ARES Conference
International Conference on Availability, Reliability and Security

The 15th International Conference on Availability, Reliability and Security (ARES 2020)

August 25 to August 28, 2020 in Dublin, Ireland

ID-86 workshop paper (IoT-SECFOR)

"TAXONOMY AND CHALLENGES IN MACHINE LEARNING-BASED APPROACHES TO DETECT ATTACKS IN THE INTERNET OF THINGS"

Universitat Oberta de Catalunya

CYBERCAT

Omair FARAJ – IN3, UOC, CYBERCAT, Spain

David Megías– IN3, UOC, CYBERCAT, Spain

Abdel-Mehsen Ahmad – LIU, BIU, Lebanon

Joaquin Garcia-Alfaro– SAMOVAR, Télécom SudParis, IMT & IP Paris, France

R&I IN3 Internet Interdisciplinary Institute

TELECOM SudParis

IP PARIS

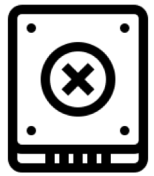
s@movar

1 Objectives

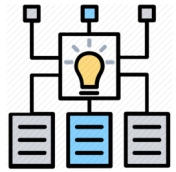
1. Survey recent IDS systems and methods for IoT networks based on ML
2. Analyze different aspects of study that should be taken into consideration during the design of an IDS for IoT
3. Propose an IDS taxonomy
4. Discuss open issues and research challenges with new security solutions.

2 Introduction

Challenges & Security issues in IoT networks



Restricted device capabilities



Presence of many standards

Limited computing power

High number of interconnected devices

Presence of malware, spyware and eavesdroppers

Critical infrastructures, such as transportation, healthcare systems and household appliances can lead to dreadful consequences when subject to attacks

2 Introduction

Security Solutions

Traditional security approaches and countermeasures → Cryptography...

These approaches may fail to defend IoT environments due to the mentioned challenges and vulnerabilities

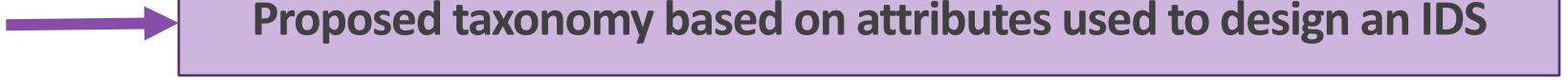
Intrusion Detection Systems (IDSs) are proposed and designed to detect these attacks and protect IoT networks overcoming restrictions

