A Framework for Counterfeit Smart Grid Device Detection

Leonardo Babun, Hidayet Aksu, and A. Selcuk Uluagac
Cyber-Physical Systems Security Lab (CSL)
Electrical & Computer Engineering Department
Florida International University
E-mail: {lbabu002, haksu, suluagac}@fiu.edu

Abstract

The core vision of the smart grid concept is the realization of reliable two-way communications between smart devices (e.g., IEDs, PLCs, PMUs). The benefits of the smart grid also come with tremendous security risks and new challenges in protecting the smart grid systems from cyber threats. Particularly, the use of untrusted counterfeit smart grid devices represents a real problem. Consequences of propagating false or malicious data, as well as stealing valuable user or smart grid state information from counterfeit devices are costly. Hence, early detection of counterfeit devices is critical for protecting smart grid's components and users. To address these concerns, in this poster, we introduce our initial design of a configurable framework that utilize system call tracing, library interposition, and statistical techniques for monitoring and detection of counterfeit smart grid devices. In our framework, we consider six different counterfeit device scenarios with different smart grid devices and adversarial settings. Our initial results on a realistic testbed utilizing actual smart-grid GOOSE messages with IEC-61850 communication protocol are very promising. Our framework is showing excellent rates on detection of smart grid counterfeit devices from impostors.

