

# Differential Anomaly Detection

Scenario 05

Nokia Bell Labs: Noosha, Vicky

Arcada University: Emil, Anton

20.04.2017

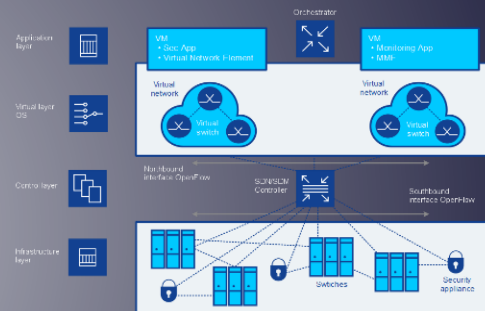
# Anomaly Detection

- 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

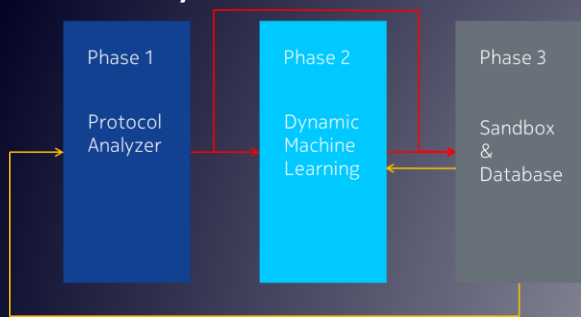


# IoT Security

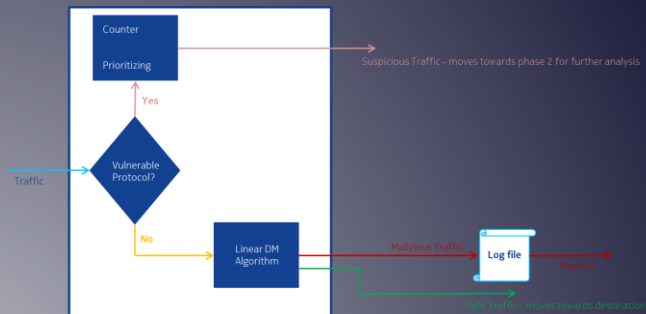
- New use cases require automated and orchestrated security mechanisms
  - Industry 4.0
  - Health
  - Megacities and military
- High criticality level for health, military and public safety require accurate and fast detection mechanisms



