MITIGATION OF MAN-IN-THE-MIDDLE ATTACKS ON PLCs

MTP-II report submitted to

Indian Institute of Technology Kharagpur

In partial fulfilment for the award of the degree of

Master of Technology In

Electronics and Electrical Communication Engineering

By

Sudarshan Biswas

(18EC35052)

Under the supervision of

Dr. Debdeep Mukhopadhyay

Department of Electronics and Electrical Communication Engineering

Indian Institute of Technology Kharagpur

Autumn Semester 2022-23

November 2022

DECLARATION

I certify that

I. The work contained in this report is original and has been done by me under the guidance of my supervisor.

II. The work has not been submitted to any other Institute for any degree or diploma.

III. I have followed the guidelines provided by the Institute in preparing the report.

IV. I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.

V. Whenever I have used materials (data, theoretical analysis, figures, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references. Further, I have taken permission from the copyright owners of the sources, whenever necessary.

Sudarshan Biswas

CERTIFICATE

This is to certify that the report entitled, "**Mitigation of Man-in-the-middle attacks on PLCs**" submitted by **Sudarshan Biswas (18EC35052)** to the Indian Institute of Technology Kharagpur, India, is a record of bonafide project work carried out by him under my supervision and guidance towards partial fulfilment of requirements for the award of degree of Master of Technology in Electronics and Electrical Communication Engineering.

Date: Signature of the Supervisor

(Dr. Debdeep Mukhopadhyay)

Contents

Chapter 1

Introduction

Industrial control systems (ICS) interconnect, control and monitor industrial environments such as electrical power generation, transmission and distribution, chemical production, oil and gas refining and transport, and water treatment and distribution. Over the years ICS have seen widespread use in industries due to their ease of use, control, and versatility. Since most industries have started adopting ICS and are integrating it into IoT systems, vulnerabilities and other security concerns need to be addressed due to their exposure to the network and thus inevitably to Cyber Physical/ Hardware Attacks. Especially since ICS are often connected to critical infrastructures.

These security vulnerabilities lead to attacks including malware injection that modifies the software state of an embedded system. One such recent attack was the Stuxnet worm used against Iranian nuclear enrichment facilities which goes to show how targeted hardware attacks on ICS can cause catastrophic failures with substantial impact.

Traditionally, ICS security has been handled by IT and Network security practices. However, the security goals of traditional IT security and ICS vary due to additional requirements and conditions of operation. The interconnection of physical systems and cyber systems (CPS) is a special feature of ICS which is not accounted for in traditional IT.

1.1 ICS System Model

ICS is a distributed system which consists of physical systems like sensors and actuators which interact with the physical systems and cyber components. Although ICS are self-contained (generally) interfaces exist for external agents to monitor/ alter the functionalities. For example, an employee may observe and interact with the ICS using a Human Interface Machine (HMI) which is connected to the network on Programmable Logic Controllers (PLC) using ethernet and thus, are part of a network. In turn the PLCs are connected to the sensors/ actuators which do the actual physical interfacing. Figure 1.1 portrays the system model.

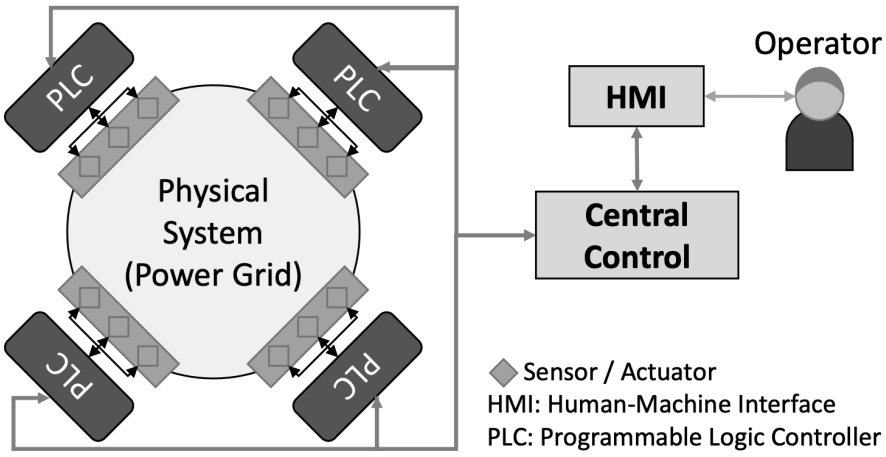

Fig 1.1: ICS System Model [1]

