one major limitation (i.e.,under-utilize the available bandwidth) in [RFC4303] and enhances IPsec traffic flow security (IP-TFS) by adding Traffic Flow Confidentiality capability to encrypted IP encapsulated traffic. Both [RFC4303] and [I-D.ietf-ipsecme-iptfs] conceal the characteristics of specific, individual subscriber traffic flows.

4.3.2. TOR Encryption

Similar to VPN encryption, Tor aims to conceal its users' identities and their online activity from surveillance and traffic analysis by separating identification and routing. It is an implementation of onion routing, which encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe Internet. These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in a network location. ESP may be employed as part of a higher-layer traffic flow confidential system, i.e., Onion Routing.

4.3.3. Non VPN encryption

Non VPN traffic is a regular network traffic without VPN support or TOR support. Non VPN encryption techniques can be further broken down into the following categories.

4.3.3.1. DNS + TLS 1.2

Use normal DNS to look up domain name and use TLS 1.2 to provide secure communication between the client and the server.

4.3.3.2. DNS + TLS 1.3

Use normal DNS to look up domain name and use TLS 1.3 to provide communication between the client and the server.

4.3.3.3. DNS + QUIC

Use normal DNS to look up domain name and use QUIC as encryption protocol to provide secure communication between the client and the server.

4.3.3.4. DOH + TLS 1.2

Secure Web using DOH and use TLS 1.2 to provide secure communication between the client and the server.

4.3.3.5. DOH + TLS 1.3

Secure Web using DOH and use TLS 1.3 to provide secure communication between the client and the server.

4.3.3.6. DOH + TLS 1.3 +ECH

Secure Web using DOH and use TLS 1.3+ECH to provide privacy preservation communication between the client and the server.

4.4. Internet Traffic Categorization

4.4.1. Encrypted traffic vs Unencrypted Traffic

Identify which traffic is encrypted, which is not.

4.4.2. Protocol Identification

Identify the encryption protocols or technques such as TLS, SSH,IPSEC,etc.

4.4.3. Application classification

Internet traffic can be characterized into the following categories such as VoIP, File Transfer, Video, Gaming etc.

4.4.4. Class of Service Identification

Identify the type of service to which encrypted traffic belongs, e.g. web browning, streaming media), instant messaging and cloud storage.

4.4.5. Malicious Traffic Identification

Malicious traffic identification is to identify DDoS, APT, Malicious traffic such as Botnet.

4.4.6. Web Page Recognition

Web page recognition is to identify web browsers under the HTTPS protocol such as Google, Amazon or Bank.

4.4.7. Classification based on Traffic Flow per Connection

The Internet traffic can be classified into two categories based on traffic flow per connection,

- Single flow per connection: The communication between the client and the server supports multiple connections with each one carrying a single flow.
- multiple flows per connection: The communication between the client and the server supports a single connection with multiple flows included.

4.5. Metadata information Categorization

Metadata is defined as the data providing information about one or more aspects of encrypted internet traffic. Metadata information can be either captured from packet header and payload, or from the outside of the data packet. Metadata can be captured from the host or captured from the network. The Metadata information can be static statistics data or dynamic statistics data.

4.5.1. Host based Data Feature

Host based Data Feature is metadata information captured from the end system. The Host based Data feature include but is not limited to :

- Process Name;
- OS Name;
- OS Edition;
- OS Version;
- Hash of the process;
- The number of the ports;

Corrleating metadata information from the host with other traffic flow metadata information can be used to identify specific device types, e.g., IoT device type which support specific operating system.

4.5.2. Network based Data Feature

4.5.2.1. Static Flow Characteristics

4.5.2.1.1. On Path Information

On Path information is metadata information captured from the packet header. On Path information includes but is not limited to 5 Tuples

- Physical input interface
- Source and destination MAC address

- Class of Service (CoS) IP Precedence value
- Differentiated Services Code Point (DSCP) values
- Source and destination IP address
- Protocol type
- Application type

4.5.2.1.2. Off Path Information

Off Path information is metadata information captured from the outside of the packet header or payload data. The off path information includes but is not limited to

- Flow start time
- Flow End time

4.5.2.2. Dynamic Flow Characteristics

4.5.2.2.1. On Path Information

The on path information include but is not limited to:

- packet size value
- flow control window setting
- protocol flag
- IPid value

4.5.2.2.2. Off Path Information

The off path information includes but is not limited to:

- Packet event times
- Packet inter-arrival time
- Inter-burst times
- Bytes per packet
- Cumulative Bytes per packet
- Bytes per burst
- Periodical Throughput samples

4.5.2.3. Packet Level Charateristics

The packet level mainly focuses on the characteristics and arrival process of data packets. Packet-level features mainly include packet size distribution, packet arrival time distribution, etc.

4.5.2.4. Session Level Charateristics

The session level mainly focuses on the characteristics and arrival process of the session, such as The amount of data requested by the video is large, and a request will be divided into multiple Session transfer, session-level features including session bytes and session persistence time etc.

