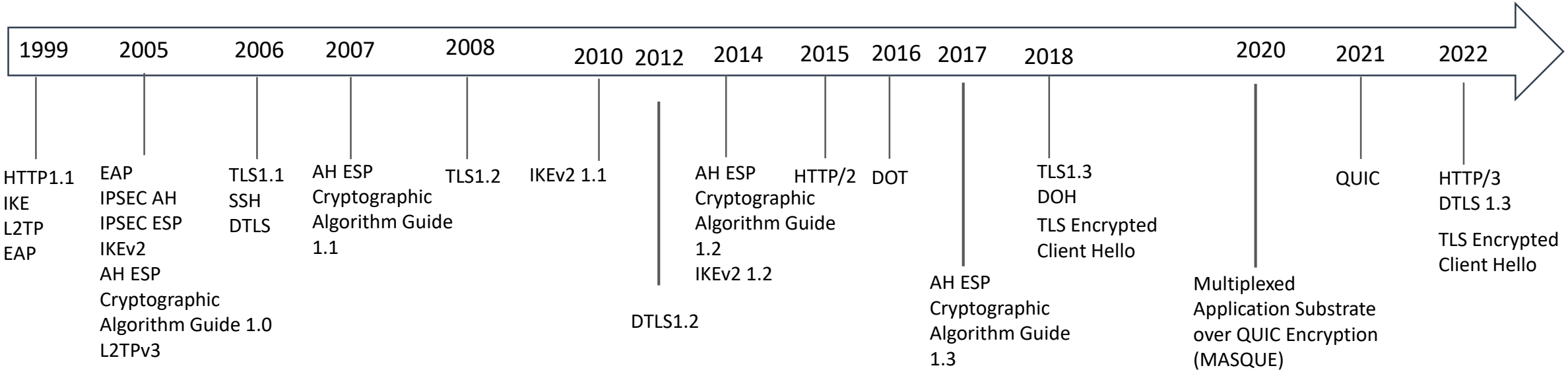
Network Management of Encrypted Traffic: Detect it don't decrypt it

draft-wu-mten-taxonomy-00

IAB M-TEN Workshop (virtual) 10/17/2022

Qin Wu, Jun Wu, Qiufang Ma

Some Context

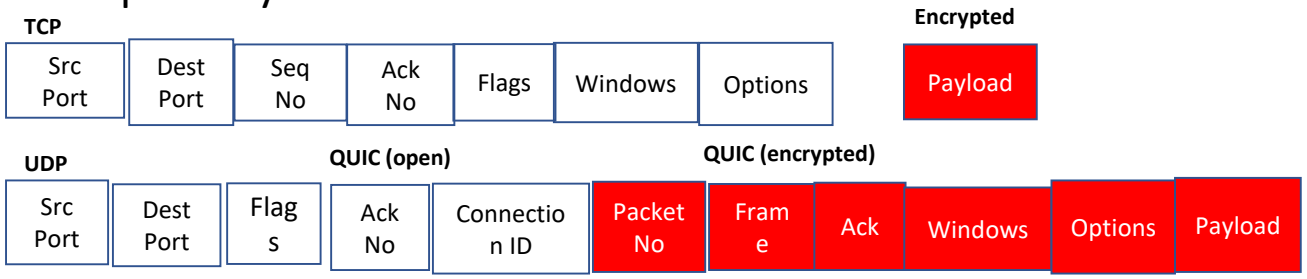


MACSEC

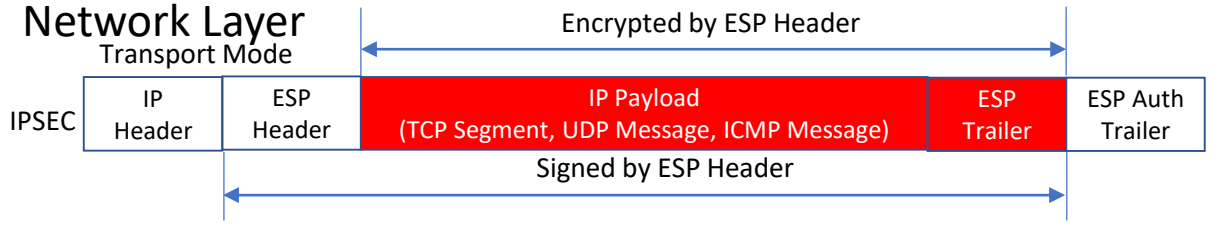
IEEE Std 802.1AE 2006
IEEE Std 802.1AEbn-2011
GCM-AES-256 Cipher Suite
IEEE Std 802.1AEbw-2013
extended packet numbering Cipher Suites
IEEE-Std 802.1AEcg-2017
Ethernet Data Encryption devices (EDEs)
transmission using multiple secure
channels (SCs)
IEEE Std 802.1AE-2018