1.1.1 Programmable Logic Controllers

PLC are the main devices of interest in this entire report. PLCs are cyber-physical systems which are used to control industrial systems. They interact with the physical actuators/sensors and using their pre-programmed control logic, control them. PLCs act as the interface between these physical components and central control and all communication between them is facilitated by the PLCs. The PLC can be thought of to have three levels after it's abstraction. The control logic, firmware and its hardware components as shown in figure 1.2.

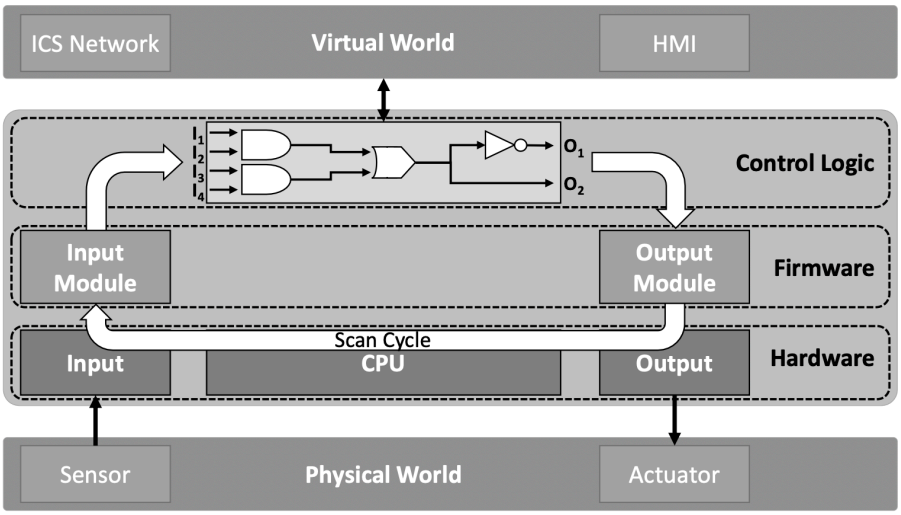

Fig 1.2: PLC Architecture [1]

The firmware acts and kind of Operating System and contains the functionality to read/write to/from the physical systems among other things. It can be thought of to have the drivers necessary to write/read data from the physical system (GPIO ports is available) to/from the memory.

The control logic can be thought of to be the application layer which reads data from the memory and writes it to the memory depending on the task it has been programmed to do.

1.2 Adversary Model

The main properties of the attack adversary should be:

(a) Stealthy: The sensor readings observed by the central control/ HMI should align with the expected values. This also means that it is assumed that the operator has no direct way of observing the system being controlled by the ICS i.e. lack of line-of-sight or other observational methods. Stealthiness will help in prolonging the presence of the malware in the system and thus maximise the damage caused.

(b) PLC exclusive attack: The attack should target only the PLCs of the ICS and not the other components like central

control/HMI. This is done because HMIs have intrusion-detection mechanisms and the risk of detection increases with increase in number of HMIs infected.

(c) Physical model information: The malware works on the basis that the physical/operational model of the ICS can be extracted so that it can be used to maintain (a) i.e the stealthiness of the attack because showing the expected values to the observation system necessitates knowing the working model of the system.¶

Chapter 2

HARVEY

Considering all of the aforementioned properties, HARVEY [1] was designed. It's central property is the physics awareness of the ICS it is attacking. Due to this property it gains unique capabilities wrt the virtual ICS world, the biggest one being undetectable by intrusion-detection systems and also the human operators (assuming that the operators are in out-of-band channel). This property alone makes it uber-powerful and goes beyond any traditional attack.

