Node Compromising Detection to avoid Poisoning Attacks in IoT Networks

Ph.D. Student : Floribert KATEMBO VUSEGHESA

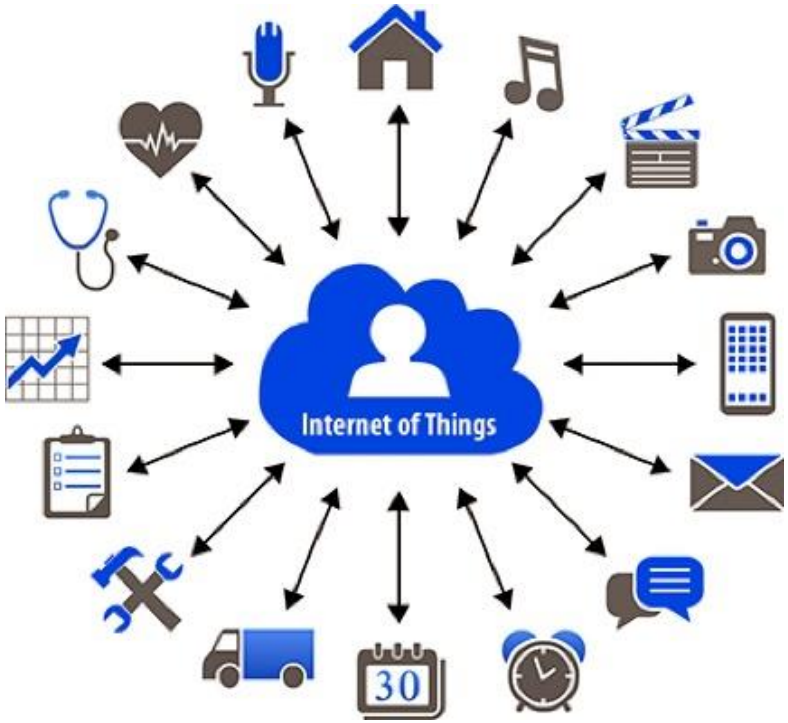
Supervisors : Fadila BENTAYEB et Mohamed-Lamine MESSAI

ERIC Laboratory, Lyon University, France

Content

Context

IoT networks ?



Objectives

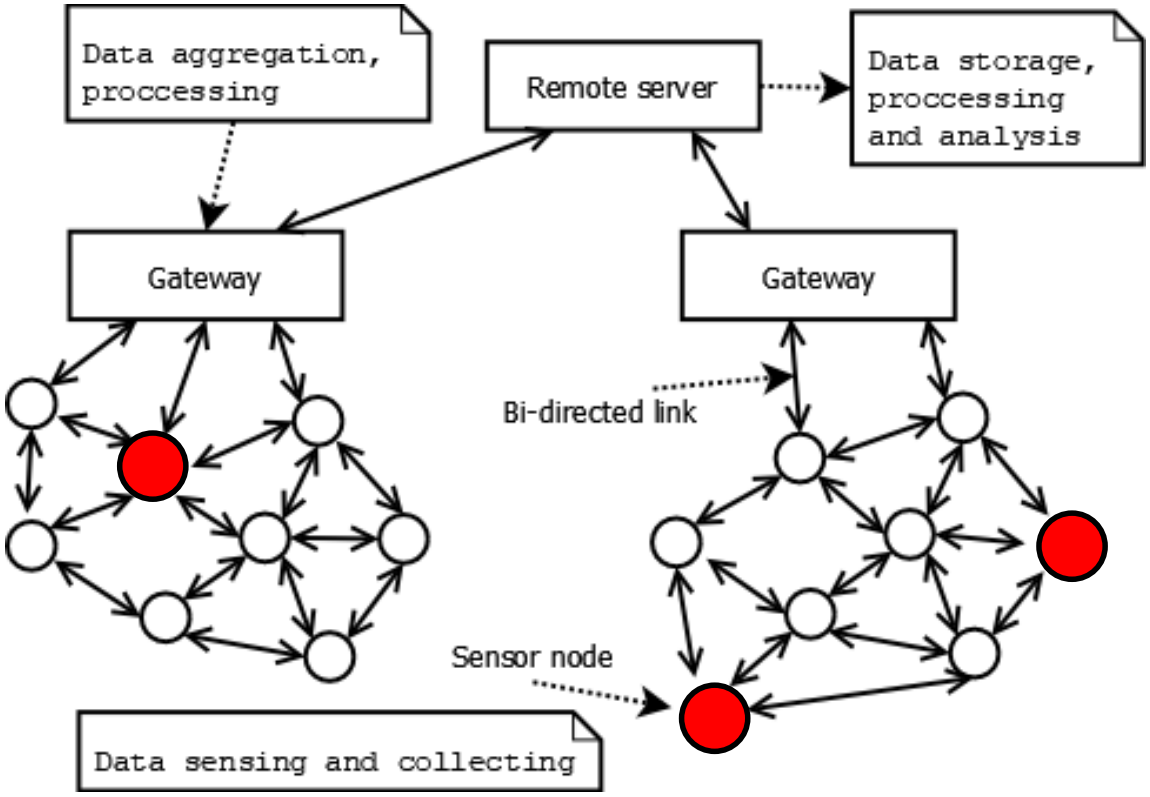
- Collection, analysis and sharing data in real-time
- Aid to decision-making
- Improving efficiency in various fields