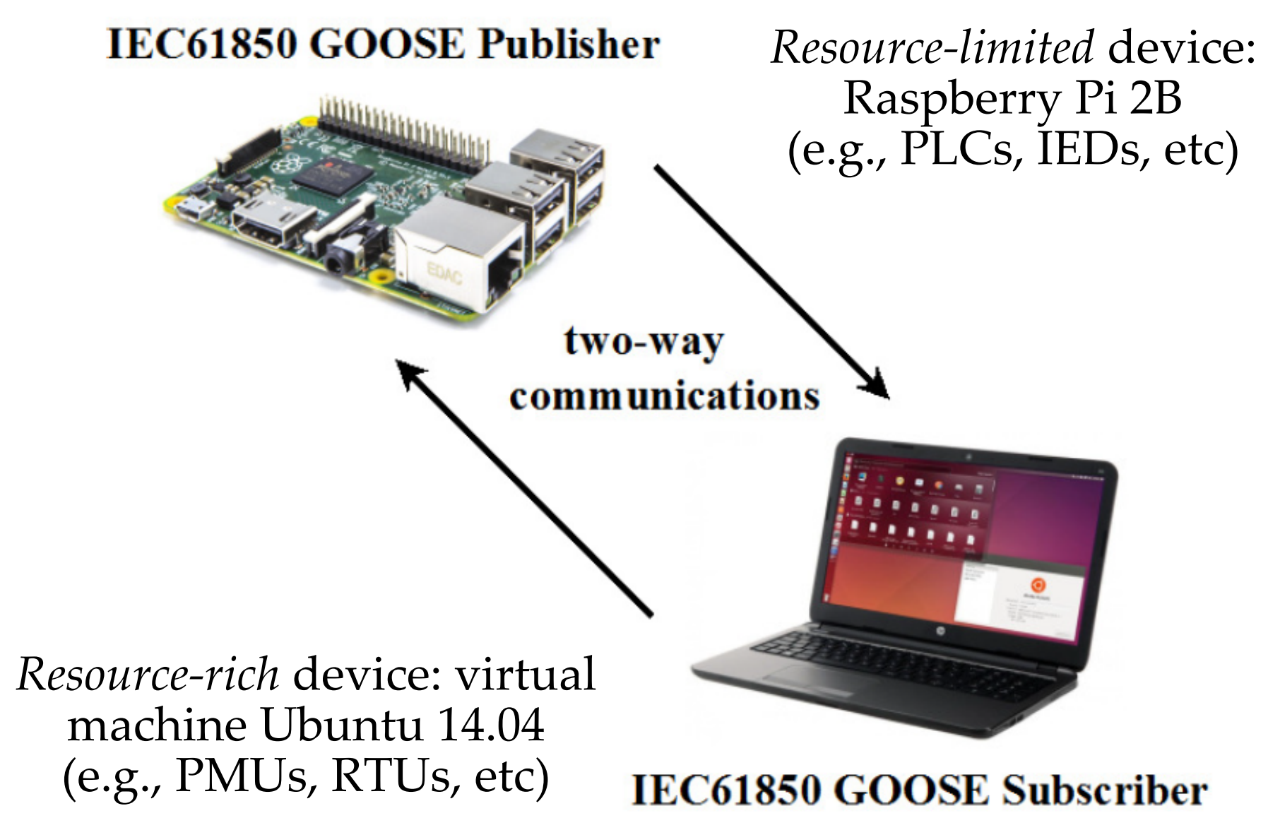
Introduction

The use of untrusted counterfeit devices could negatively impact the smart grid performance and could be catastrophic for the integrity of the power grid and/or user's privacy.

We propose a configurable framework that is capable of detecting counterfeit devices which are performing unauthorized operations inside critical parts of the smart grid architecture.

We utilize system call tracing , library interpolation, and statistical techniques to monitor and detect counterfeit device behavior.

The proposed testbed includes resource-limited (e.g., IEDs, PLCs) and resource-rich (e.g., PMUs, RTUs) devices that follow a GOOSE publisher-subscriber configuration using open source libiec61850 libraries.



Adversary Model (I)

Information leakage
- the counterfeit smart grid device can open additional communication channels simultaneously to leak information from the fake device.

Store-and-send-later
- the fake device can store and hide information in files that can be recovered later by the attacker.

Poisoning real measurements
- malicious code can generate fake data that can be used to poison the real status of the smart grid.

Adversary Model (II)

