

Capstone Project 20.1: Initial Report and Exploratory Data Analysis (EDA) Update

Shaji Nathan

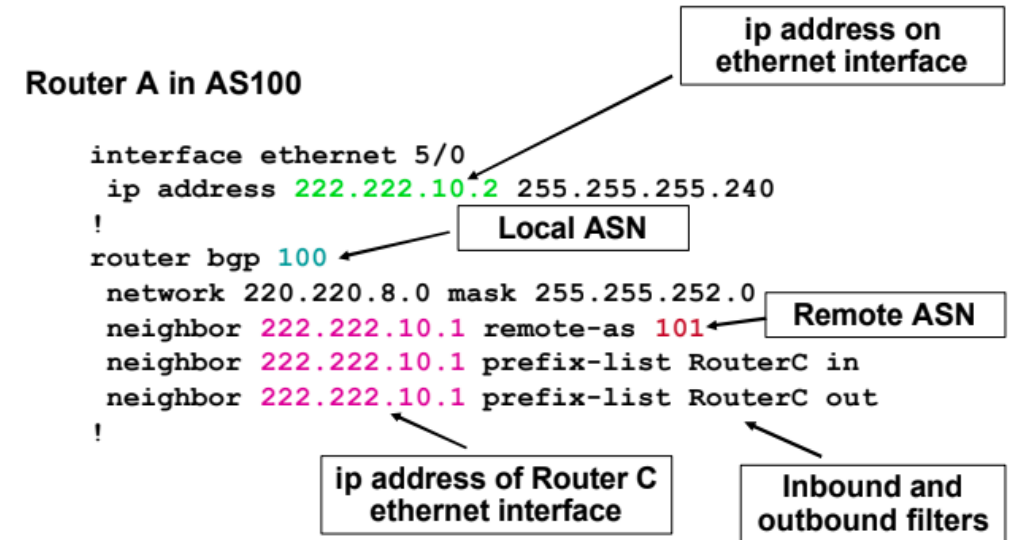
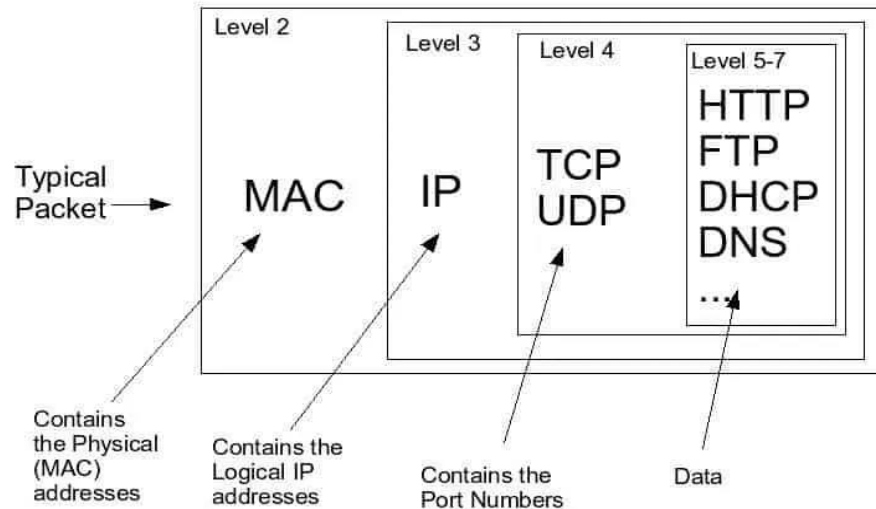
11/01/2022

BGP Anomaly Detector



BGP Routing

Border Gateway Protocol — the “post office of the internet”



Responsible for sending information in the form of “packets.”

Recent News : BGP related Malicious Activity

- Attacks on BGP can disrupt individual internet hosts or networks and destabilize the operation of the global network
 - Example: BGP Route Hijacking, also called prefix hijacking, route hijacking or IP hijacking, is the illegitimate takeover of groups of IP addresses by corrupting Internet routing tables maintained using the Border Gateway Protocol (BGP).

Edge Articles | 8 MIN READ | ARTICLE

101: Why BGP Hijacking Just Won't Die

A look at the dangers of attacks on the Internet's Border Gateway Protocol and what ISPs and enterprises can do about them.



Seth Rosenblatt
Contributing Writer

July 28, 2021



Financial Impact Example:

- On Monday, October 4 2021, a BGP outage cost Facebook roughly \$60 million in revenues over its more than six-hour period.
- Facebook shares fell 4.9 percent on the day, which translated into more than \$47 billion in lost market cap.
- Reference: <https://www.datacenterdynamics.com/en/opinions/too-big-to-fail-facebooks-global-outage/>

Forbes




BGP Attacks Pose A Substantial Operation Risk -- Are Enterprises Paying Attention?