Problems

Target of various types of attack

- Physical Attacks
- Node compromise attacks
- Black / grey hole attacks
- Sybil attacks
- Clone attacks, …

A model of IoT networks



Example of an IoT system model incorporating a compromised node detection technique.

The threat model

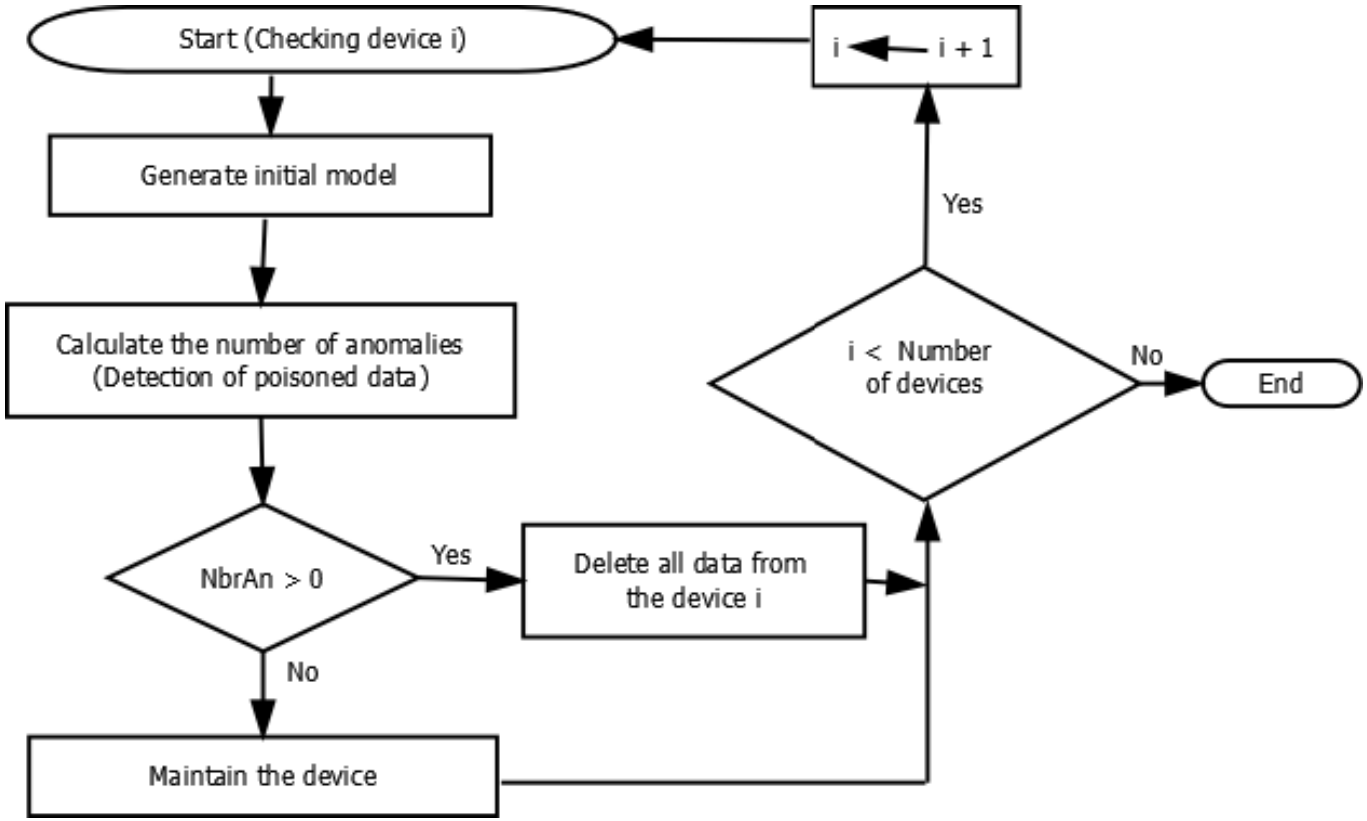
- We suppose that an attacker can capture and compromise IoT nodes within the network
- He/she injects manipulated values into the sensed data transmitted by compromised nodes