Assisted by  Machine Learning → Intelligent Tool to deal with Big Data

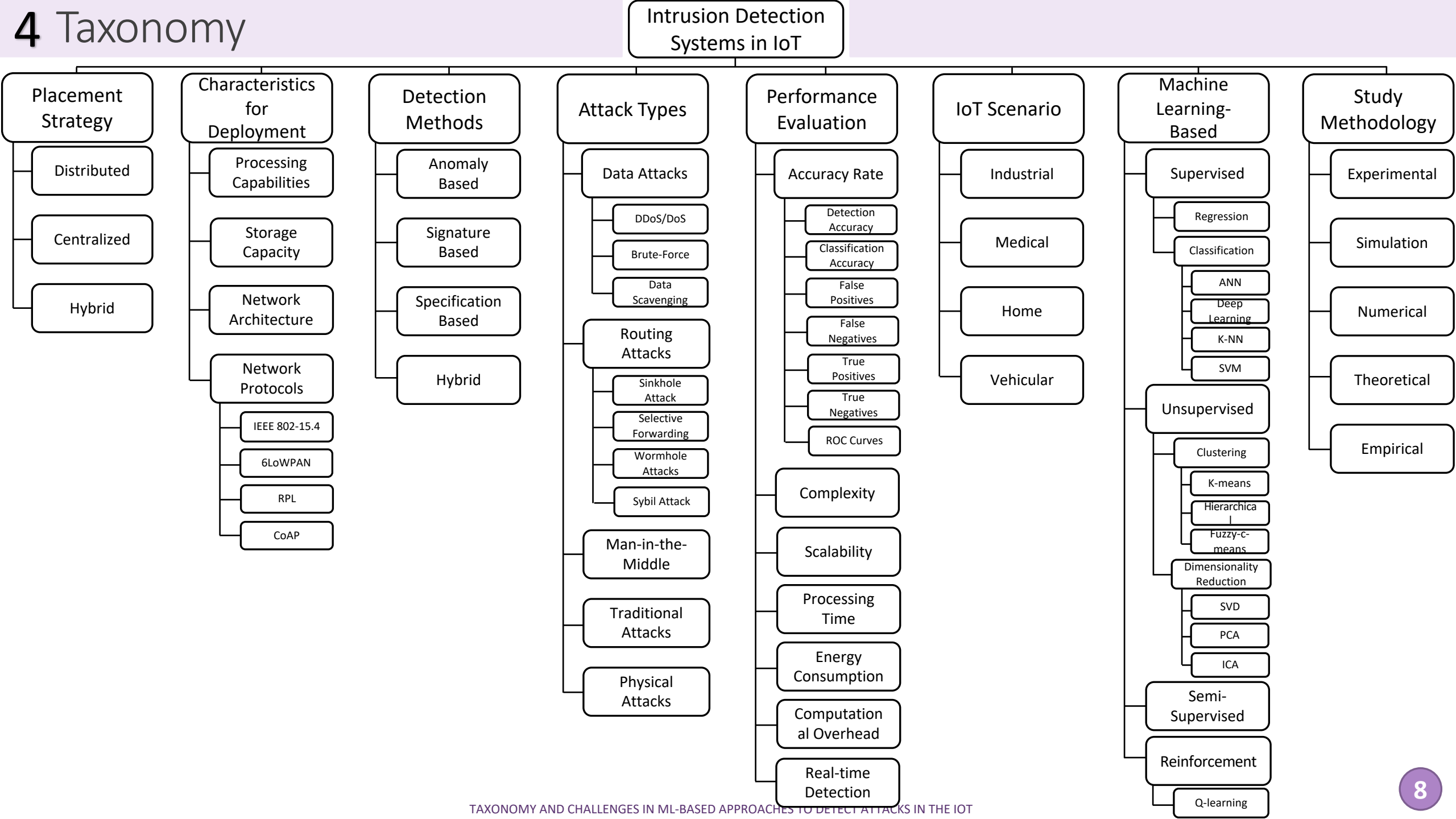
3 Related Work

1. Some reviews have been conducted regarding intrusion detection in the fields of cloud computing, Wireless Sensor Networks (WSN) and traditional networks.
2. Few surveys are focused on intrusion detection methods in IoT environments.
3. Most of the them overlook many aspects that are needed for studying an IDS.
4. These surveys are used to build our taxonomy & indicate missing aspects researchers must take into consideration while developing a new system.

4 Taxonomy


Proposed taxonomy based on attributes used to design an IDS

4 Taxonomy


Intrusion Detection Systems in IoT
Placement Strategy
Distributed
Centralized
Hybrid
Characteristics for Deployment
Processing Capabilities
Storage Capacity
Network Architecture
Network Protocols
IEEE 802-15.4
6LoWPAN
RPL
CoAP
Detection Methods
Anomaly Based
Signature Based
Specification Based
Hybrid
Attack Types
Data Attacks
DDoS/DoS
Brute-Force
Data Scavenging
Routing Attacks
Sinkhole Attack
Selective Forwarding
Wormhole Attacks
Sybil Attack
Man-in-the-Middle
Traditional Attacks
Physical Attacks
Performance Evaluation
Accuracy Rate
Detection Accuracy
Classification Accuracy
False Positives
False Negatives
True Positives
True Negatives
ROC Curves
Complexity
Scalability
Processing Time
Energy Consumption
Computational Overhead
Real-time Detection
IoT Scenario
Industrial
Medical
Home
Vehicular
Machine Learning-Based
Supervised
Regression
Classification
ANN
Deep Learning
K-NN
SVM
Unsupervised
Clustering
K-means
Hierarchica
Fuzzy-c-means
Dimensionality Reduction
SVD
PCA
ICA
Semi-Supervised
Reinforcement
Q-learning
Study Methodology
Experimental
Simulation
Numerical
Theoretical
Empirical