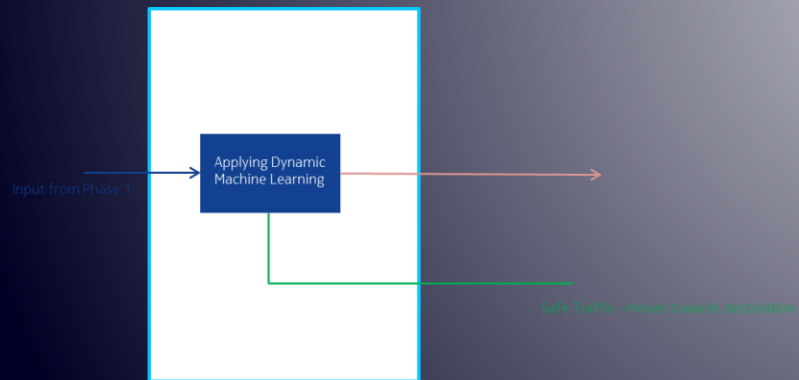
# Anomaly Detection: DaaS



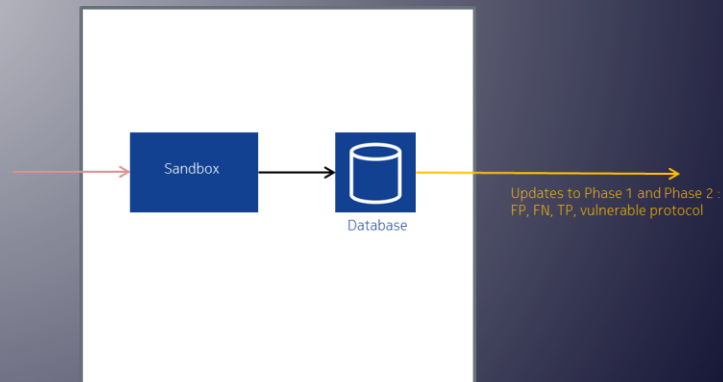
## 1) Protocol Analyzer



## 2) Dynamic Machine Learning

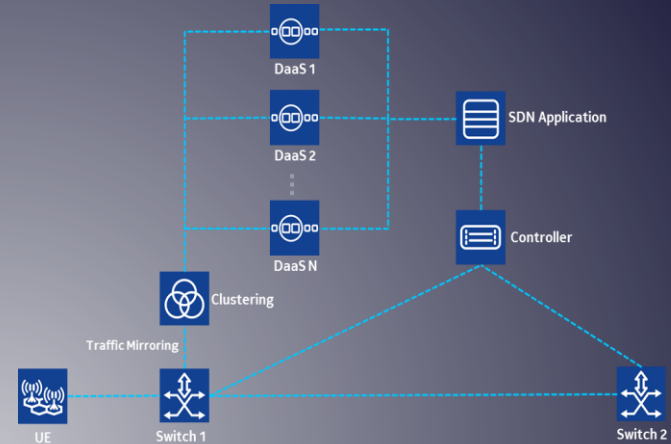
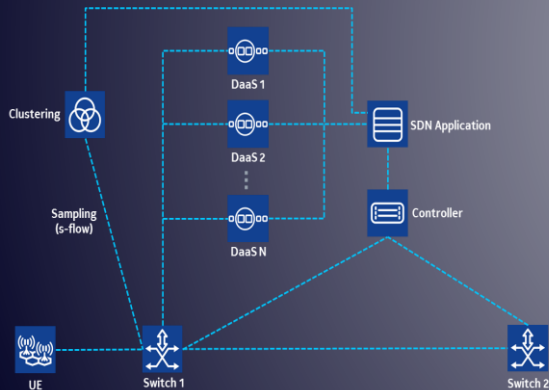


## 3) Sandbox and Database



# 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

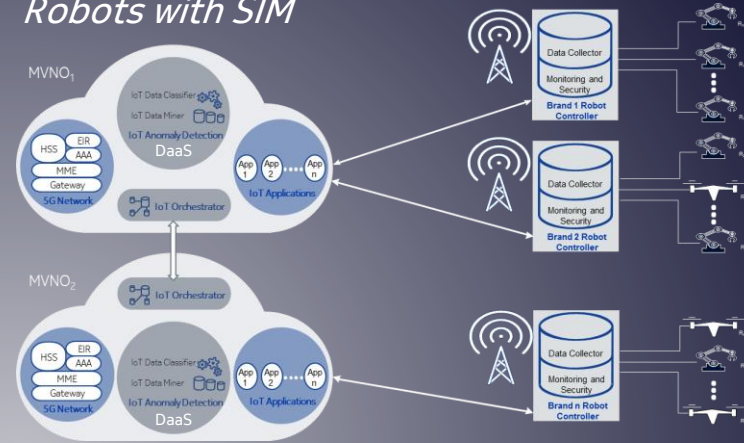


- Two approaches
  - Sampled clustering
  - Clustering for each packet
- Traffic mirrors from switch 1 to clustering node and sent to corresponding DaaS node
- Anomaly detection is applied in DaaS and results are sent to SDN Application
- SDN Application communicates with controller for mitigation

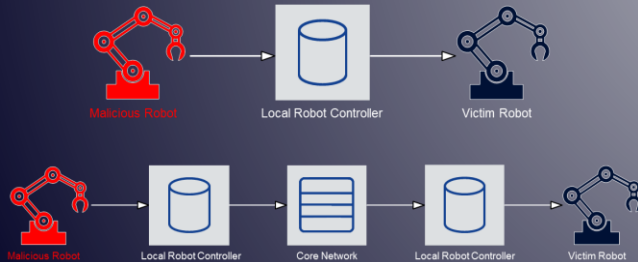
# IoT Security, Robots Use Case

- 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

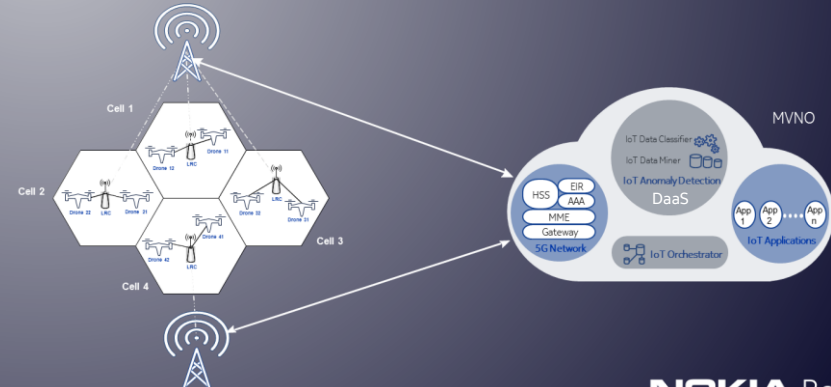
## Robots with SIM



## 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
  - Benign 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

---

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use of Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose,

are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.