HARVEY lies in the firmware of the PLC and hence has access to reading and writing to the control logic of the PLC and the physical actuators/sensors. Because it lies in the firmware and

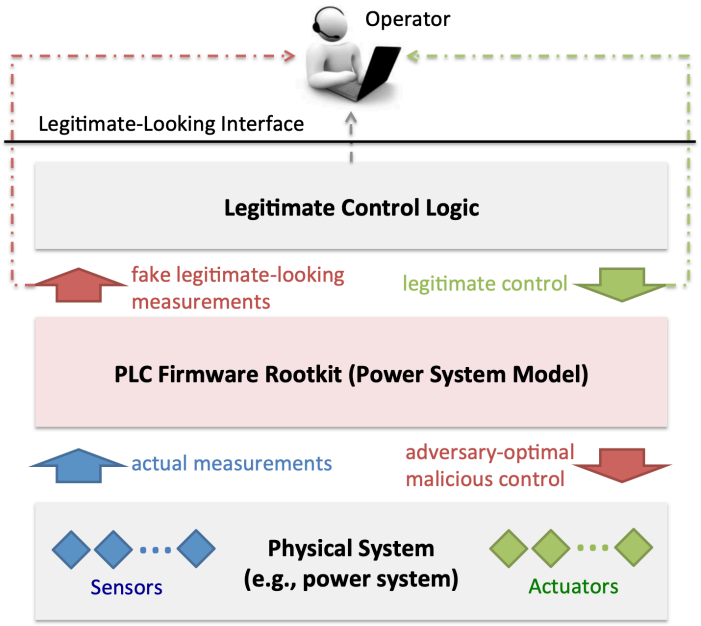

Fig 2.1: HARVEY infected PLC control flow [1]

controls all information flow in the firmware, it is completely invisible to the central control. It writes arbitrary values to the actuators, maximising it's effect and alters the sensor readings thus hiding it's activity. Fig 2.1 shows the control flow diagram of a HARVEY infected PLC. The model awareness helps in manipulating the inputs and the outputs to and from the PLC. This way, it can feed the expected input to the cyber world while manipulating the physical world: complete secrecy.

There are many methods of injecting this rootkit into the firmware of a PLC which we shall not be delving into right now because that is outside the scope of my project. To briefly summarise, firmware updates, JTAGs and physical access can be used to infect the PLC.

Chapter 3

Real Time Pricing Model

Modern information and communication technologies used by smart grids are subject to cybersecurity threats. Real-time pricing (RTP) is a key feature of smart grids that uses such technologies to improve system efficiency. Recent studies have shown that RTP creates a closed loop formed by the mutually dependent real-time price signals and price-taking demand. Such a closed loop can be exploited by an adversary whose objective is to destabilise the pricing system. Specifically, small malicious modifications to the price signals can be iteratively amplified by the closed loop, causing inefficiency and even severe failures such as blackouts.