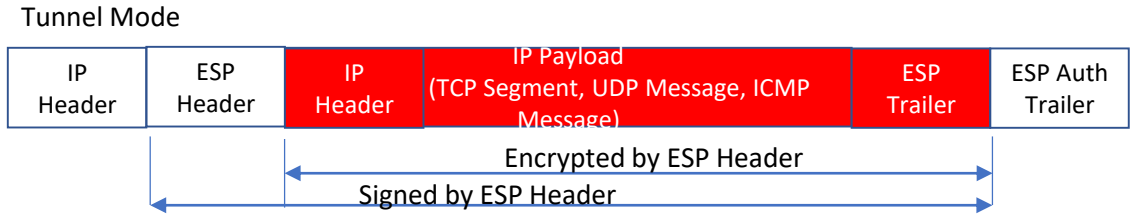
Traffic Encryption at network, transport, or application layer

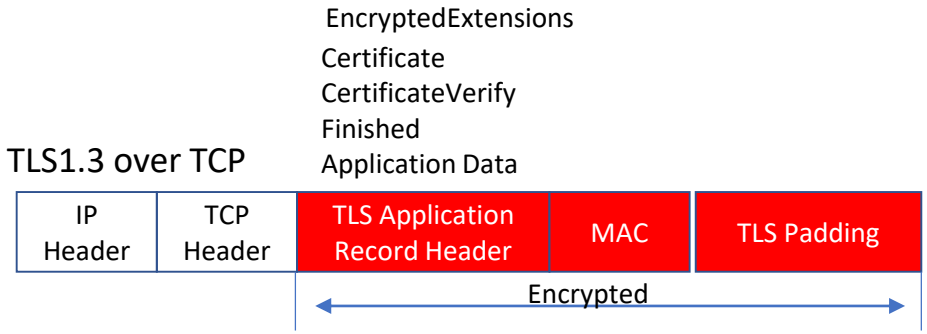
Transport Layer

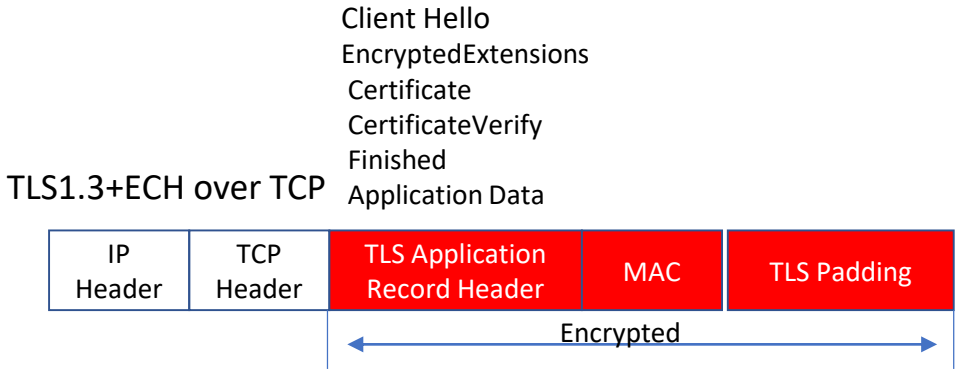


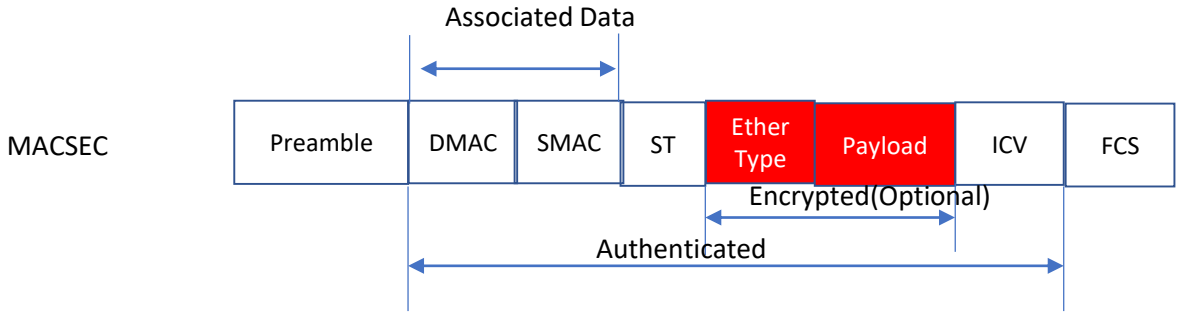
Network Layer



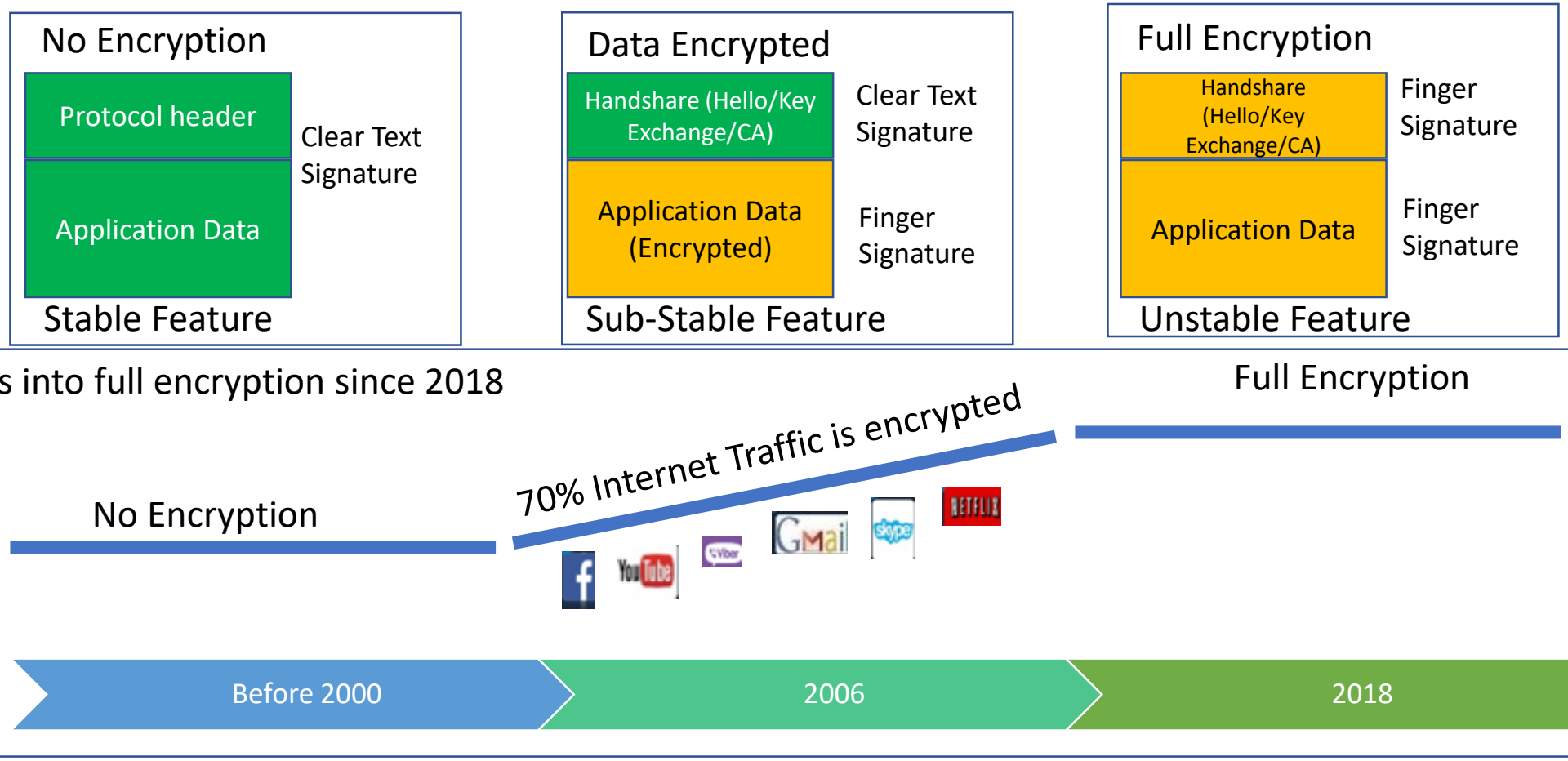








Traffic Encryption Is The Trend of Future Internet