 **Jason Crabtree** Forbes Councils Member
Forbes Technology Council
COUNCIL POST | Membership (Fee-based)

Jan 11, 2021, 08:40am EST

 Jason Crabtree is the CEO and Co-Founder of [QOMPLX](#). Previously, he served as a Special Advisor to senior leaders in the DoD cyber community.



 SIGN IN **The Register**  


{ NETWORKS }


BGP super-blunder: How Verizon today sparked a 'cascading catastrophic failure' that knackered Cloudflare, Amazon, etc

'Normally you'd filter it out if some small provider said they own the internet'

Kieren McCarthy in San Francisco

Mon 24 Jun 2019 // 19:01 UTC

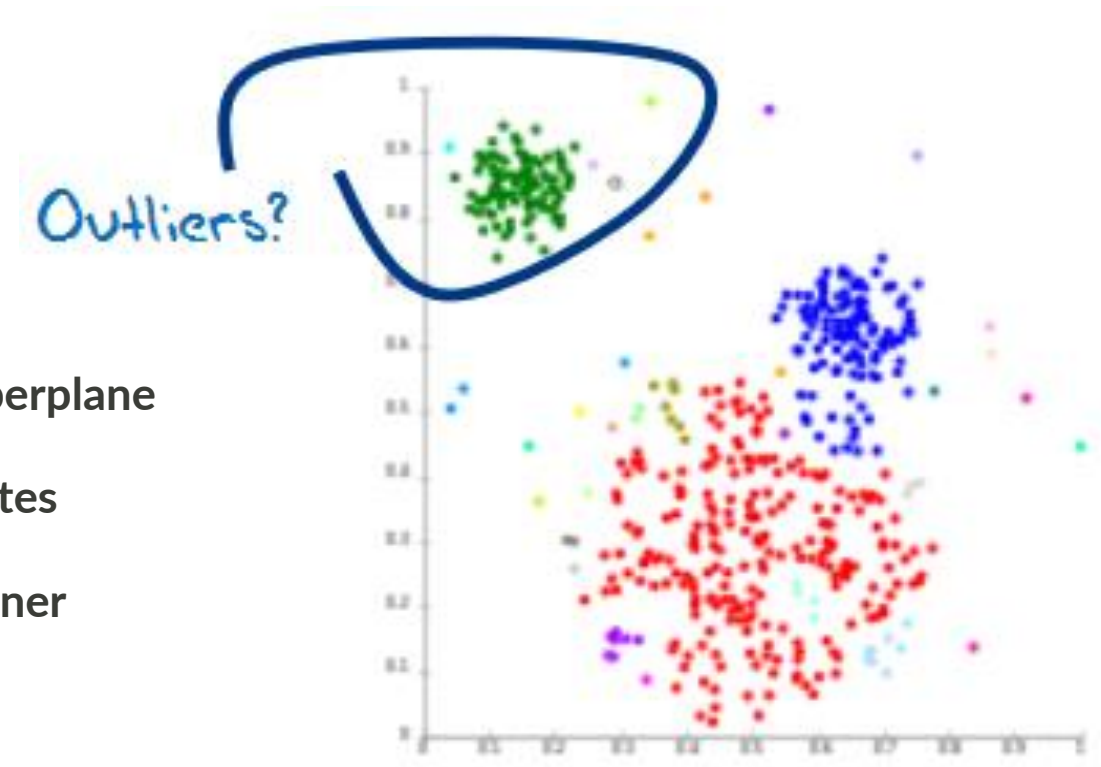
61 



UPDATED Verizon sent a big chunk of the internet down a black hole this morning – and caused outages at Cloudflare, Facebook, Amazon, and others – after it wrongly accepted a network misconfiguration from a small ISP in Pennsylvania, USA.