Overview of the method

Method name is NoComP (*Node Compromising detection*) with 3 main stages :

1. Model initialization
2. Data analysis
3. Node compromising detection

Overview of the method



Flowchart of NoComP

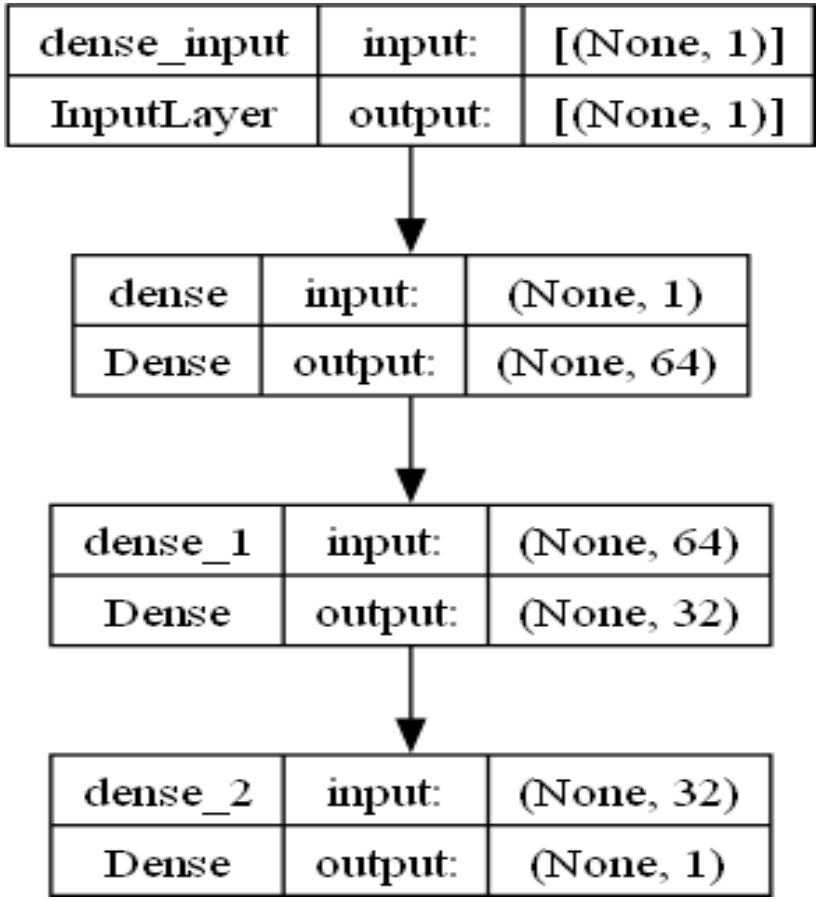
Choice of algorithm : MLP-Multilayer Perceptron

MLPs are powerful deep learning models that can be used for a variety of machine learning tasks

- Ability to efficently manage complex, high-dimensional data

- Ability to learn complex data representations using multiple layers of hidden neurons
- Flexibility that allows them to be used for different types of supervised learning tasks

Architecture of the neural network used



MLP architecture

3 layers are connected to each other: input layer (64 neurons), hidden layer (32 neurons), output layer (1 neuron)

This model follows a sequential architecture in which data passes from the input layer to the output layer via hidden layers, without any upward connections

Datasets used :

1. Temperature data from *OpenML*

- A real IoT network made up of devices that record temperature
- This dataset contains 5 columns and 97606 rows of data

2. Humidity data

- This data was collected by AWS IoT services
- The dataset contains telemetry data
- The dataset contains 9 columns and 405184 rows of data

Implementation and testing

- Create a python script to train the model on the two types of data
- Compromised IoT nodes are selected randomly
- They send false data to poison the database

The efficiency

- Choice of metrics: ROC-AUC, Precision, F1-Score
- Balance to be struck between true and false positives and also between true and false negatives

The efficiency

Types of data	*ROC-AUC*	*Precision*	*F1-Score*	*Efficiency%*
Poisoned	0.76	0.59	0.58	**64.3**
Cleaned	0.50	0.95	0.98	**80.6**