4.5.3. Protocol specific Data Feature

4.5.3.1. TLS Data

4.5.3.1.1. Client based TLS specific features

Client based TLS specific features include but are not limited to:

- The list of offered ciphersuites;
- The list of advertised extensions;
- and the client's public key length;

4.5.3.1.2. Server based TLS specific features

Server based TLS specific features include but are not limited to:

- The selected ciphersuite, supported extensions;
- The number of certificates;
- The number of subject alternative names;
- The validity in days
- Whether there was a self-signed certificate.

4.5.3.2. DNS Data

DNS data includes but is not limited to:

- The lengths of both the domain name and the FQDN;
- Most common suffixes;
- The common TTL values;
- The number of numerical characters;
- The number of non-alphanumeric characters;
- The number of IP addresses returned by the DNS response;

4.5.3.3. HTTP Data

HTTP data includes but is not limited to:

- the presence of outbound and inbound HTTP fields;
- Content-Type;
- User-Agent;
- Accept Language;
- Server;
- and code.
- URL.

4.5.3.4. QUIC Data

QUIC data [I-D.ietf-quic-manageability] includes but is not limited to:

- Spin bit for passive measurement;
- Negotiated version;
- SNI;
- Destination Connection ID;

4.5.3.5. IPSEC Data

IPSEC Data includes 2-tuples (Source address, Destination address) in the tunnel mode and 5-tuples in the transport mode [RFC8404].

4.5.3.6. IPFIX Flow Data

IPFIX Flow Data includes Sequence of Packet Lengths and Times (i.e.,the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the inter-arrival times of those packets), packet data from the first packet of a flow such as HTTP URL, DNS hostname/address and TLS specific features such as cipher suites, TLS versions, and the client's public key length.

4.6. Encrypted Traffic Management Methodologies

4.6.1. Detect after Decryption

Payload based traffic classification methods, also referred as deep packet inspection (DPI), need to capture metadata information from packet payload. These methods are computation expensive and are not able of tackling most of today's traffic that uses encryption. What is more, they are problematic since they don't respect the user privacy.

4.6.2. Detect, don't decrypt

4.6.2.1. Port based Methods

Port based methods are based on packet headers fields values. The most commonly used packet header fields value is the TCP/UDP port number. Port based methods are fast and simple, were widely used before, but with the increased use of dynamic ports and default ports, these methods fall short in their efficiency.

4.6.2.2. Statistics based Traffic Identification and Classification

Statistics based methods also referred as fingerprint based methods (See section 2.1.3 of [RFC8404]), are based on size and time related features.They can be used to identify applications, provide insight into network traffic, and detect malicious activity. To realize this, they manually extracting them and applying complex patterns or supervised learning algorithms as classifiers.

4.6.2.3. Multiple Flows Correlation

Multiple flows correlation methods are applied to one single connection having multiple flows. These methods are based on common features such as protocol class, IP address, port, time, etc and They can be used to identify the relation between these flows.

4.6.2.4. Event and Flow Correlation

Event and flow correlation methods [EFC] are based on common features such as protocol class, IP address, port, time, event,etc and They can be used to identify the relation between these flows.

4.6.3. Active Collaboration between endpoints and the network

During flow analysis, threat detection and performance monitoring, when TLS 1.3 and TLS Encrypted Client Hello [I-D.draft-ietf-tls-esni] are applied to provide full encryption at the TLS layer, the collaboration between endpoints and the network is encouraged to establish trust relationship with the monitoring party (i.e., in network functionality) in the network and enhance user privacy by providing less information to two ends. Two collaboration schemes can be allowed:

- Collaboration between the host and the proxy in the network; The proxy needs to be configured and authorized by the host or UE;
- Collaboration between the proxy in the network and the server; The server needs to generate session key and distributed to the proxy in the secure channel.

4.6.4. Active Measurement

The active detection method [RFC7799] obtains the response by sending requests to the target device and extracts the features for traffic identification by analyzing the content of the response. This method can also be used for device identification.

4.6.5. Passive Measurement

Unlike the active detection, the passive method [RFC7799] extracts features by analyzing the daily traffic generated by the device.

4.7. Future Directions

With the increased deployment of traffic encryption and obfuscation methods, the technologies for classification and identification of encrypted traffic have gradually evolved, which are mainly divided into port-based, payload-based and flow-based methods.

Port-based classification methods infer the type of service or application by assuming that most applications use the default TCP or UDP port number. However, methods such as port masquerading, port randomization, and tunneling make this method ineffective quickly. The payload-based method, Deep Packet Inspection (DPI) technology, needs to match the packet content and cannot handle encrypted traffic. Flow-based methods usually rely on statistical features or time series features, and use machine learning algorithms such as support vector machines, decision trees, random forests and other algorithms for modeling and identification.

