Distributed Client Behavioural Anomaly Detection

Tech Con 2025 Abstract 322

HPE Edge;

Distributed Client Behavioural Anomaly Detection

Abstract

In a regular medium to large scale Network multiple user devices get connected to numerous network appliances. The network of today has exploded because of two simultaneous phenomena in the last decade and half, IOT and BYOD. Even in a controlled environment like a Campus network, there can be devices that are compromised or are behaving anomalously. It becomes imperative that such patterns are understood, and proactive actions are taken. The sheer volume and variety of traffic makes it difficult to analyze them for anomaly through cloud-based Network Management Systems (NMS). There is a compelling case of building something locally for an early anomaly detection. This work proposes a novel and smart method for client device and related network anomaly.

Problem Statement

The global campus networking equipment market is expected to reach $40.55 billion by 2028[4].The modern enterprise campus network is more complex than ever before. The sheer volume and complexity of devices connected to the network is huge. Internet of Things (IOT[1]) and Bring Your Own Device (BYOD[2]) phenomenon have led to exploration of devices in Campus Networks. There is a good chance that some IOT device is compromised, or some legacy handheld device is sending proprietary traffic that cannot be decoded, or some actual authenticated client is infected and is misbehaving and depriving the network of its resources. It has been observed that a majority of attacks on campus have been because of attacks from inside because of a compromised device. There are also cases where a Network device like a Switch/Router is sending unnecessary control or data messages because of some misconfiguration or malformed software.
It has been seen in typical customer deployments that the majority of the network issues can be categorized into two classes.

1. *Misconfigured Network*
2. *Misbehaving devices (Client or Network)*

2 is sometime caused by 1 but mostly they are orthogonal problems.

The issue that network administrator faces today is that once the issue has happened most of the debugging starts. Reactive resolution typically causes a lot of business hours and resources. This work aims to solve this critical problem by focusing on innovative methods to detect client anomalies and doing proactive action wherever possible. We need to find better ways to troubleshoot client issues to make our products and solutions more competitive and compelling.

Our Solution

The main idea behind the solution is to characterize a particular client device which is connected to a Switch, or an Access Point is by analyzing its behavior over a period. Once the baseline behavior is built for a client, potential anomaly from that baseline is identified. The baseline behavior can be simply based on the Client traffic pattern, traffic volume, device type or anything else that can be built on monitoring its characteristics. Clustering of clients based on their behavior is done in the steps as explained below.

Mobility pattern and deviation

1. An IOT device will typically be stationary and will not move around. Any IOT device which is showing unusual mobility can be tracked and flagged for anomaly.
2. Any fast-moving device typically will not move beyond a threshold. As any moving client could be typically climbing floors or moving across rooms, a certain threshold will be built. Any deviation needs to be flagged.
3 A fast-moving device will not be an Internet Protocol Television(IPTV) source. So, if it sends Multicast Data and is moving around, then it needs to be further analyzed.

Traffic Pattern and deviation

1. Unnatural traffic from a device- A device type once identified through Device finger printing services, can further be analyzed if it is sending unusual traffic. e.g. IOT device sending video streams. This client needs to be analyzed.
2. Multicast Joins/Leaves sent by a device – Any multicast client like an IPTV receiver typically would send certain patterns of Jois and Leaves. E.g. a single device cannot send more than one Join without sending a leave. There needs to be certain thresholds before a Leave and Join is sent by the same client.

3. Device opening too many TCP connections – Any client sending way too many TCP connections is a cause of concern. This could be actual client opening too many applications or a compromised client. A Client suddenly sends too many Data/ARP requests – This is like the previous case when a client is suddenly sending too much data or sending unusual number of ARP requests.
4. A chatty client has become silent or vice versa – There are devices which are silent compared to others and some which are noisy. An IOT device is typically silent, same as a Syslog server, suddenly if they start sending more data, the type of data needs to be analyzed. The reverse is also true of some chatty devices suddenly sending very little data.
5. A unicast client has become multicast or vice versa- Typically a client is Multicast receiver/sender or unicast sender. If we see a change in trend that action needs to be monitored.
6. The Application viewed by the Client has suddenly changed – If a client is watching a particular class of Application (say Video, Social Network) and suddenly the pattern is changed then this traffic needs to be analyzed as well.

General Pattern deviation

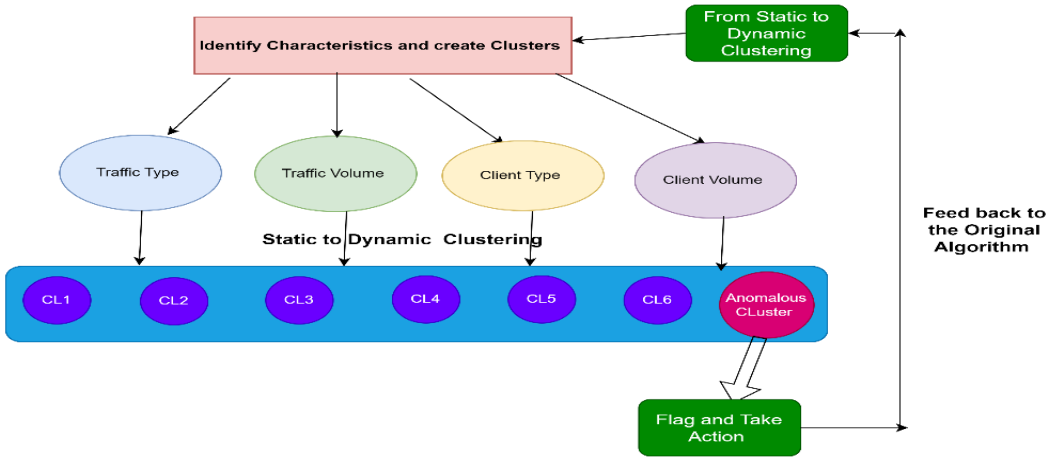
1. Many more actions like TCP Burst from a client, multiple IPs from the same Client (MAC) etc can also because of concern and analyzed.
2. Misbehaving Network devices (Routers), sending way too many Protocol messages (Route Updates, Adjacency messages etc).