Traffic Encryption at network, transport, or application layer

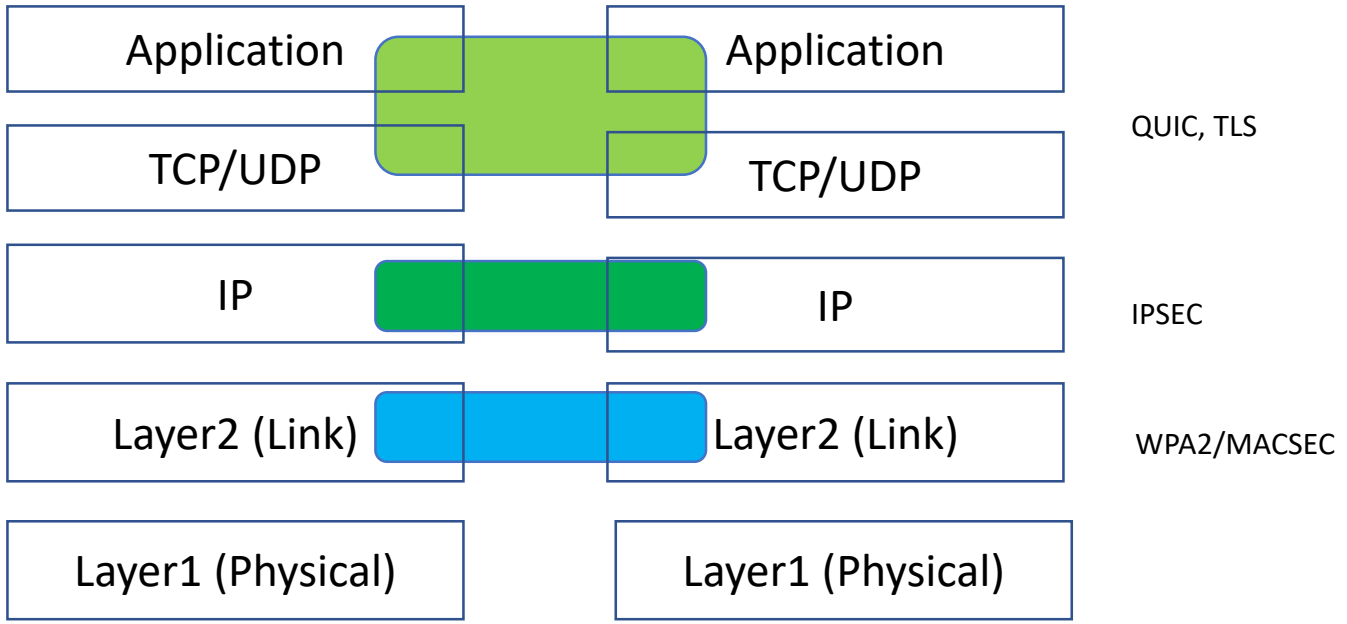
- TLS
- Transport Layer Security (IETF)
- Secure Communication between two applications
  - Web Browser – Web Server
  - Client App – Cloud API
  - Sensor Chip – App Processor
- Encryption Algo: AEAD, 3DES, RC4, CBC in TLS 1.2, AEAD in TLS 1.3

- IPSEC
- Internet Protocol Security (IETF)
