Impact and Detection of Synchronization Attacks on Distributed and Cooperative Control of Microgrids

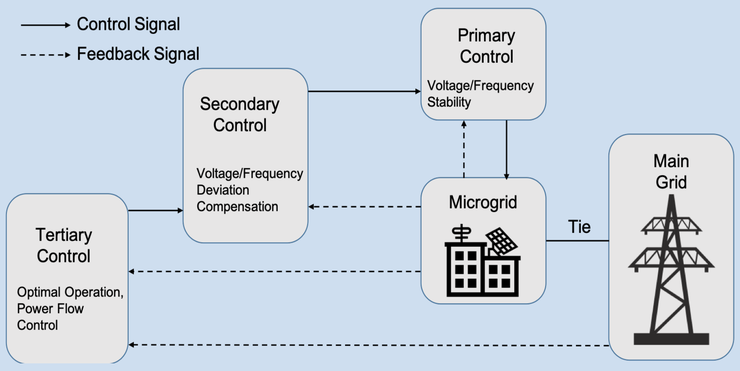
Mingxiao Ma, Abdelkader Lahmadi, Isabelle Chrisment
Université de Lorraine, CNRS, Inria, Loria, F-54000 Nancy, France

Overview

Microgrid platforms are subject to several threats because of the widely use of communication networks in their control layers. Hereby we propose the impact assessment and detection of a novel attack, named **Measurement as Reference attack (MaR)**, on the distributed control mechanism of a microgrid, where an attacker replaces the reference values with measurements during its synchronization operations.

Background and Motivation

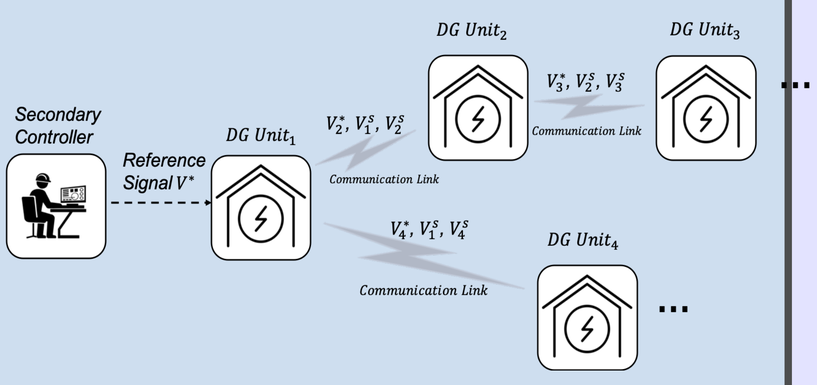
Control structure of a Microgrid



The task of the microgrid control system

- Regulate voltage and frequency for different operating modes
- Achieve proper load sharing among DGs
- Control the power flow between the main grid and the microgrid
- Optimize the cost of its operations

Distributed cooperative control model of microgrid system



- Primary control: voltage quadratic droop controller, i.e., the voltage dynamics of each DG unit is modeled as a single integrator
- Secondary control: modeled as a *tracking problem* in cooperative control

Motivation: security concerns

- Increasing penetration level of DGs and widely use of communication networks introduce new security vulnerabilities
- There exist various cyber attacks targeting system availability and reliability and transmitted data integrity
- Countermeasures: attack detection, mitigation, prevention

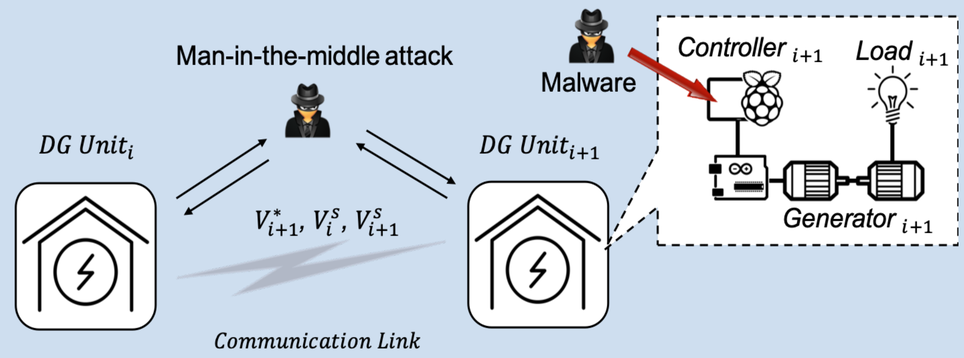
Acknowledgements

This work has been funded by the French Government under grant FUI 23 PACLIDO (Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets).