The table below shows typical thresholds that were considered for client devices and actions

Device Type	Device Identification	Anomaly Characterization	Action on Anomaly
IOT Devices	Protocols used for IOT Communication – MQTT[10], COAP[11]. Device Finger Printing (DFP) [12]	Fast Mobility Unnatural Traffic like Video	Send the Sampled traffic to a centralized Network Management System (NMS) for further analysis Flag as Anomaly. Quarantine Device
Mobile Clients	Device Finger printing	Mobility beyond a threshold. Application watching pattern changes. Laptop/Desktop is moving continuously. Too many DNS/DHCP/ARP requests. Application type changes	Same
Static Clients	Deep Packet Inspection (DPI) or DFP[12]	Any sort of Mobility Too many DNS/DHCP/ARP requests. Application type changes	Same
Multicast IPTV Source	Based on Flows and DFP	Mobility beyond a threshold. Sending volume goes low suddenly Starts sending Unicast traffic	Same
Multicast Clients	Based on Internet Group Management Protocol (IGMP) [7] Packets	Too much mobility. Too many IGMP packets Too little IGMP Packets	Same
Infra/Network Devices	Link Layer Detection Protocol (LLDP) to detect the MAC	Any sort of Mobility. Too many Control packets. Adjacencies going DOWN and UP.	Reset Configuration or look at the Link status

Putting it All Together

In summary, the idea is to create clusters based on client characteristics and then find deviations from the clusters and flags anomaly. The anomalous characteristics can then be analyzed by a Centralized NMS like Aruba Central [5] and can be fed to some AI based algorithm to characterize. The characterization can then be fed back to the device as well and more sophisticated anomaly detection can be built.



Evidence the solution works

Currently with the Aruba CX devices all client information is maintained in different modules. Host IP information is maintained in the Neighbor Tables. Multicast Client and Source information is maintained by IGMP and Protocol Independent Multicast(PIM) Modules. Authenticated client information is maintained by Port Access. Other information about Clients like DNS and DHCP requests are also maintained by different modules. Flow/Application Information and Counter information are also maintained and published periodically. In addition, MAC Move Alerts are also available as the ARP Module always detects a moving client based on the Port to which it has connected.

We have built an anomaly detector module that analyses these tables and their patterns periodically and builds the Clusters. It also builds the Anomalous Clusters based on deviation. We have built CLI Command to dump these clusters and the corresponding reasons and weights of the clusters. This table can be viewed from Centralized NMS through REST APIs[13] also. In addition, Alerts are also generated for any Anomaly. The Centralized NMS can respond to the Alert and dump the full table through a REST API Query and Response.

Competitive Approaches

Anomaly Detection Market Size was valued at USD 5.3 billion in 2022[6]. The anomaly detection market industry is projected to grow from USD 6.1 Billion in 2023 to USD 15.0 billion by 2030, exhibiting a compound annual growth rate (CAGR) of 16.10% during the forecast period (2023 - 2030). The on-network device Anomaly detection and prediction approach seems to be unique. We have not seen any competitor providing similar offerings.

Current Status

The solution is prototyped and implemented in the Aruba OS-CX device. The solution is also filed as a Patent in 2024. This will be productized next year and will help us increase our market share in the Campus Networks where Aruba is already a Global leader.

Next steps

In the next steps, the plan is to integrate this solution with Next Gen Aruba Central. The solution will also be incorporated into other devices like Access Points. This can be one of our plus points when Aruba integrates with Juniper MIST solutions as this is a distributed anomaly detector in the network device themselves,

References

[1] IOT Market Size - https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html#:~:text=What%20is%20the%20market%20size,18.8%25%20from%202024%20to%202029.
[2] BYOD Market Size - https://www.mordorintelligence.com/industry-reports/byod-market
[3] Troubleshoot market Size - https://www.fortunebusinessinsights.com/network-monitoring-market-108432
[4] Campus Market Size -https://www.linkedin.com/pulse/campus-network-market-size-share-strategies-growth-ixdyf
[5] Aruba Central - https://www.arubanetworks.com/products/network-management-operations/central/
[6] Anomaly Detection Market Size - https://www.marketresearchfuture.com/reports/anomaly-detection-market-5756#:~:text=Anomaly%20Detection%20Market%20Size%20was,period%20(2023%20%2D%202030).
[7] IGMP - https://datatracker.ietf.org/doc/html/rfc3376
[8] PIM - https://datatracker.ietf.org/doc/rfc7761/
[9] Juniper MIST - https://www.juniper.net/us/en/products/mist-ai.html
[10] MQTT - https://www.hivemq.com/mqtt/
[11] COAP - https://www.geeksforgeeks.org/constrained-application-protocol-coap/
[12] DFP - https://clearcode.cc/blog/device-fingerprinting/
[13] REST API - https://www.ibm.com/topics/rest-apis