Comparison of scores before and after the elimination of compromised nodes from the model trained on temperature data

The efficiency

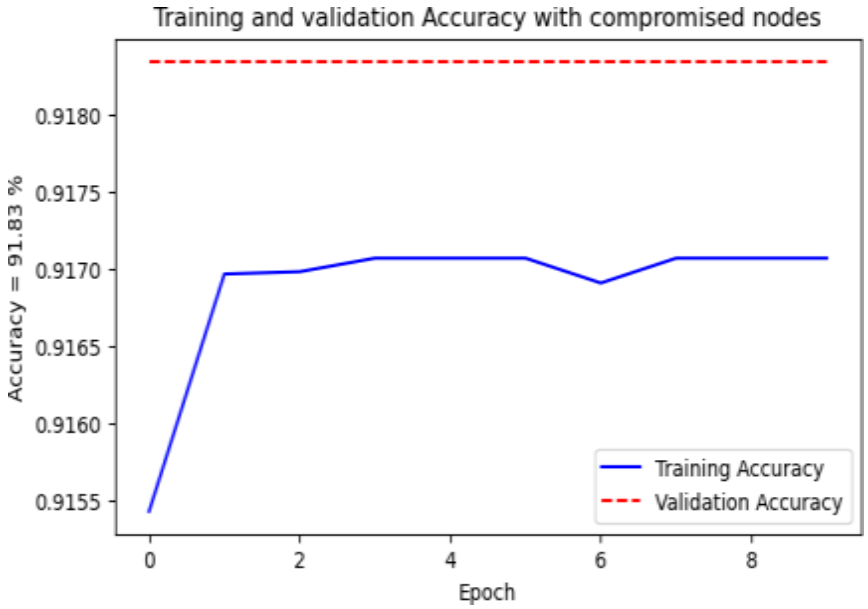
Types of data	*ROC-AUC*	*Precision*	*F1-Score*	*Efficiency%*
Poisoned	0.74	0.59	0.58	**63.6**
Cleaned	0.50	0.92	0.96	**79.3**

Comparison of scores before and after the elimination of compromised nodes of the model trained on the humidity

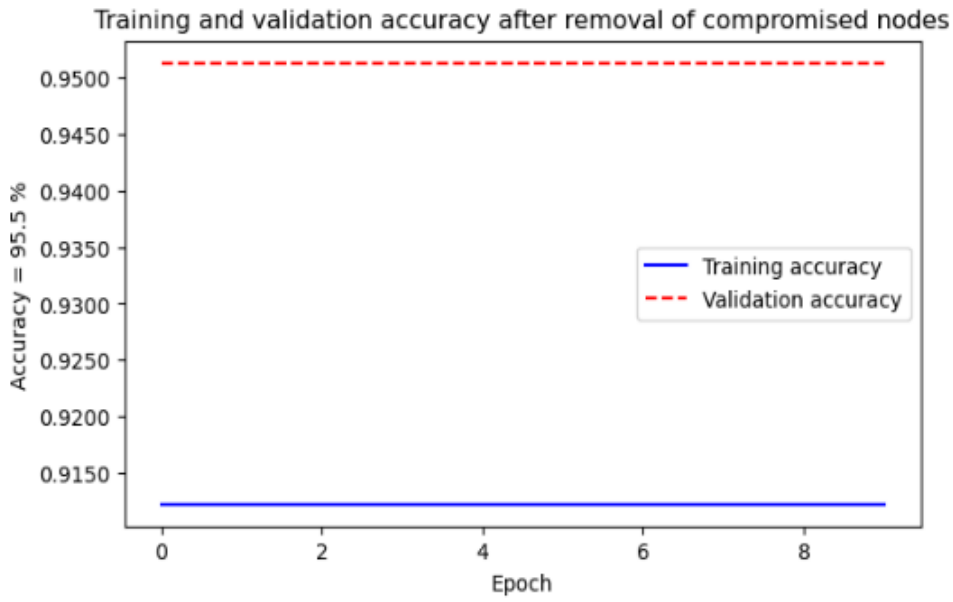
The accuracy

- **Training accuracy** measures the model's precision on training data
- **Validation accuracy** measures the accuracy of the model on a validation dataset, which is separate from the training dataset.