MaR Attack Model

Measurement as reference (MaR) attack

In a measurement as reference attack on the communication link between DG unit i and $i+1$, the attacker manipulates the exchanged data by replacing the reference signal $V_{i+1}^*(t)$ for DG unit $i+1$ with the voltage measurement $V_i^s(t)$ of DG unit i



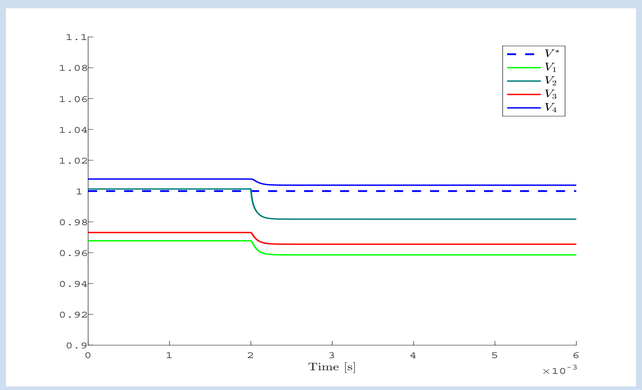
MaR with a man-in-the-middle attack

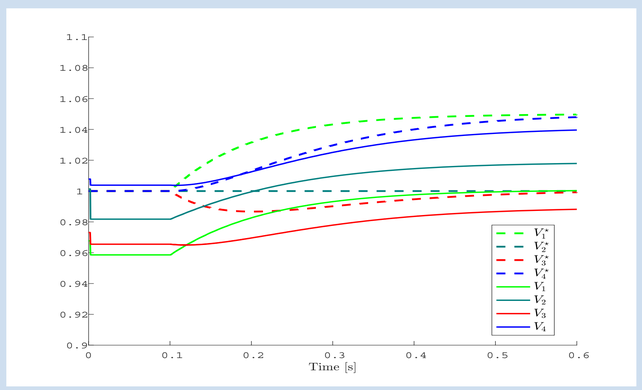
- The communications between DGs are not encrypted.
- Only neighbouring nodes exchange data through the communication link between them.
- ARP poisoning is used to allow the attacker to introduce itself into a communication between two DG units and acts as relay/proxy, impersonates both nodes and gets access to the reference and measurements values that the two nodes are sending to each other.

Attack Impact and Detection

Attack Impact:

- **Attack Impact on Voltage Deviation.** The attack causes voltage deviation at each DG unit, which is a short-term impact on the primary control. The voltages reach a stable state again very quickly.
- **Impact on Reference Voltage Synchronization.** The affected DG 2 and DG 3 no longer reach the consensus V^*, which could lead to a heavy impact on voltage regulation in a microgrid system.





Attack Detection based on machine learning algorithms:

- The ROC curves show that Random Forest has an $AUC = 0.99$, which is larger than any other algorithms. It means that it has 99% chance that model will be able to distinguish between positive class and negative class. Naive Bayes has the relatively worse performance in terms of three metrics. SVM has the best performance in terms of precision, however, Random Forest has the best performance in terms of recall and accuracy. As a result, we find that a detection method based on Random Forest has the best performance.

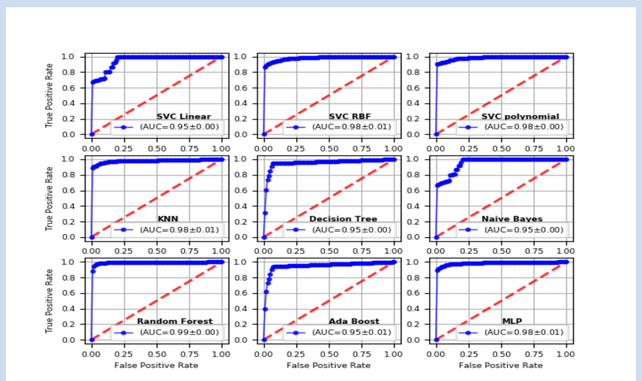


TABLE I: Performance of the different attack detection algorithms.

Detection algorithms	Precision	Recall	Accuracy
Threshold Comparison ($\delta = 0.3$)	0.39	0.32	0.53
Ada Boost	0.93	0.94	0.96
Decision Tree	0.93	0.94	0.95
KNN	0.99	0.88	0.96
Multi Layer Perceptron	0.97	0.87	0.95
Naive Bayes	0.79	0.72	0.83
Random Forest	0.96	0.95	0.97
SVC Linear	0.74	0.85	0.84
SVC polynomial	1.00	0.85	0.95
SVC RBF	1.00	0.82	0.94

References

M. Ma and A. Lahmadi, **On the Impact of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems**, in IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, Aalborg, Denmark, Oct. 2018.