GRIFIN

Cognitive and Programmable Security for Resilient Next-Generation Networks

Gregory Blanc

IMT/Télécom SudParis, Institut Polytechnique de Paris

RESSI 2022

Chambon-sur-Lac , May 10th, 2022

Ever heard about GRIFIN?

Ever heard about GRIFIN?

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)
  - Vantage points are distributed but traffic may be sampled

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)
  - Vantage points are distributed but traffic may be sampled
- Cyber-threats are diverse and malicious events are proliferating

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)
  - Vantage points are distributed but traffic may be sampled
- Cyber-threats are diverse and malicious events are proliferating
  - Fatigue promotes automation, leaving the human off the loop

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)
  - Vantage points are distributed but traffic may be sampled
- Cyber-threats are diverse and malicious events are proliferating
  - Fatigue promotes automation, leaving the human off the loop

- *Machine Learning* and *Software-Defined Networking* are emerging as **enablers**

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)
  - Vantage points are distributed but traffic may be sampled
- Cyber-threats are diverse and malicious events are proliferating
  - Fatigue promotes automation, leaving the human off the loop

- *Machine Learning* and *Software-Defined Networking* are emerging as **enablers**
  - **ML** is expected to provide knowledge, inference and reasoning

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)
  - Vantage points are distributed but traffic may be sampled
- Cyber-threats are diverse and malicious events are proliferating
  - Fatigue promotes automation, leaving the human off the loop

- *Machine Learning* and *Software-Defined Networking* are emerging as **enablers**
  - Algorithms are usually *data-hungry* and costly in resources

Challenges in Next-Generation Networks

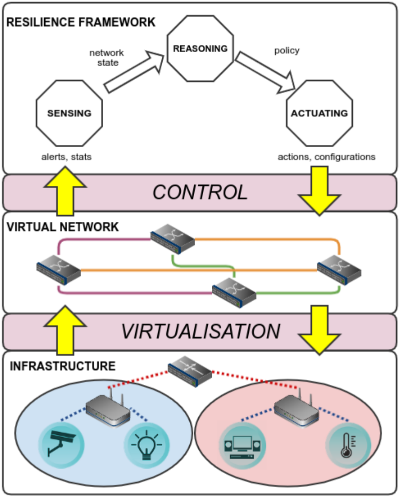
- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)
  - Vantage points are distributed but traffic may be sampled
- Cyber-threats are diverse and malicious events are proliferating
  - Fatigue promotes automation, leaving the human off the loop

- *Machine Learning* and *Software-Defined Networking* are emerging as **enablers**
  - Algorithms are usually *data-hungry* and costly in resources
  - **SDN** is expected to provide reactiveness and adaptation

Challenges in Next-Generation Networks

- Devices are increasingly connected to the Internet (wearables, sensors, IoT, IIoT)
  - Numerous, heterogeneous, with diverse traffic patterns and throughputs
- Networks are getting segmented into more distinct domains (cloud, fog, edge)
  - Vantage points are distributed but traffic may be sampled
- Cyber-threats are diverse and malicious events are proliferating
  - Fatigue promotes automation, leaving the human off the loop
- *Machine Learning* and *Software-Defined Networking* are emerging as **enablers**
  - Algorithms are usually *data-hungry* and costly in resources
  - Programmable orchestration are heavy and lack granularity

Objectives


RESILIENCE FRAMEWORK
REASONING
network state
policy
SENSING
ACTUATING
alerts, stats
actions, configurations
CONTROL
VIRTUAL NETWORK
VIRTUALISATION
INFRASTRUCTURE

Deep Learning Inside™

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by
   - Reduce training time by avoiding feature engineering

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by
   - Reduce training time by avoiding feature engineering
   - Reduce training data by leveraging transfer learning

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by

2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by

2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted
   - Make anomaly detection more trustworthy by adopting a reproducible evaluation methodology

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by

2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted
   - Make anomaly detection more trustworthy by adopting a reproducible evaluation methodology
   - Make anomaly detection more understandable by leveraging explainable methods

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by

2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted

3. Intrusion response requires extensive domain knowledge to be effective and prevent adverse impacts

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by
2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted
3. Intrusion response requires extensive domain knowledge to be effective and prevent adverse impacts
   - Reduce pressure on operators by enabling to express high-level intents

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by
2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted
3. Intrusion response requires extensive domain knowledge to be effective and prevent adverse impacts
    - Reduce pressure on operators by enabling to express high-level intents
    - Improve resilience by selecting least damageable countermeasures

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by

2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted

3. Intrusion response requires extensive domain knowledge to be effective and prevent adverse impacts

4. SDN applications abstract away low-level network operations, with no proof that its execution results into an equivalent data plane configuration

