NOKIA Bell Labs

Differential Anomaly Detection

Scenario 05

Nokia Bell Labs: Noosha, Vicky

Arcada University: Emil, Anton

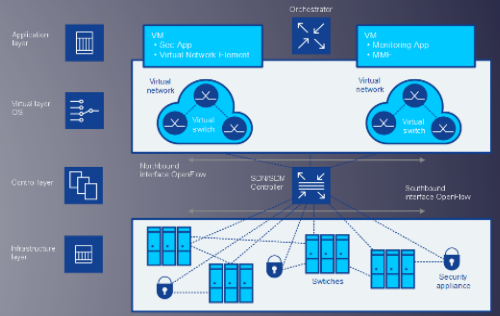
20.04.2017

Anomaly Detection

- Reduce detection process time while handling big data in cloud
- Current IDS and IPS rely on static signatures
- Signatures are released after attack has been done

SDN Security

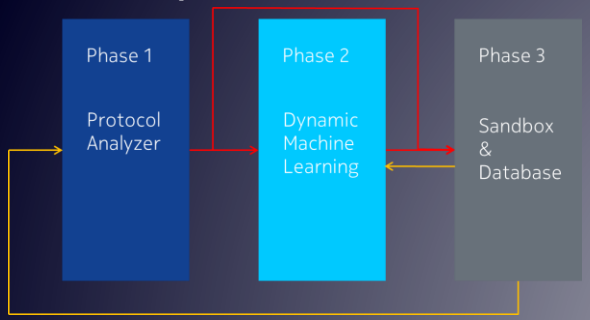
- Programmability of SDN/NFV increases attack surface and introduces new security challenges to cloud
- DoS attack or malicious code injection on SDN controller and switches



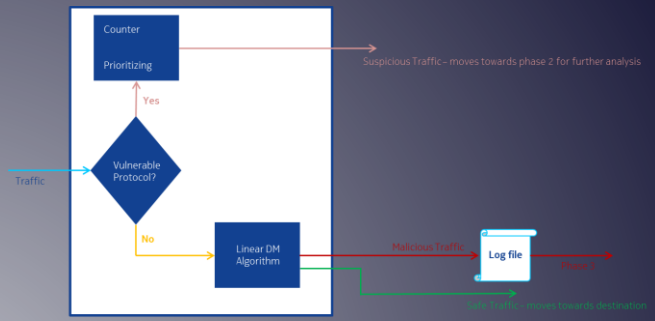
IoT Security

- New use cases require automated and orchestrated security mechanisms
  - Industry 4.0
  - Health
  - Megacities and military
- High criticality level for heath, military and public safety require accurate and fast detection mechanisms