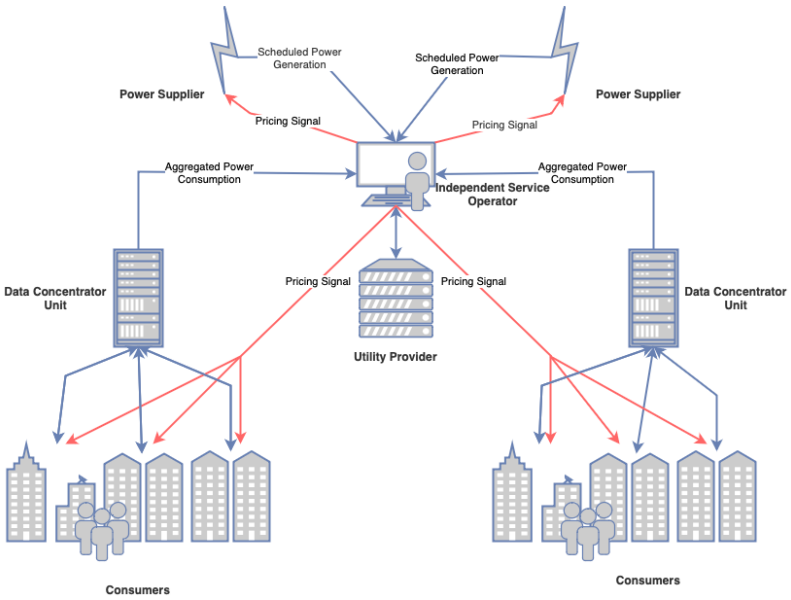

Fig 3.1: Smart Grid system with an ISO

One solution is to consider an Independent System Operator (ISO) which is a profit neutral agent that aims to balance overall supply and demand. This agent periodically establishes a pricing signal and shares it with the suppliers and consumers. Here, the market model explicitly relays RTP signals to end-users. Figure 3.1 depicts a generic Smart grid system consisting of individual and building loads from the consumer side, power generation units and a closed-loop pricing system.

For easier analysis, this closed loop RTP system can be simplified into a control-theoretic model which has been showcased in figure 3.2.

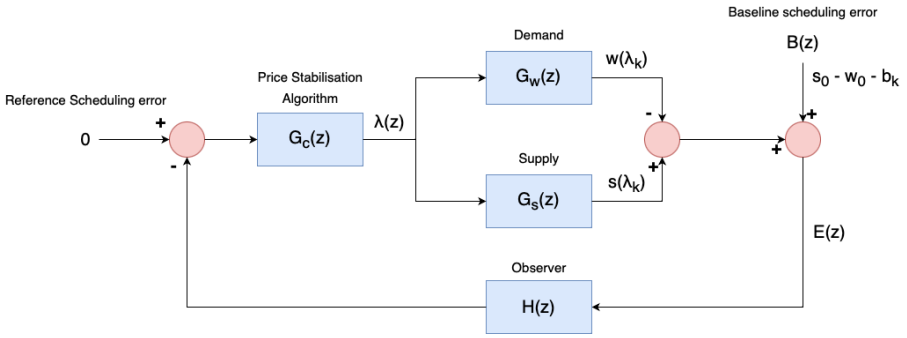

Fig 3.2: Control theoretic RTP model

Check appendix for more details on the transfer functions and formulae accompanying it.

3.1 Supplier Model

In the dynamic pricing scheme, the suppliers schedule their power generation, aiming to maximise their profits. Depending on the power generation, the ISO periodically generates the RTP signals and relays them to the suppliers. This relationship between the scheduled supply for k^{th} pricing cycle and the pricing signal λ_k can be represented as a linear equation as $s(\lambda_k) = p\lambda_k + q$ where p and q are respectively the slope and intercept of the supply model.

3.2 Consumer Model

The power consumption of any consumer is a sum of their baseline or nominal demand which depends on time, bounded and independent of pricing signal and also the pricing dependent consumption. This pricing dependent consumption can be modelled as a function of the RTP as $w_j(\lambda_k) = D_j\lambda_k^{\epsilon_j}$ where w_j is the consumption of the j^{th} consumer, D_j and ϵ_j are positive and negative constants respectively. Hence the individual consumption/demand can be modelled as $d_j(\lambda_k) = b_{j,k} + w_j(\lambda_k)$. Moreover, the overall baseline, price responsive and total demand of all the consumers at the k^{th} sampling period are represented as b_k, $w(\lambda_k)$, $d(\lambda_k)$ respectively.