Research locks

GRIFIN attempts to tackle some scientific and technological locks

1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by

2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted

3. Intrusion response requires extensive domain knowledge to be effective and prevent adverse impacts

4. SDN applications abstract away low-level network operations, with no proof that its execution results into an equivalent data plane configuration
   - Ensure high-fidelity translation of high-level policy to distributed data plane configurations

Research locks

GRIFIN attempts to tackle some scientific and technological locks

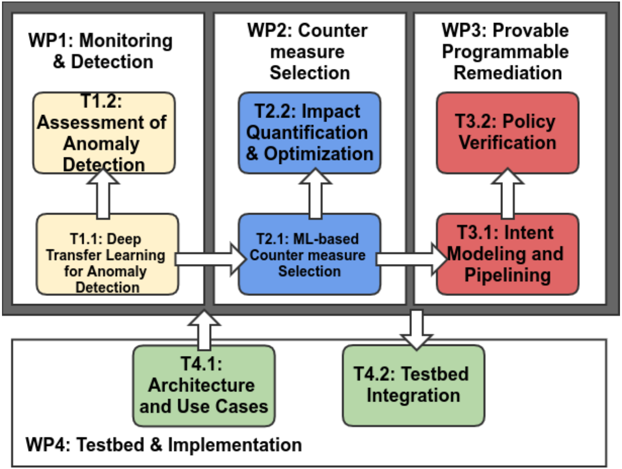
1. Leveraging DL methods relies on massive IoT datasets that are often hard to come by

2. Anomaly detection is only efficient if errors can be investigated, or at least decisions leading to alerts can be interpreted

3. Intrusion response requires extensive domain knowledge to be effective and prevent adverse impacts

4. SDN applications abstract away low-level network operations, with no proof that its execution results into an equivalent data plane configuration
    - Ensure high-fidelity translation of high-level policy to distributed data plane configurations
    - Enable formal verification of the effective enforcement of the policy

Approach


WP1: Monitoring & Detection
T1.2: Assessment of Anomaly Detection
T1.1: Deep Transfer Learning for Anomaly Detection
WP2: Counter measure Selection
T2.2: Impact Quantification & Optimization
T2.1: ML-based Counter measure Selection
WP3: Provable Programmable Remediation
T3.2: Policy Verification
T3.1: Intent Modeling and Pipelining
T4.1: Architecture and Use Cases
T4.2: Testbed Integration
WP4: Testbed & Implementation

First directions

- Started working on WP1

First directions

- Started working on WP1
  - (intern) survey of ML best practices to evaluate proposed IDSs

First directions

- Started working on WP1
  - (intern) survey of ML best practices to evaluate proposed IDSs
  - (intern) proposal of a robust and adaptive RL-based IDS

First directions

- Started working on WP1
  - (intern) survey of ML best practices to evaluate proposed IDSs
  - (intern) proposal of a robust and adaptive RL-based IDS
- Future works on all WPs

First directions

- Started working on WP1
  - (intern) survey of ML best practices to evaluate proposed IDSs
  - (intern) proposal of a robust and adaptive RL-based IDS
- Future works on all WPs
  - taxonomy of evaluation methodologies for IDS

First directions

- Started working on WP1
  - (intern) survey of ML best practices to evaluate proposed IDSs
  - (intern) proposal of a robust and adaptive RL-based IDS
- Future works on all WPs
  - taxonomy of evaluation methodologies for IDS
  - survey of intent pipelining approaches

First directions

- Started working on WP1
  - (intern) survey of ML best practices to evaluate proposed IDSs
  - (intern) proposal of a robust and adaptive RL-based IDS
- Future works on all WPs
  - taxonomy of evaluation methodologies for IDS
  - survey of intent pipelining approaches
  - survey of policy verification methods

First directions

- Started working on WP1
  - (intern) survey of ML best practices to evaluate proposed IDSs
  - (intern) proposal of a robust and adaptive RL-based IDS
- Future works on all WPs
  - taxonomy of evaluation methodologies for IDS
  - survey of intent pipelining approaches
  - survey of policy verification methods
  - implementation of an IoT testbed including probes

Ph.D Offer

- Ph.D position in Télécom SudParis, Palaiseau : Cognitive and Programmable Security (starting **Oct. 2022**):
  - AI-based countermeasure selection
  - intent-based countermeasure refinement
  - countermeasure enforcement verification

Applications are open until June 30th, 2022.

Contact:

@ `anr-grifin.telecom-sudparis.eu`

✉ `gregory.blanc@telecom-sudparis.eu`