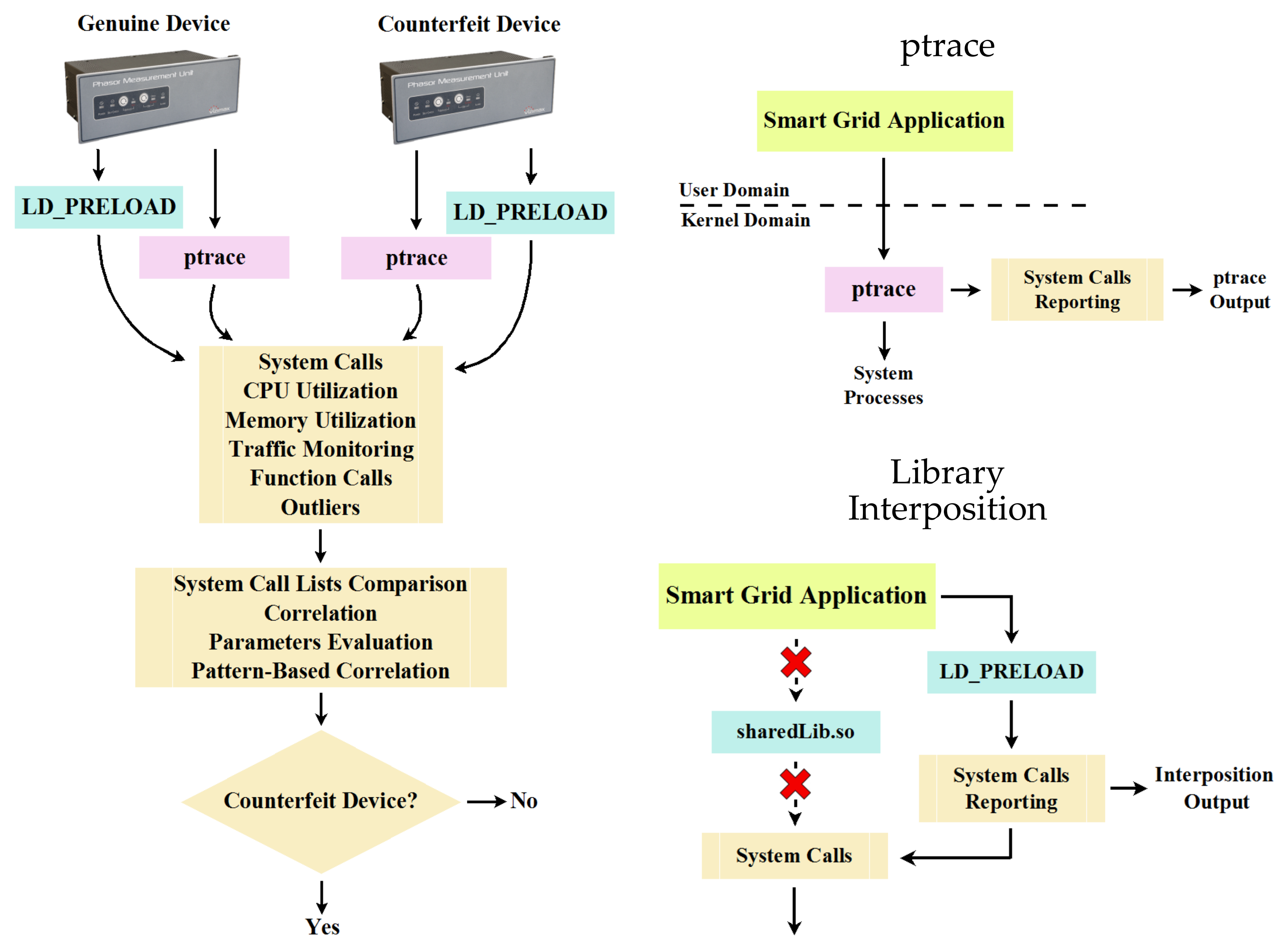
Name	Resource availability	Impact
CD_1	Limited	Memory, communications
CD_2	Limited	Memory, data,
CD_3	Limited	Memory, confidentiality
CD_4	Rich	Memory, communications
CD_5	Rich	Memory, data
CD_6	Rich	Memory, confidentiality

Malicious code performs its attacks following a Poisson distribution where the probability of having an attack is:

$$P_{cd} = \frac{\lambda^k e^{-\lambda}}{k!}, \quad k \in \mathbb{R},$$

where:
λ - average number of attacks during interval *t*
k – total number of attacks during interval *t*