5 Intrusion Detection in IoT

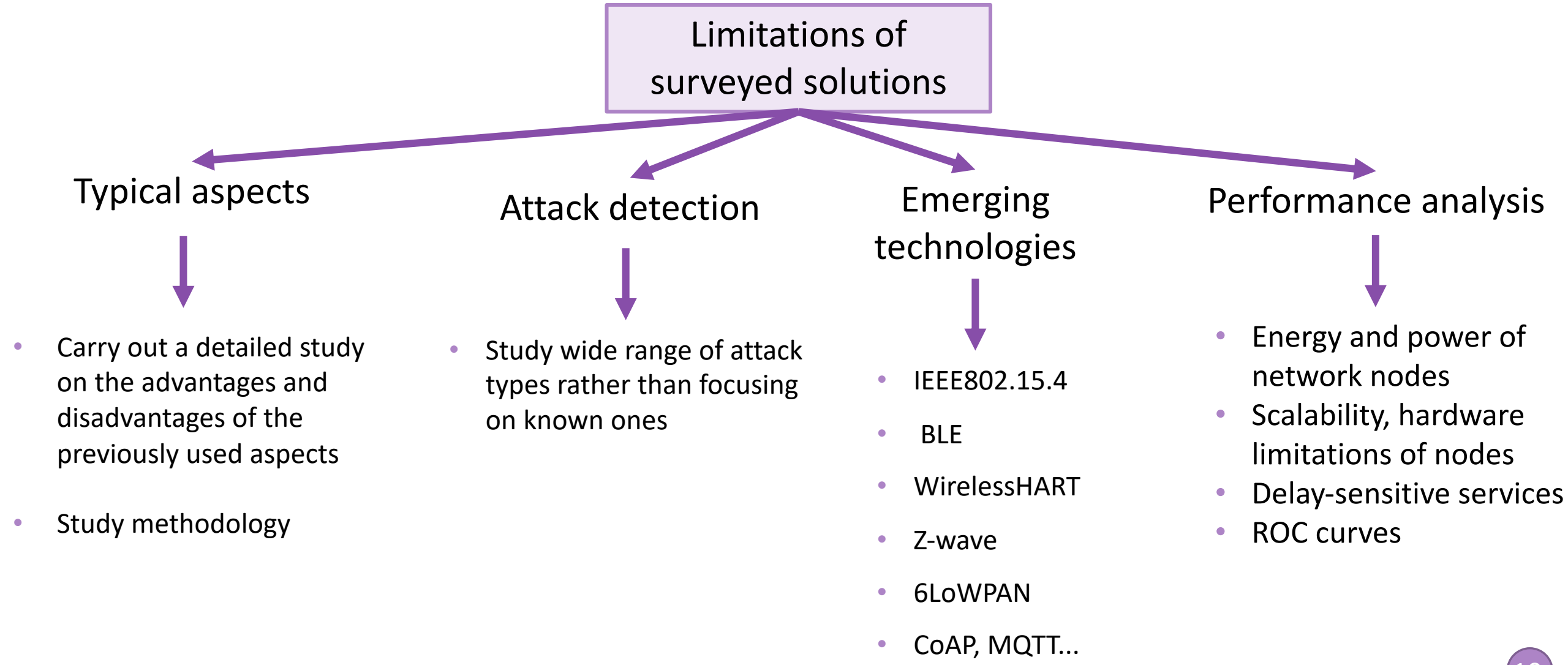
16 recent published papers from 2016 to 2019 were reviewed & classified, based on:

Two published papers as an example

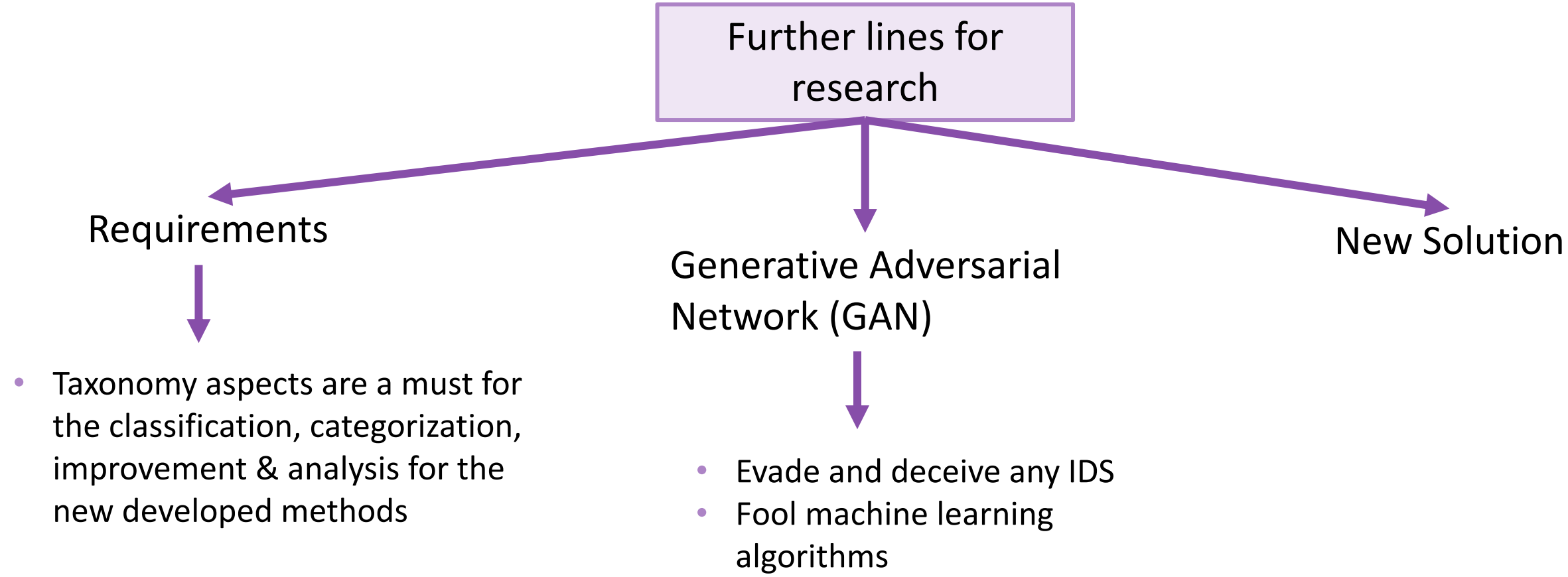
Ref	Method	Placement Strategy	Detection Method	Attack Type	IoT Scenario	Machine Learning	Study Methodology
[43]	Classifying normal and threat patterns in an IoT network using ML	Centralized	Anomaly-based	DDoS/DoS	-	NN	Simulation
[44]	Detecting Suspicious activities in home devices using Open-Flow	Centralized	Signature-based	Routing attacks, man-in-the-middle	Home	Regression , SVM	Experiment

Ref	Detection Accuracy	Classification Accuracy	TPR	FPR	TNR	FNR	ROC curves	Processing time	Energy consumption	Computation overhead	Real-time detection
[43]	-	99%	99.4%	0.6%	-	-	-	-	-	-	Offline
[44]	94.25%	85.05%	35.47%	5.74%	-	-	-	-	-	-	Real-time

6 Open Issues and Research Challenges



6 Open Issues & Research Challenges



6 Open Issues & Research Challenges

Further lines for research

New Solution → **Challenge-response mechanisms**

Watermarking

- Lightweight
- Less energy consumption
- Implement anomaly detection
- Solution for: data integrity, confidentiality, secure transmission, authentication, etc.
- No additional overhead on network communication and storage capacity of nodes
- Reduce end-to-end delay

7 Conclusion & Recommendations

- Due to weak designs, low computational capabilities, and faulty protocol implementations found in IoT networks, traditional security techniques cannot be implemented
- Intrusion Detection Systems (IDSs) are designed to detect malicious activities to protect IoT networks
- Enormous quantity of data generated in these networks lead to the need of intelligent tools to assist IDSs (Machine Learning)
- IDSs need to study detection rates, false positive rates, real-time detection, computation overhead and energy consumption in a combined manner
- Researchers must consider all aspects while designing and implementing a new IDS

7 Conclusion & Recommendations

- More research should be conducted to cover all attack types and recent IoT technologies
- Research efforts are needed to find the optimal placement strategies to compute machine learning-based detection that could benefit to the security of IoT networks
- Watermarking algorithms are recommended to be deployed that are much lighter and require less power, storage and computational capabilities