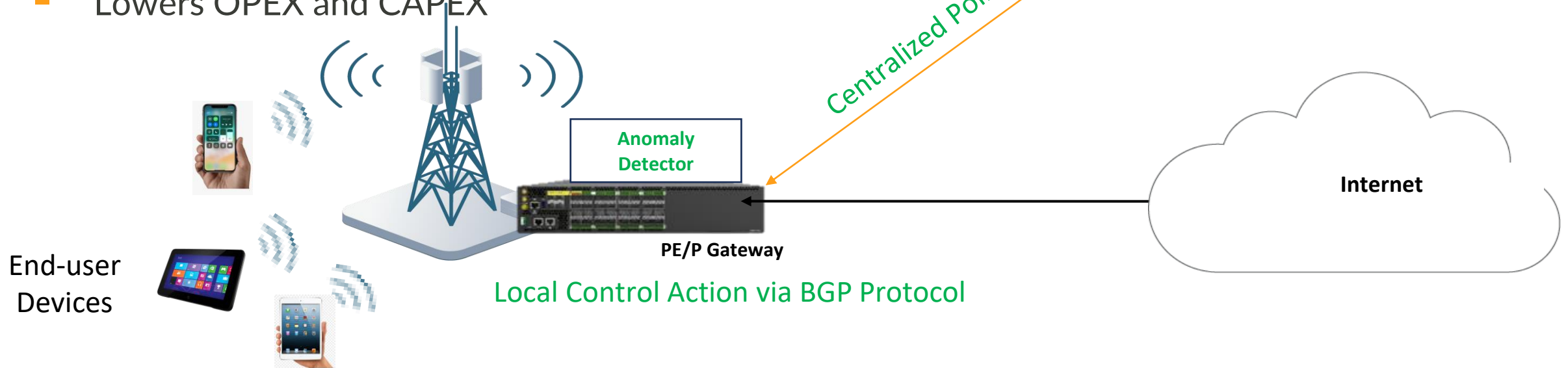
Machine Learning (ML) for Anomaly Detection

- Initial goal is to use a supervised learning model
- Real time Classification of BGP Updates
 - Normal
 - Anomalous Traffic
- Labeled training samples to learn a classification hyperplane
- Machine Model developed from real time BGP updates
- Model is pushed to control plane via a docker container
- Works with ACLs and BGP module in OCNOS
- Sold as an upsell application on OCNOS

