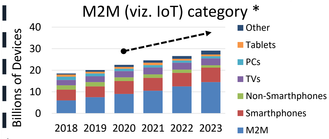
Giampaolo Bovenzi

Tutor: Antonio Pescapé

XXXIV Cycle - II year presentation

Hierarchical Learning in IoT Scenarios: a Hybrid Intrusion Detection Approach

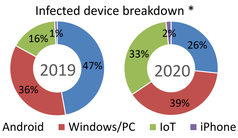
The growth of the number of Internet enabled-devices is majorly impacted by the M2M (viz. IoT) category *



*Cisco Annual Internet Report (2018-2023) White Paper

IoT devices are increasingly infected (e.g., by Mirai to form botnets)

Infected device breakdown *



*Nokia Threat Intelligence Report 2020

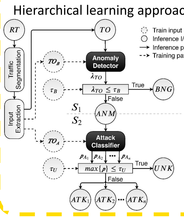
- Huge number of **new malwares and variants**
- **Resource-constrained** nature of IoT devices
- **Increasingly diffusion** of IoT in home networks

Need for an *unknown-aware, lightweight, scalable*, and *easily re-trainable* Intrusion Detection System

Proposed Solution [1]

Hybrid Hierarchical Intrusion Detection (H2ID) Approach

Hierarchical learning approaches enables *scalability* and *easily re-training* [2]



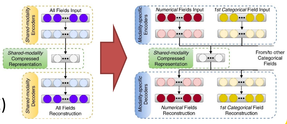
Stage 1 (S1) Anomaly Detection
Anomaly threshold (τ_B)
→ *Fast path for benign traffic*

Stage 2 (S2) Attack Classification
Censoring threshold (τ_U)
→ *Unknown class of attack*

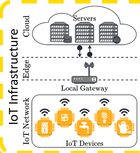
Lightweight Anomaly Detection Module

Exploiting different modalities reduces the number of neural connections

Extension of Deep AutoEncoder (DAE) [3] to Multi-modalities
→ *MultiModal Deep AutoEncoder* (M2-DAE)



Deployment Scenarios



Scenario A

S1 →

S2 →

Scenario B

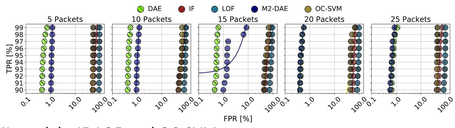
S1 → or

S2 →

Evaluation on BotIoT Dataset [4]

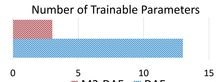
S1 evaluation: model choice

M2-DAE overperforms Machine Learning (ML) models and is lighter than the Deep Learning (DL) counterpart, i.e. DAE



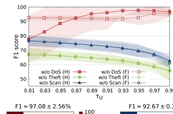
ML models: IF, LOF, and OC-SVM
→ > 40% FPR w/ high TPR

DL models: DAE and M2-DAE
→ < 1% FPR w/ high TPR
→ M2-DAE 4x less complex than DAE



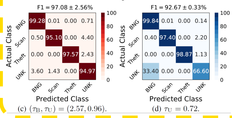
S1 + S2 evaluation: Hybrid Hierarchical vs Misuse Flat

H2ID is more effective than a flat approach in unknown detection



Fixed τ_B to obtain 1% FPR and each attack class per time as UNK

→ no differences for Theft and Scan
→ proposal (H) shows gain for DoS



Fixed τ_B and τ_U to obtain lowest FPR (≤1%) by fixing DoS as UNK

→ higher F1 score for proposal (red)
→ higher UNK hot-rate for proposal

Contacts
Email: giampaolo.bovenzi@unina.it
Wpage Unina:

Traffic Research Group
http://traffic.comics.unina.it

Future works will explore

- threshold design for specific use cases
- more classes of attacks (on new datasets)
- privacy-preserving distributed implementations of H2ID
- predictive- anomaly detection

References

[1] **Bovenzi, G.**, Aceto, G., Ciuonzo, D., Persico, V., & Pescapé, A. (2020) A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios. *GLOBECOM 2020 IEEE Global Communications Conference*.

[2] Montieri, A., Ciuonzo, D., **Bovenzi, G.**, Persico, V., & Pescapé, A. (2019). A dive into the dark web: Hierarchical traffic classification of anonymity tools. *IEEE Transactions on Network Science and Engineering*.

[3] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17* (3), 12-22.

[4] Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

Ph.D iTEE INFORMATION TECHNOLOGY ELECTRICAL ENGINEERING