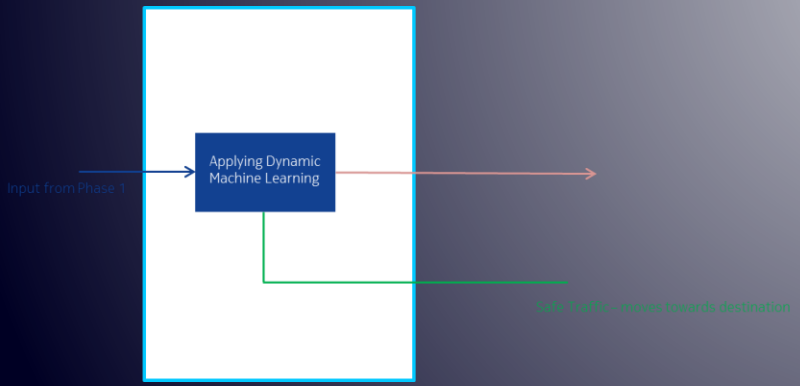
Anomaly Detection: DaaS



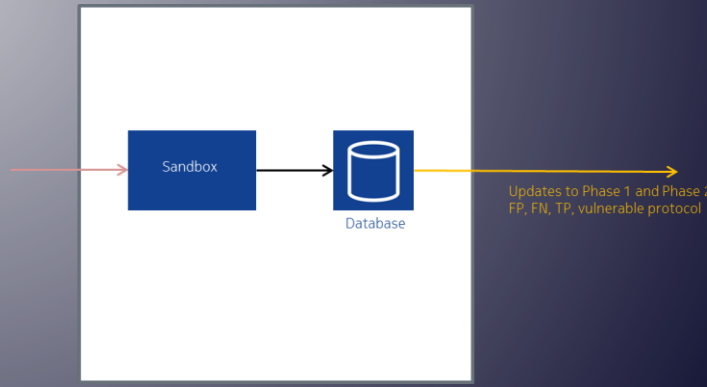
1) Protocol Analyzer



2) Dynamic Machine Learning

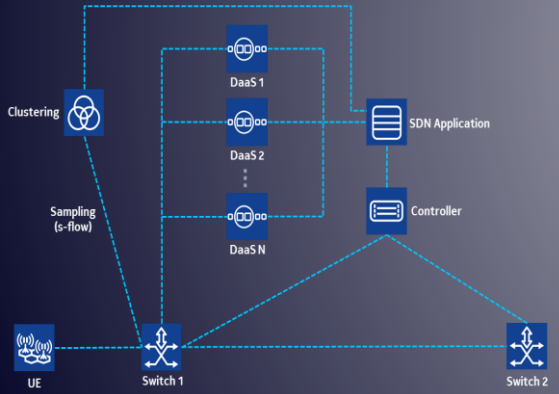


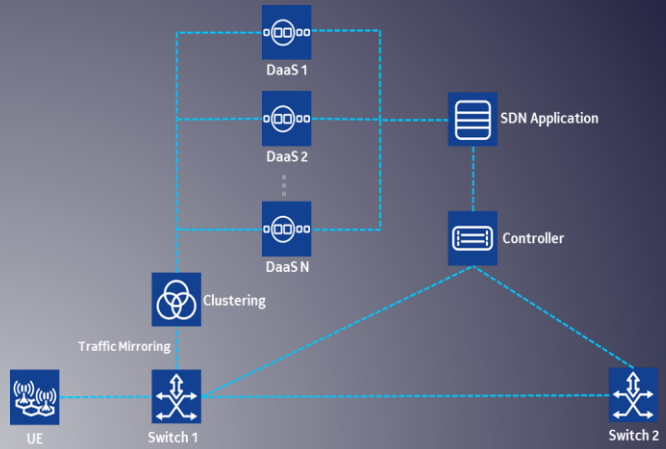
3) Sandbox and Database



SDN Security

- Applying s-flow (UP and CP) on SDN switches
- Clustering and load balancing on DaaS instances
- Analyzing traffic and detecting attack patterns (DaaS)
- Orchestrating DaaS instances with SDN application
- Blocking malicious traffic with SDN controller using flow control mechanisms



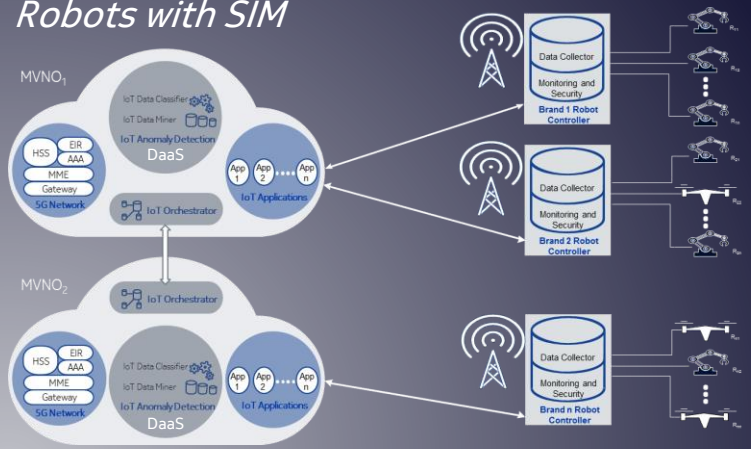


- Two approaches
  - Sampled clustering
  - Clustering for each packet
- Traffic mirrors from switch 1 to clustering node and sent to corresponding DaaS node
- Anomaly detection is applied in DaaS and results are sent to SDN Application
- SDN Application communicates with controller for mitigation

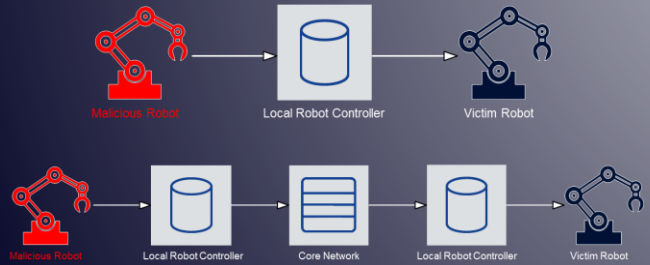
IoT Security, Robots Use Case

- Collecting data (UP and CP) from local robot controller
- IoT data classification and mining for labeling traffic
- Informing other robots about malicious drone/robot via IoT orchestrators within multiple MVNOs
  - Inter MVNO communication
  - Intra MVNO communication
  - Roaming drones/robots
- Optimizing learning methods for IoT security and learn new attacks
- Data orchestration and chain management for IoT robots/drones security among MVNOs

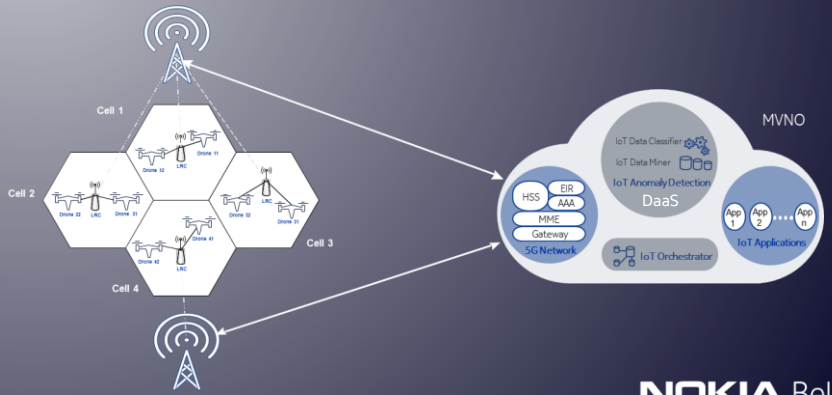
Robots with SIM



Attack Scenarios



SIMless Robots



Data and Performance Evaluation

Labeled Attack

- Nokia Lab
  - Executed windows and android malware in lab
  - Captured Network traffic
  - Filtered benign traffic
- ISCX IDS dataset
  - Malicious Traffic
  - Beningn traffic

Performance Evaluation

- Expected F ratios for different attack per algorithm SOM
  - SVM, DT, SOM, NN, GA/SI
  - Backdoor, DoS, trojan, bot, downloader, spyware, ransomware,…
- Expected Accuracy (TP+TN) / (TP+FP+TN+FN) and process time
  - ?
  - ?

NOKIA

Copyright and confidentiality