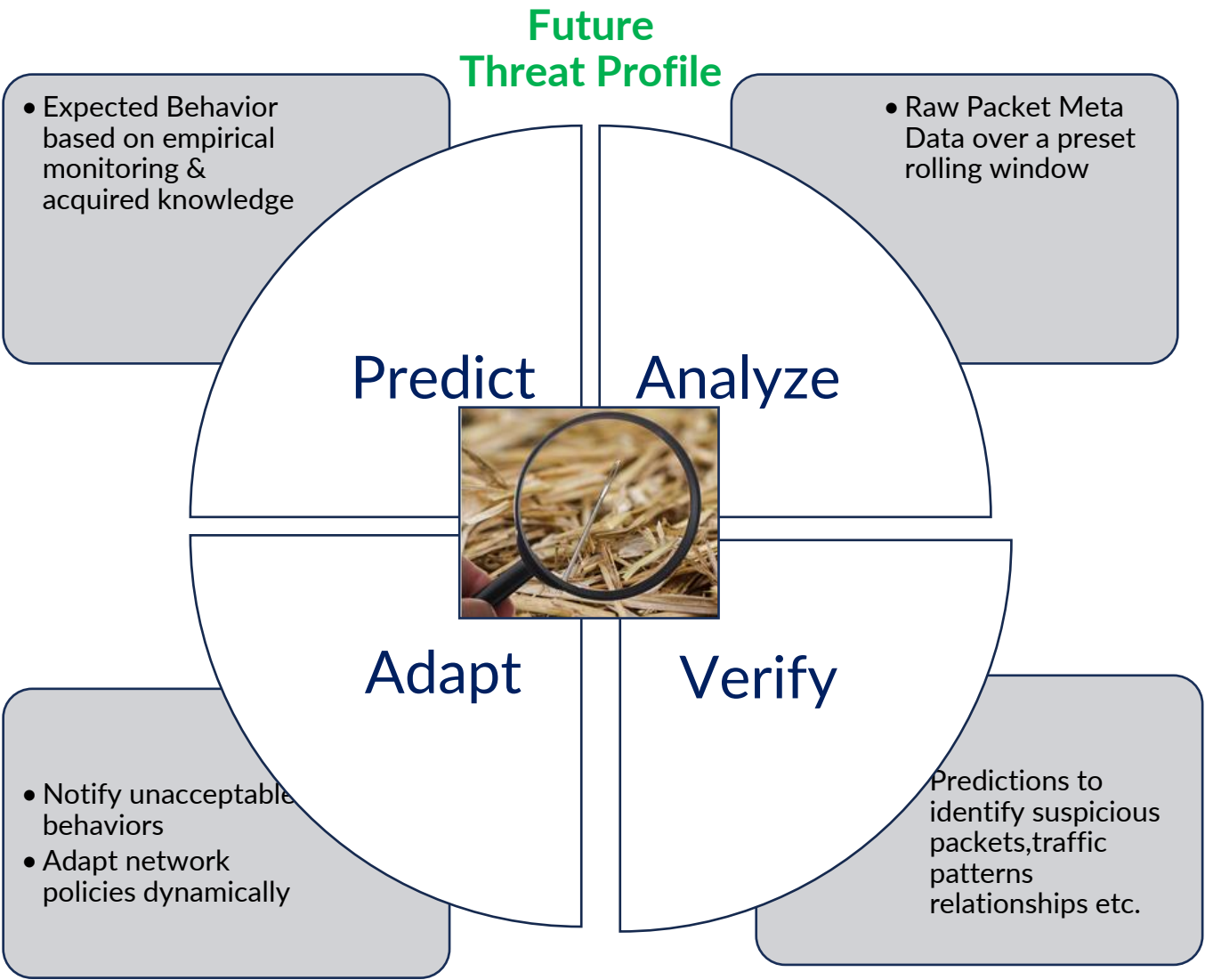
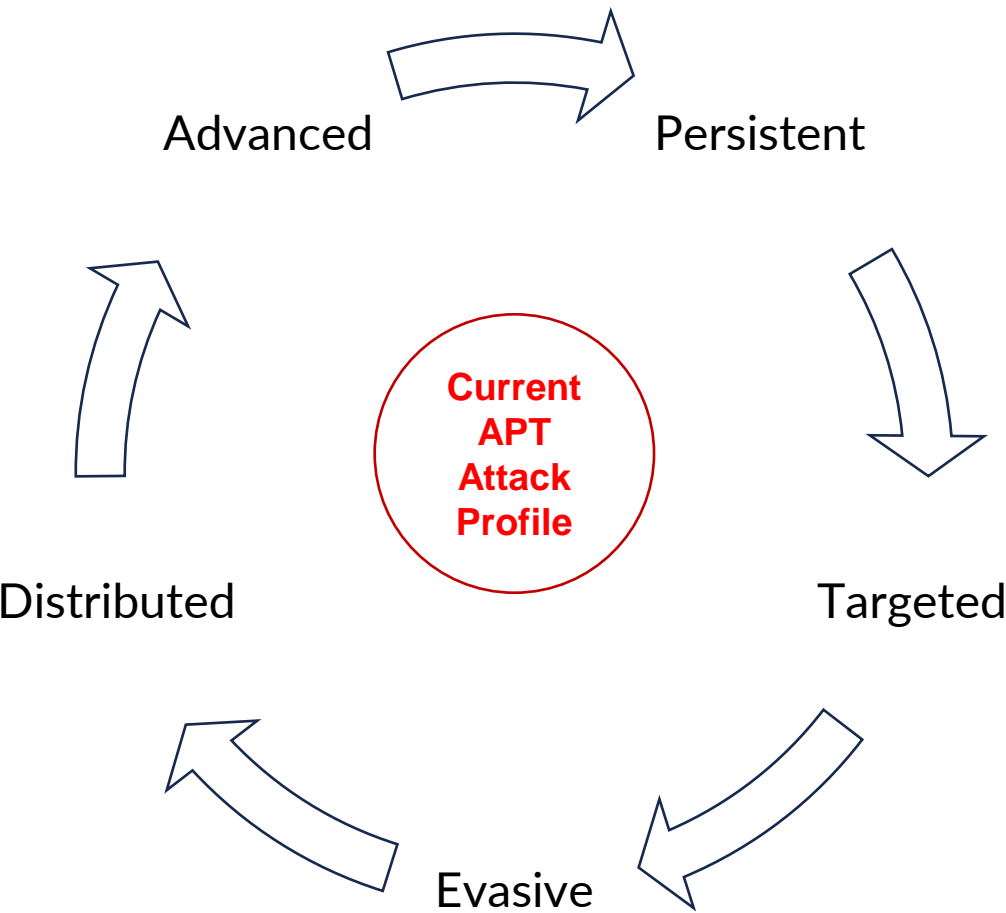


Sample Application: PE Gateway Protection

- Software Module on PE/P Gateway
- Realtime detection of BGP Anomalies
- Autonomously blocks/reroutes anomalous traffic
- Enables Telco Carriers to respond in real time to
 - Emerging Threats
 - Zero Day Attacks
 - Routing Anomalies
- Prevents Loss of Service without Truck Roll
- Lowers OPEX and CAPEX



The Business Benefit:



Thanks !