- Set up a VPN, Secure IP Traffic between
  - Network to Network
  - Network to Host
  - Host to Host
- Encryption Algo: DES, 3DES

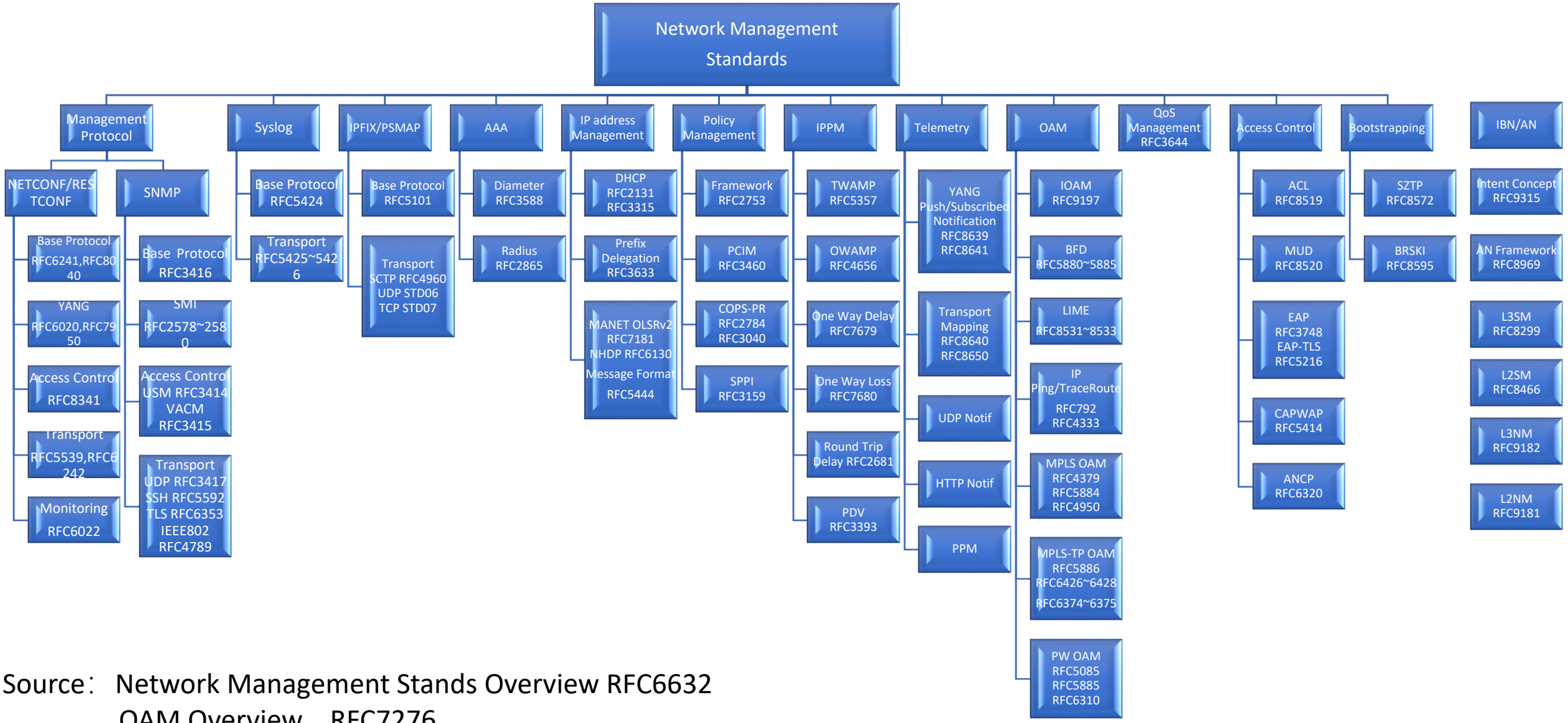
- MACSEC
- Media Access Control Security (IEEE)
- Deploy over Lan, Protect Ethernet Links between
  - Switch to Switch
  - Switch to Host
  - Host to Host
- Encryption Algo: AES-GCM