Overview of Our Framework



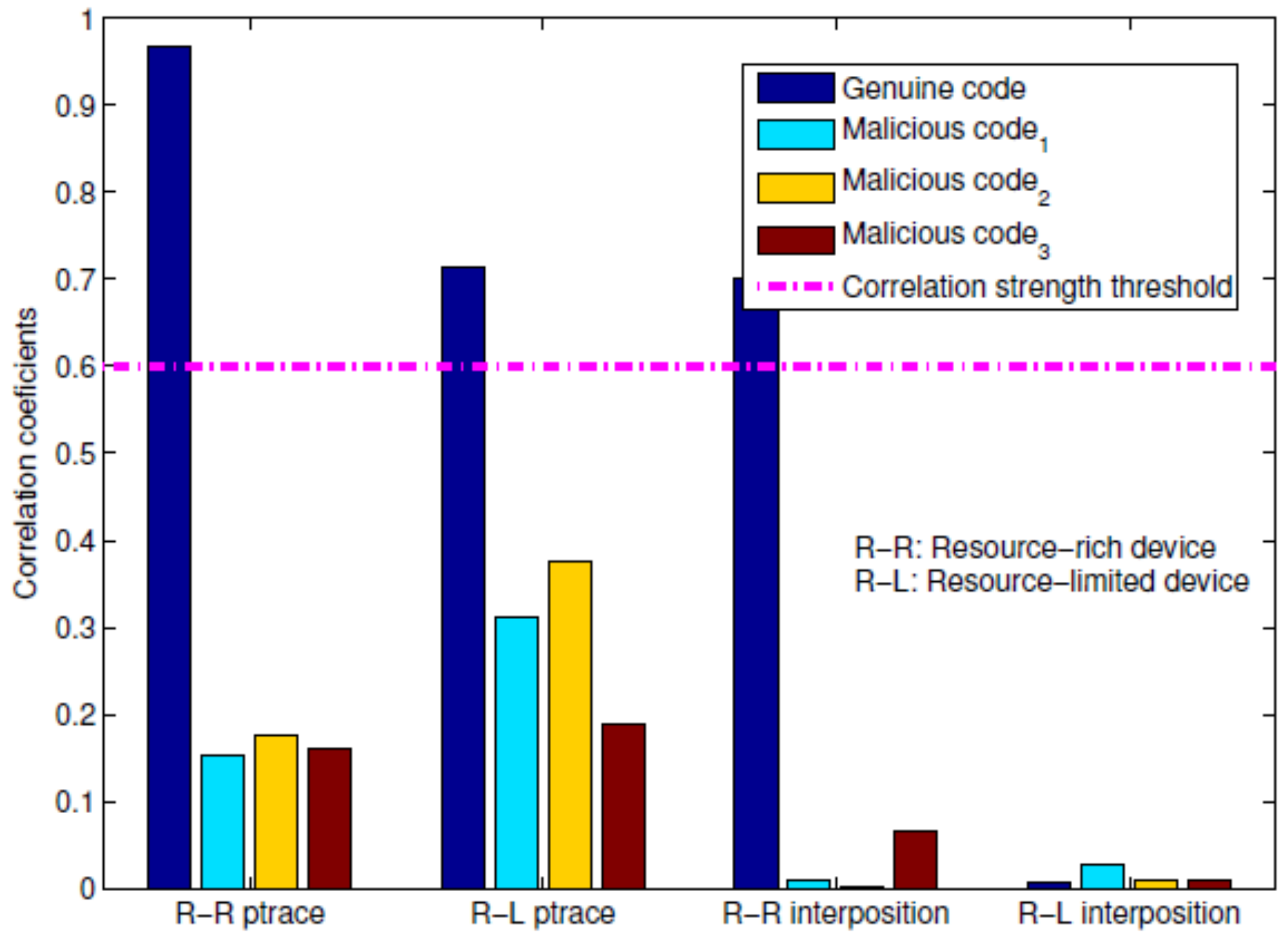
•By using system call tracing techniques and library interposition, our framework would be more adaptive and configurable for a wider range of different type of devices so it can be used in more realistic scenarios.

Three different detection techniques are proposed: (1) system calls comparison, (2) statistical correlation simple, and (3) statistical correlation advanced

Performance Analysis

	Type of call	Gen.	Mal. 1	Mal. 2	Mal. 3
ptrace	*mmap2*	1	2.4	4.4	2.4
	mprotect	1	2.8	1.1	1
	munmap	1	1	2	13
	open	1	1	1	5
	rt_sigaction	1	1	3	3
Interposition	*mmap*	1	12.5	1	1
	mprotect	1	12.5	1	1
	pthread_create	1	12.5	1	1
	sendto	1	4.3	~1	~1
	signal	1	24	1	1

Normalized rate of system calls detected in our framework for resource-limited devices (e.g. IEDs, PLCs)



Correlation between genuine and malicious codes for both resource-rich and resource-limited type of counterfeit devices after using our framework.

Acknowledgements

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000779.

References

[1] NIST Special Publication 1108r3, "NIST framework and roadmap for smart grid interoperability standards, release 3.0," Sep 2014. [Online] Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r3.pd
[2] http://financialspots.com/2016/01/11/smart-grid-a-grid-suitable-for-renewable-energy/
[3] http://www.nist.gov/smartgrid/upload/nistir-7628 total.pdf