3.3 Control Theoretic Price Stabilisation

The objective of an ISO is to find the clearing price such that scheduled supply equals the overall demand of the system. A control theoretic price stabilisation algorithm to minimise the overall generation scheduling error is proposed [2]. The generation scheduling error, denoted as ϵ_k (for k^{th} pricing period) mainly denotes the difference between total scheduled supply and overall demand of the system, i.e. $\epsilon_k = s(\lambda_k) - d(\lambda_k)$. In this formulation, the ISO observes the generation scheduling error of previous pricing period and uses it to generate new pricing signals for next period. The objective is to maintain the controlled variable ϵ_k close to its reference (which is zero) under the manipulated variable λ_k. Figure 3.2 illustrates this control loop. The demand and supply models can be non-linear and hence can be represented as

$$s(\lambda_k) = s(\lambda_0) + \dot{s}(\lambda_0)(\lambda_k - \lambda_0) \tag{3.1}$$

$$w(\lambda_k) = w(\lambda_0) + \dot{w}(\lambda_0)(\lambda_k - \lambda_0) \tag{3.2}$$

where λ_0 is the fixed operating point and $\dot{s}(\lambda_0)$ and $\dot{w}(\lambda_0)$ are first derivatives of their respective functions at k=0; and as s_0 and w_0 are independent of the current pricing signal, it can be added to the pricing independent baseline b_k.

Based on all of these assumptions the price stabilisation algorithm is formulated as

$$\lambda_k = \lambda_{k-1} - a \cdot e_{k-1} \tag{3.3}$$

where a is shown in the appendix and is the price stabilisation gain. The ISO sets the price according to the generation scheduling error, such that any changes in price is inversely proportional to the previous error e_{k-1}. This ensures that the system can converge to an equilibrium where the generation scheduling error is zero. Hence, for a linearised system, with fixed λ_0, the above RTP algorithm ensures stability.[2]

In the following chapters this RTP system is modelled (in Simulink) and studied. Subsequently HARVEY was used to attack the model to see it's effects on real time systems on OPAL-RT.

Chapter 4

Experimental Observations

The RTP model described in Chapter 3 is vulnerable to man-in-the-middle HARVEY like attacks and hence, to study the impacts it has on the RTP pricing stabilisation, HARVEY based malware has been used to infect the ISO of the model described in fig 3.2 using Simulink. Figure 4.1 shows the Simulink model where the controller has been divided into it's control logic and firmware - which has been infected with HARVEY.

4.1 Simulink Simulations

In our experimental setup, we consider a total of 1405 consumers who are subjected to the same pricing signal. We adopt the CEO demand model for demand generation of each consumer C_j such that the parameters D_j and ϵ_j are chosen from the normal distributions $D_j \sim \mathcal{N}(7, 3.52)$ (KW) and $\epsilon_j \sim \mathcal{N}(-0.8, 0.12)$ respectively. The baseline load b_k for each consumer is selected from the range [0.276,0.488] KW. We configure our supplier model accordingly by scaling the values of p and q for 1405 consumers. We define $p = 43.638 \times 10^{-3}$ and $q = 1.287$, and set the price stabilisation gain value as $\eta = 0.1, 0.3, 0.5, 0.7, 0.9$. HARVEY uses a scaling attack to manipulate the pricing signal with a scaling factor of $\gamma = 0.59$. The Simulink simulations were done on a system with Intel i7 2.40 GHz processor and 24 GB RAM. Figure 4.2 shows the various simulation results showing