- WPA2
- WiFi Protected Access 2(WFA)
- Deployed over WLAN, Protect Wireless Links between
  - AP to AP
  - AP to Host
  - Host to Host
- Encryption Algo: AES-128 in CCM
- AES-256 in GCM

- QUIC
- Quick UDP Internet Connection(IETF)
- Secure Communication between two applications
  - Web Browser – Web Server
  - Client App – Cloud API
  - Client App – Web Proxy



IETF Network Management Standards Overview



Source： Network Management Stands Overview RFC6632
OAM Overview RFC7276

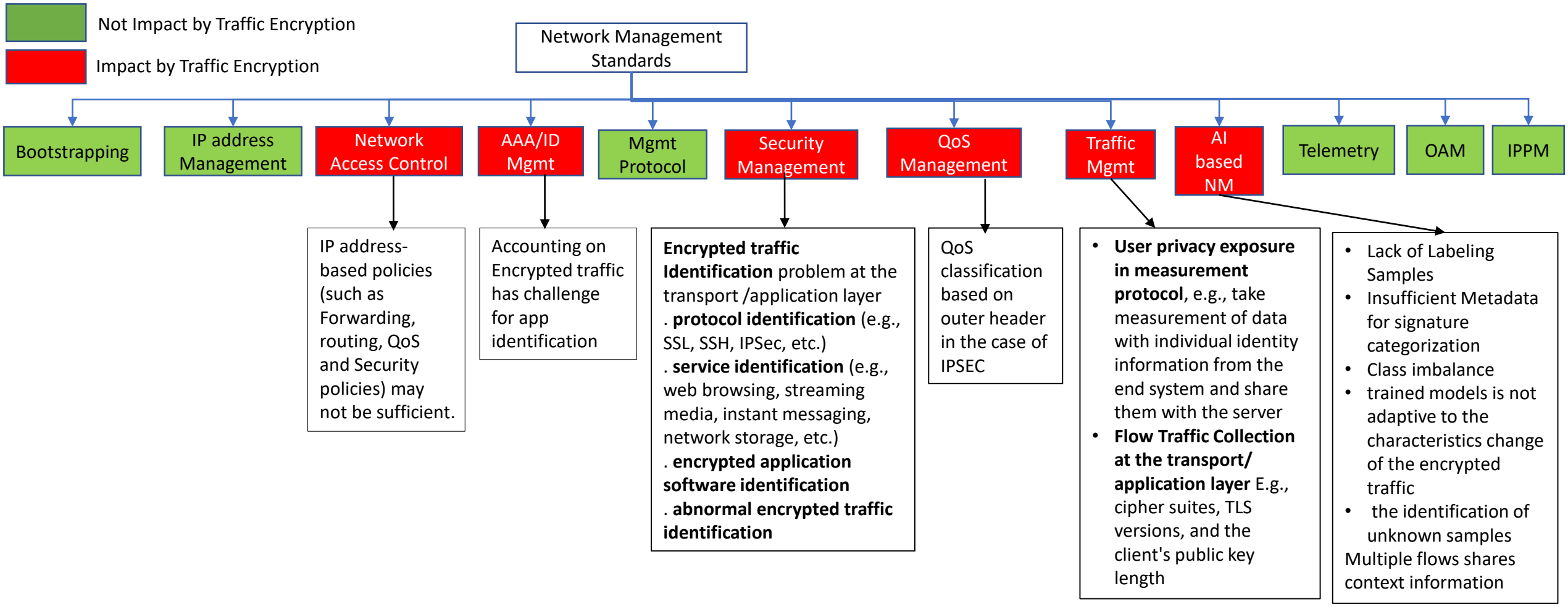
Network Monitoring Classification

Protocols supporting passive Monitoring	Protocols supporting active Monitoring
IPFIX (network) PSAMP (network) SNMP (network and device) NETCONF (device) RADIUS (accounting) Diameter (accounting) CAPWAP (device)	OWAMP (network) TWAMP (network) PPM

Protocols supporting Pull Mechanism	Protocols supporting Push Mechanism