Although machine learning methods can solve many problems that cannot be solved by port- and payload-based methods, there are still some limitations: a. It is impossible to automatically extract and select features, and it needs to rely on the experience of domain experts, resulting in the application of machine learning to encrypted traffic, there is a lot of uncertainty in classification; b. Features are prone to failure and need to be updated continuously.

The author believes that too much of the current technology is network centric, i.e., the data needing to accommodate the network in specific standards or formats, data driven approach will be more beneficial, i.e., the network needs to accommodate the data. The Artificial intelligence functions can be placed in the location that is more suitable for them, e.g., introduce AI function not only in the Cloud Platform, SDN controller, but also in the Edge computing device and in network function. The hierarchical and distributed network management architecture can be built to support AI function and computing function at each level. Since encrypted traffic is not visible or completely hide from intermediate nodes, more coordination between endpoint device and Edge Device or between Edge Device and Cloud Platform is required to initiate active measurement [RFC7799] and address the challenges in the existing passive measurement methods and technologies. The network management will switch from network management automation to autonomous networking or intelligent network management. Here are several aspects in the following we need to consider for the future directions:

- New measurement protocol : Define protocol, data formats and information models for the storage and exchange of the results of measurements or meata data information of measurements to support new network management requirements such as privacy preservation, observability, self management. The Privacy Preservation Measurement protocol [I-D.ietf-ppm-dap] and IPFIX [RFC7011] are two examples of such measurement protocol.
- New Metrics and models: Develop new metrics and models to accurately characterize the network paths under test and/or the performance of transport and application layer protocols on these paths. These metrics are not necessary directly measured or calculated. Cumulative metrics or sampled metrics or application level metrics can be used to reflect the performance of transport and application layer protocols through specific network path.
- New Bechmark Methodology: Benchmarks for live, operational networks with encrypted traffic support. Describe the class of network function, system, or service being addressed; Discuss the performance characteristics that are pertinent to that class; Clearly identify a set of metrics that aid in the description of those characteristics; Specify the methodologies required to collect said metrics;
- New algorithms and Schemes: New algorithms for modeling and identification based on selected features, e.g., Identification based on data packet size distribution or host based application behavior or machine learning algorithms. Introduce new collaborbation scheme to allow more coordination between the endpoint and in network functionality.
- New network management function: It requires adoption of encryption for the management functions,integration security functionality with QoS management functionality, access control functionality. The intelligence can be built into network device and the management system e.g., using AI driven telemetry and constitute a new network management architecture and provide data-correlation and filtering on both network device and the

management system and support more sophisticated reasoning based on meatadata and identification.

5. Informative References

[EFC] Spacek, S., Velan, P., Celeda, P., "HTTPS Event-Flow Correlation: Improving Situational Awareness in Encrypted Web Traffic", June 2022.

[I-D.ietf-opsawg-mud-tls] Reddy, T., Wing, D., and B. Anderson, "Manufacturer Usage Description (MUD) (D)TLS Profiles for IoT Devices", Work in Progress, Internet-Draft, draft-ietf-opsawg-mud-tls-07, 26 August 2022, <https://www.ietf.org/archive/id/draft-ietf-opsawg-mud-tls-07.txt>.

[I-D.ietf-ppm-dap] Geoghegan, T., Patton, C., Rescorla, E., and C. A. Wood, "Distributed Aggregation Protocol for Privacy Preserving Measurement", Work in Progress, Internet-Draft, draft-ietf-ppm-dap-01, 11 July 2022, <https://www.ietf.org/archive/id/draft-ietf-ppm-dap-01.txt>.

[I-D.ietf-quic-manageability] Kuehlewind, M. and B. Trammell, "Manageability of the QUIC Transport Protocol", Work in Progress, Internet-Draft, draft-ietf-quic-manageability-18, 15 July 2022, <https://www.ietf.org/archive/id/draft-ietf-quic-manageability-18.txt>.

[I-D.ietf-tls-esni] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-14, 13 February 2022, <https://www.ietf.org/archive/id/draft-ietf-tls-esni-14.txt>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC4305] Eastlake 3rd, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, DOI 10.17487/RFC4305, December 2005, <https://www.rfc-editor.org/info/rfc4305>.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, DOI 10.17487/RFC4306, December 2005, <https://www.rfc-editor.org/info/rfc4306>.

[RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, DOI 10.17487/RFC4307, December 2005, <https://www.rfc-editor.org/info/rfc4307>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[RFC8404] Moriarty, K., Ed. and A. Morton, Ed., "Effects of Pervasive Encryption on Operators", RFC 8404, DOI 10.17487/RFC8404, July 2018, <https://www.rfc-editor.org/info/rfc8404>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

Authors' Addresses

Qin Wu
Huawei
101 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China
Email: bill.wu@huawei.com

Jun Wu
Huawei
101 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China
Email: junwu.wu@huawei.com

Qiufang Ma
Huawei
101 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China
Email: maqiufang1@huawei.com