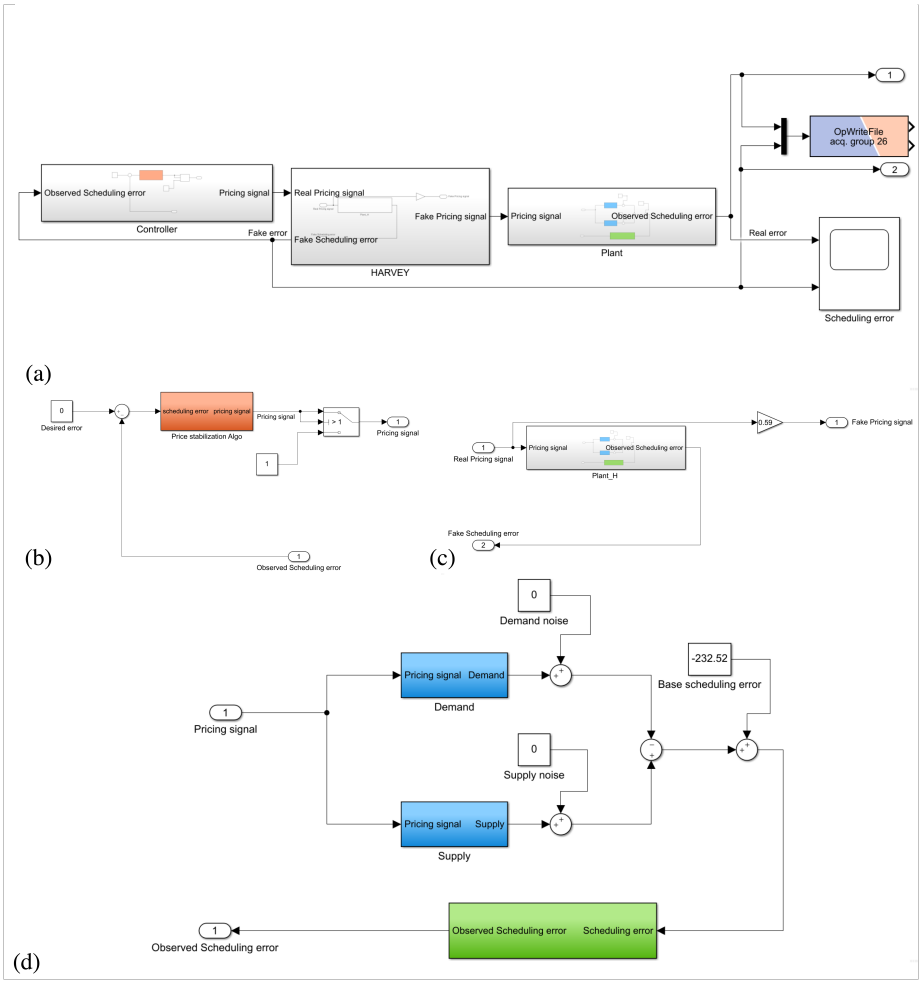

Fig 4.1: The Simulink model for the control-theoretic RTP (a) The entire model (b) Inside the controller block (c) Inside HARVEY (d) Inside the plant block

the actual plant scheduling error (Real error) and the plant scheduling error which the control logic gets (Fake error).

4.2 OPAL-RT Simulations

We evaluate the real-time performance of our privacy scheme by employing a Hardware-In-the-Loop (HIL) simulation test-bed. Our experimental HIL is an OPAL-RT real-time simulator connected with a PC having RT-LAB and Matlab/Simulink software. The host PC based RT-LAB software allows users to edit and modify various power system models, view model data, execute the model and load it into the target simulator i.e. the OPAL-RT. HIL testing offers an excellent alternative to

traditional testing methods. When performing HIL simulation, the physical plant is replaced by a precisely equivalent computer model, running in real-time on a simulator appropriately equipped with inputs and outputs (I/Os) capable of interfacing with control systems and other equipment. In this way, the HIL simulator can accurately reproduce the plant and its dynamics, together with sensors and actuators, providing comprehensive closed-loop testing without the need for testing on real systems. Figure 4.2 also contains the real-time simulated errors.