SNMP (except notifications) NETCONF (except notifications) CAPWAP	SNMP notifications NETCONF notifications IPFIX PSAMP Syslog RADIUS accounting Diameter accounting

Source： Network Management Stands Overview RFC6632

Impacts of Encryption on Network Management



How network can be managed in support traffic encryption

- Irrespective of encrypted traffic or unencrypted traffic, Get what we can get from the network, resort to the network management plane or off path method
  - Data/Metadata driven management
    - Capture sufficient Network Metadata
    - Use AI/ML for encrypted traffic detection

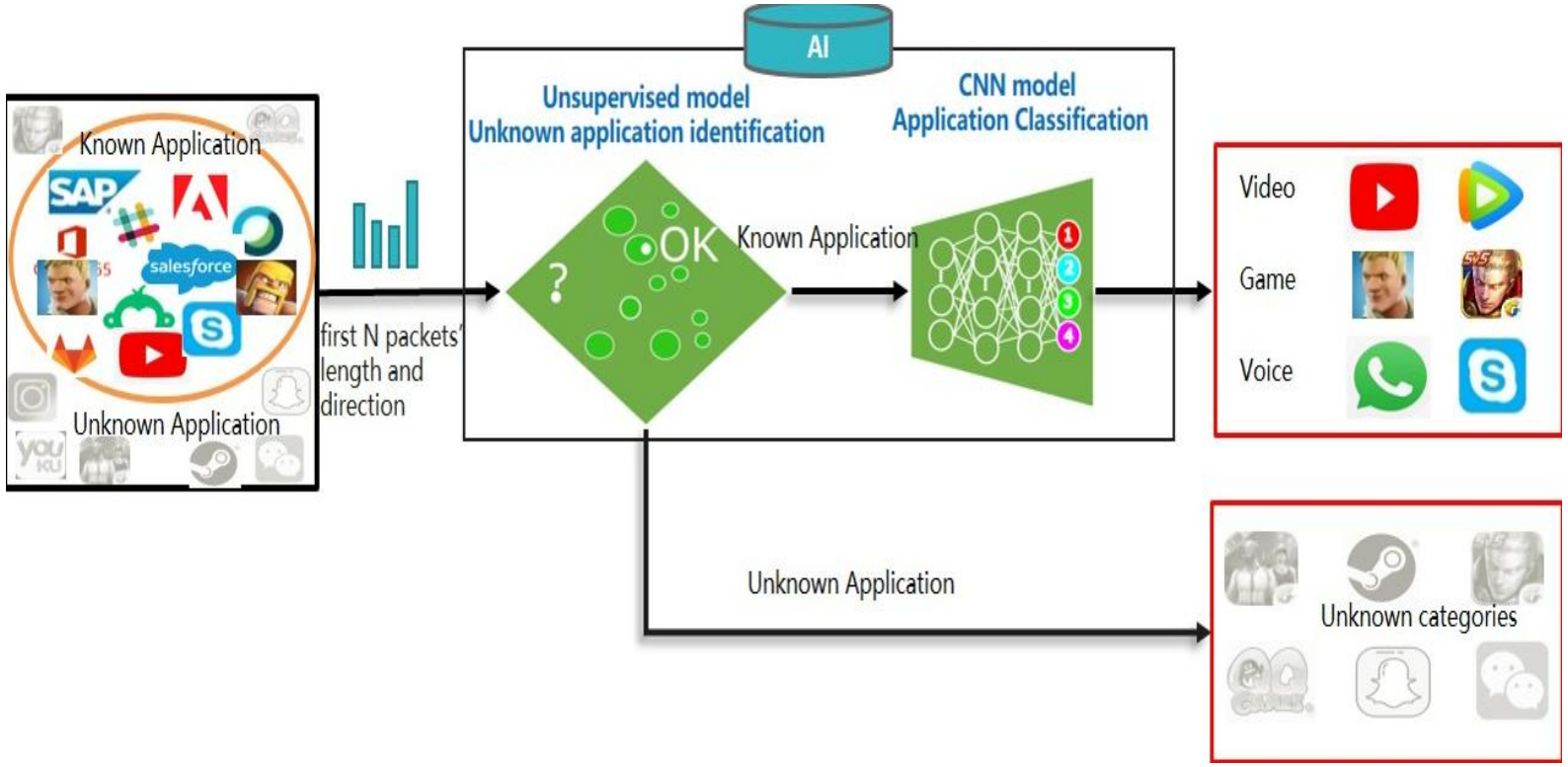
- Collaborate with User or Service Operators, more related to on path method
  - Collaborate with Users
  - Collaborate with Service Operators
  - Require more collaboration between application and network.