The accuracy

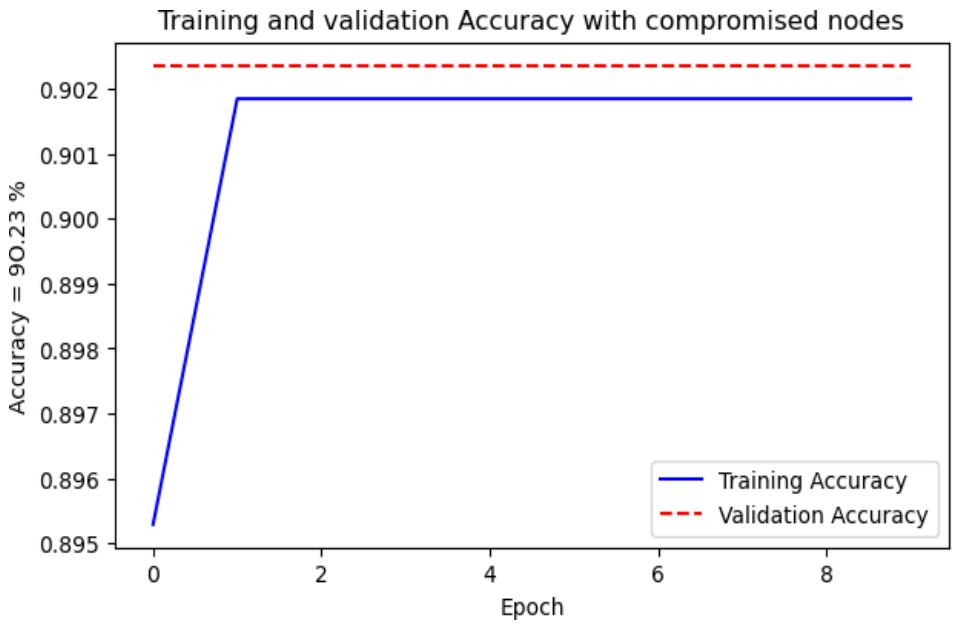


(a) On poisoned temperature data.

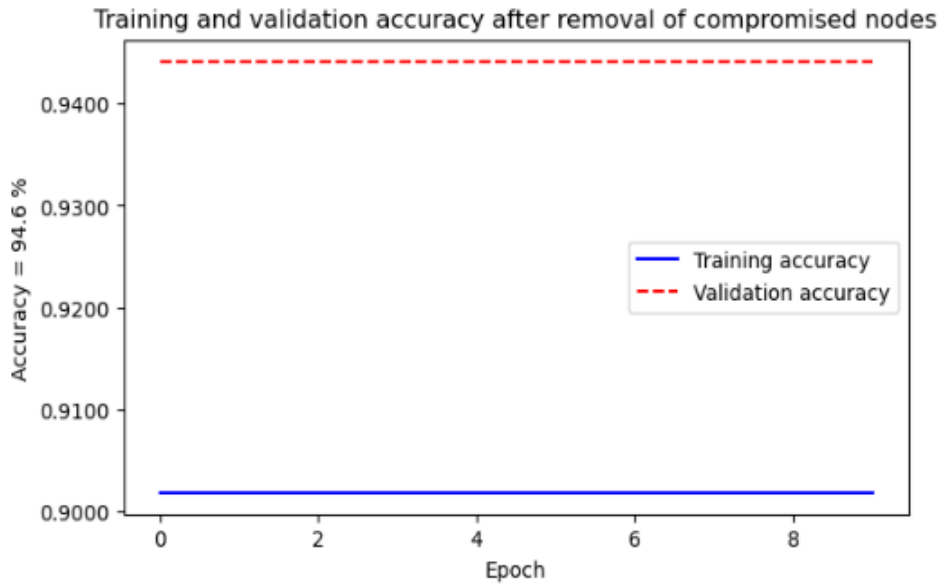


(b) On Cleaned temperature data.

The accuracy



(c) On Poisoned humidity data



(d) On Cleaned humidity data

Summary of existing and proposed methods :

Authors	Algorithms	Types of data	Efficiency %	Accuracy %
Baracaldo et al.(2018)	SVM	MNIST	**65**	**83**
Chiba et al.(2021)	SVM	MNIST, IoT	**65**	**89**
F.K. Vuseghesa (*NoComP*)	Neural Network	IoT	**80**	**93**

Performance comparison between existing and proposed methods.

Conclusion

- NoComP : a method to detect compromised nodes within IoT networks
- Goal : to enhance the security of IoT systems by identifying compromised nodes to avoid poisoning attacks

- Comparison : NoComP improves the detection efficiency of poisoned data and the accuracy of the model by over 93% after detecting and deleting compromised nodes
- Future work : Evaluation of NoComP by testing it on a broader range of IoT datasets and comprehensive comparison with more existing methods

...

Thank you for your attention!