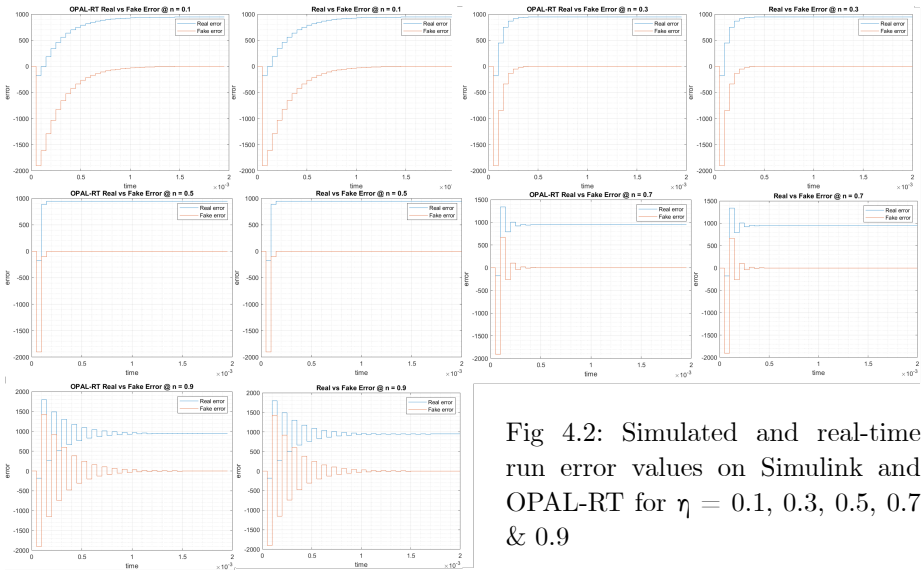

Fig 4.2: Simulated and real-time run error values on Simulink and OPAL-RT for $\eta = 0.1$, 0.3, 0.5, 0.7 & 0.9

The results accurately show what the inclusion of HARVEY does to the reading the control-logic is fed. The blue-lined error is the actual error coming out of the plant whereas the red-lined error is the error the control logic observes and assumes that the pricing is correct. Hence the attack is deemed stealthy.

Chapter 5

Future Work

Future work revolves around prevention and detection of HARVEY-esque attacks. One of the possible solutions is 'Remote Attestation'; it is a lightweight attestation framework for low-end embedded devices. The static attestation scheme verifies the integrity of the prover's memory state by performing pseudo-random walk on main memory. The dynamic attestation verifies the code execution using HPCs reflecting the footprint of the executed code. Since HARVEY does two computations which include calculating the plant behaviour as well as scaling attack we predict that the HPC values will reflect the increased time required to compute both of them. Hence using the HPC values we should be able to estimate whether the hardware is being attacked or not. Remote attestation helps in keeping the HPC values secure.

Presently both the controller and the plant is being simulated in OPAL-RT but, in the future, the communication shall occur between OPAL-RT and NI cRIO-9076 PLC. I.e. only the plant shall be simulated in OPAL-RT whereas the controller shall be simulated in the PLC cRIO-9076. Following that, the HPC values shall be obtained once by running the controller without HARVEY and then running the controller with HARVEY to analyse the changes in HPC values and detect the present of a malware. Additionally Secure Boot may be used, secure boot ensures that only a known and trustworthy software can be

loaded on a device thus preventing the malware from entering the firmware at the first place.

Appendix

Formulae:

$$a = \frac{2\eta}{\dot{s}(\lambda_0) - \dot{w}(\lambda_0)}$$

$$G_C(z) = \frac{az}{z-1}$$

$$G_w(z) = D\epsilon\lambda_0^{\epsilon-1}$$

$$G_s(z) = p$$

$$B(z) = s_0 - w_0 - b_k$$

$$H(z) = \frac{1}{z}$$

$$s(\lambda) = p\lambda + q$$

$$w(\lambda) = D\lambda^{\epsilon}$$

$$s_0 = s(\lambda_0) - \dot{s}(\lambda_0)\lambda_0$$

$$w_0 = w(\lambda_0) - \dot{w}(\lambda_0)\lambda_0$$

References

[1]Garcia, Luis & Brasser, Ferdinand & Cintuglu, Mehmet & Sadeghi, Ahmad-Reza & Mohammed, Osama & Zonouz, Saman. "Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit", NDSS, 2017.

[2]Rui Tan, Varun Badrinath Krishna, David K.Y. Yau, and Zbigniew Kalbarczyk. "Impact of integrity attacks on real-time pricing in smart grids", Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013