Data/Metadata driven management

- What is Network MetaData
  - It records the what, when, where and whom of network communications
  - It can capture from the fields from network header, transport header, application header
  - It can also capture from the outsider of the packet, e.g., inter-arrival time, packet length sequence

Metadata Type	Header Information (On Path)	behavior /pattern Information (Off Path)
TLS	The list of offered ciphersuites; The list of advertised extensions; and the client's public key length(Client); /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 (Server).	
DNS	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;
HTTP	Content-Type; User-Agent; Accept Language; Server; and code. URL; The presence of outbound and inbound HTTP fields	
QUIC	Spin bit for passive measurement; Negotiated version; SNI; Destination Connection ID;	
IPSEC		2-tuples (Source address, Destination address) in the tunnel mode and 5- tuples in the transport mode
Session Level		characteristics and arrival process of the session,session bytes and session persistence time etc.
Packet Level		packet size distribution, packet arrival time distribution, etc
Flow Level (Static)	Source and destination MAC/IP address, COS, DSCP	Flow start time, Flow End time, Application type, Physical input interface
Flow Level(Dynamic)	Packet size value, flow control window setting protocol flag, IPid value	Packet event times Packet inter-arrival time Inter-burst times Bytes per packet Cumulative Bytes per packet Bytes per burst Periodical Throughput samples
Host based	N/A	Process Name; OS Name; OS Edition; OS Version; Hash of the process; The number of the ports;

Metadata driven AI based network management



Encrypted Traffic Identification

- Protocol Identification
- Flow Classification
- Traffic Feature Extraction

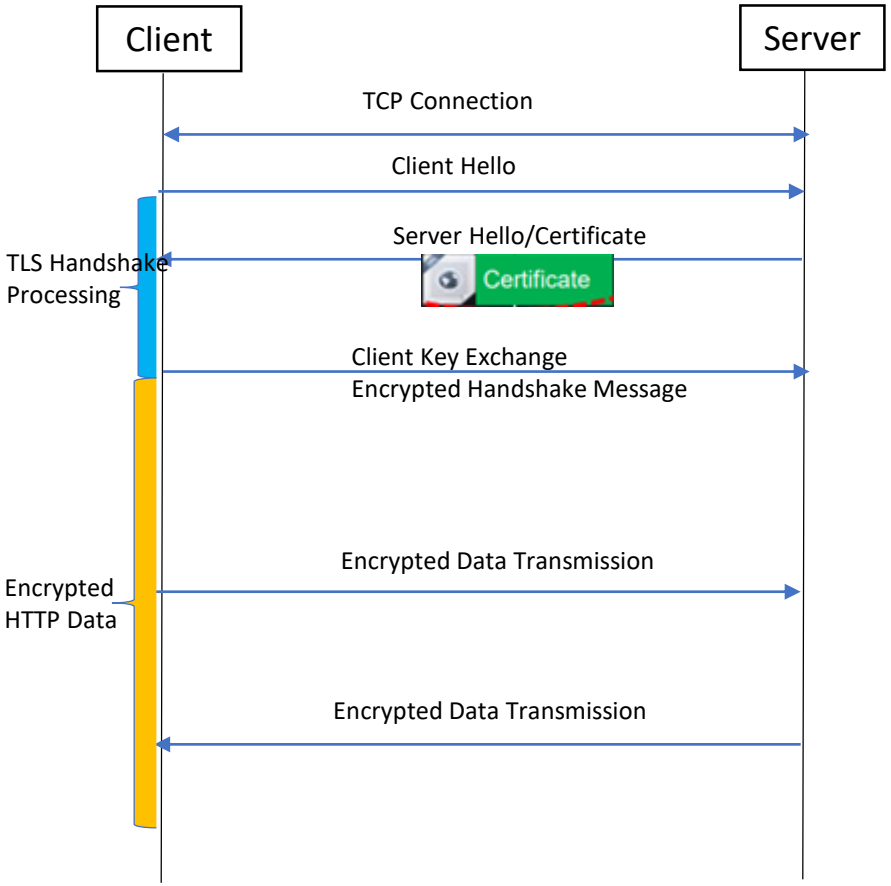
Model Training

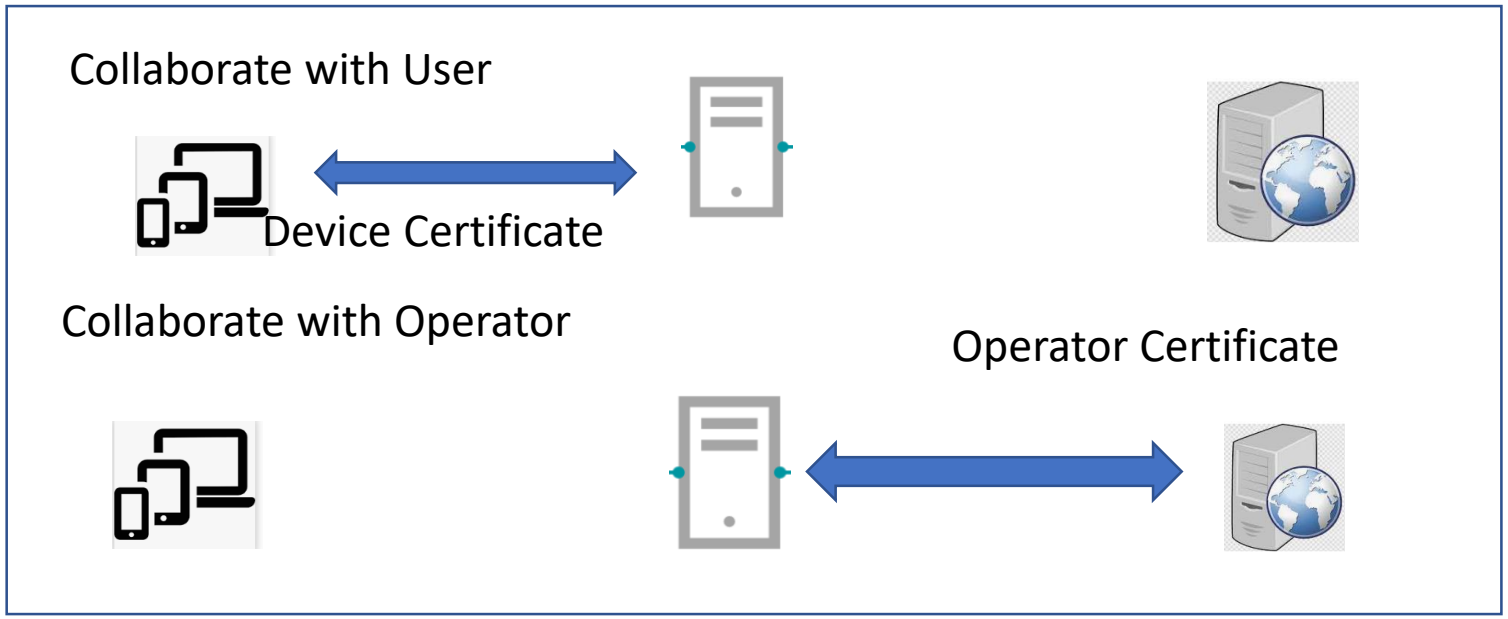
- Bayesian Network Model
- Vector Machine Model
- Decision Tree Model, etc

Pattern Matching

- Signature match

Collaborate with User or Service Operators





TLS Agent Mechanism	Feature	Cost
Collaborate with User	Not aware of Proxy by Service Operator	Proxy authorization and configuration by UE
Collaborate with Operator	Not aware of Proxy by UE	Collaborate with operator, e.g., generate session key for proxy using trust relation between UE and Server

Take Away

- **AI based network management is the best choice to tackle traffic encryption impact on the network management**
  - Develop Architecture for AI based Network Management on Encrypted Traffic in somewhere in IETF
    - **NMRG?**
- **Future direction and potential new work**
  - **Network Access Control Management**
    - IP address based Access Control -> Policy based Access Control [NIST-ABAC]
    - Diameter/Radius extension for ACL attribute or User control list (UCL) attribute
  - **Network Security Management**
    - TLS profile for malware traffic detection [TLS-MUD]
  - **Network and Application Collaboration**
    - Collaborative Method needs more innovation

Comments, Questions, Concerns?