Cyber Attack Detection for a Nonlinear Binary Crude Oil Distillation Column

H. M. Sabbir Ahmad
Department Of Electrical Engineering
Qatar University
Doha,Qatar
ha1607441@student.qu.edu.qa

Nader Meskin
Department Of Electrical Engineering
Qatar University
Doha,Qatar
nader.meskin@qu.edu.qa

***Abstract*—Cyber security for Industrial Control Systems (ICS) is increasingly becoming an area of research as advance network technology continues to evolve providing extended connectivity between cyber world and control system hardware in a plant. In this paper, we present attack detection and isolation technique for sensor attacks on a binary distillation column as an important ICS field which can be targeted by attackers. At first, we present a hybrid model of a DC where the DC has been designed in Aspen Plus Dynamics and the control system has been implemented using Simulink. Then, the mathematical model of various sensor attacks which have been considered for the study are presented. Following that an attack detection and isolation technique based on state estimation using Luenberger observer has been presented. Finally we present the results illustrating effect of sensor attacks on DC performance along with validating the effectiveness of the proposed attack detection and isolation method.**

***Index Terms*—Industrial Control Systems, crude oil distillation column, hybrid model of DC, attack detection, and Luenberger observer.**

I. Introduction

Due to the continuous development of technology, an increasing number of electronic devices are being created with networking features suitable for connecting to IT networks. This technological evolution has also made its way to ICS where an increasing number of monitoring and controlling devices have been connected to computer networks facilitating supervisory level monitoring and control with economic and performance enhancing benefits. However, it also makes ICS more vulnerable to cyber-attacks. Some typical examples of attacks in real systems are the Stuxnet worm attack, multiple recent power blackouts in Brazil, and the SQL Slammer worm attack on the Davis-Besse nuclear plant, to name a few further justifying the need to address cyber security for ICS [1], [2].

In this paper, a continuous binary DC is considered as a cyber-physical framework to investigate the effect of attacks on the performance of the DC as well as the development of attack detection and isolation algorithm. The huge worldwide demand for crude oil can make them a target for attackers. Since distillation columns (DC) handle highly flammable chemicals, attackers can launch attacks with the motivation of causing damage to the plant infrastructure or upset the column operation by degrading the quality of the distilled products.

The availability of a wide scale computer simulation tools makes it possible to simulate the dynamic behavior of a nonlinear plant based on their mathematical models, to facilitate safer tools for performing cyber security study and consequently, to save cost and time. In this paper, a model of a continuous binary DC is presented based on a hybrid simulation engine where the plant dynamics are simulated using Aspen Plus Dynamics and the ICS is implemented in MATLAB/Simulink.

ICSs are characterized by feedback closed-loop control architecture and aim to optimize the system control performance, such as reducing state estimation errors, stabilizing an unstable plant, and enhancing the robustness against uncertainties and noise. A cyber-physical system (CPS) is characterized by the number of control loops containing controller, sensors, and actuators. Hence attacks can be modelled as sensor attacks, actuator attacks and controller attacks. In [3]–[6], various different models for sensor attacks are presented. Various different actuator attack models have been presented by authors in [7], [8]. In [1], [2], [9]–[12] authors present attacks which can be applied to both sensors and actuators. This paper limits the study to sensor attacks and presents the mathematical models of attacks that have been injected to the DC.

There is no literature available in the area of cyber security for DC. In terms of application areas, in [13]–[15] authors explore the effect of cyber-attacks on Smart Grid whereas [16], [17] study the effect of cyber-attacks on Power Systems. In [18], [19], the effect of cyber-attacks on Smart Cities and Water Distribution System are investigated, respectively.

In this paper, an attack detection technique has been implemented based on state estimation using a bank of observers implemented using Luenberger observer. The DC model is a Multiple Input Multiple Output (MIMO) system and the proposed solution relies on allocating an observer for each output. For attack isolation, each observer gain is tuned optimally to detect when a particular sensor is under attack. Observer-based detection techniques have been presented in [20]–[24]. In [5], and [25] Kalman Filter (KF) is used for securely estimating the system states for detecting cyber-attacks.

As said there are no literature available for cyber security on a distillation column; this paper primarily contributes in this area. Firstly, it presents a hybrid Aspen Plus based model of a DC that can accurately represent the dynamics of a real world

978-1-7281-4821-2/20/$31.00 ©2020 IEEE

DC which can serve manifold benefits including providing option for designing data driven detection algorithms and so on. Secondly it explains the vulnerability points of a DC that can be targeted by adversaries and hence needs to be secured. Finally, the paper presents a state estimation based algorithm that facilitates both attack detection and isolation.

II. A BINARY DISTILLATION COLUMN

A continuous binary distillation column separates a crude feedstock into two product streams i. distillate, and ii. bottoms product. It is assumed that feed into the column is a two-phase (liquid and vapor phase) pseudo-binary mixture of a light product and a heavy product which is separated in the column. For successful separation it is desired that the concentration of lighter product in both distillate is close to 100% and in bottom product virtually 0% which arises the necessity for a feedback control system in DC.

The column can be divided in two sections i. rectifying section and ii. striping section. The rectifying section is located at the top just above the feed and the bottom section is called the stripping section. The original crude feedstock is passed through a preheater which heats the feed to a certain temperature to separate the feed in a two-phase fluid before feeding to the distillation column. This is one of the energy input port of the distillation column. The top product is fed to a condenser which effectively condenses the vapor distillate to a cold liquid reflux. This allows for energy to be extracted off the column. Finally, the bottom product stream is reheated using a partial re-boiler which allows for energy into the column. A flowsheet of a binary DC is presented in Fig. 1.

A. Plant Data

The distillation column is designed using Aspen Plus and then the dynamic model is derived using Aspen Plus dynamics. Table I summarizes the composition of the raw feed condensate used to design the DC in Aspen Plus.

There are a total of 32 trays inside the column. The raw crude stock is fed in liquid phase to tray 15 in the distillation column. The column has been designed to operate at a pressure of 14 atm at the top, i.e. the pressure at the reflux drum is 14 atm. The differential pressure between the stages is set to 0.1 psi. The height and length of the both the reflux drum and the reboiler have been set to 1 meter, respectively. The aim is to collect more than 98% propane in the distillate and more than 99% isobutene (i.e. <1% Propane) in the bottoms product.

TABLE I
COMPOSITION OF THE RAW CONDENSATE

Component	Mole %
Propane	40.00
Iso Butane	60.00

As part of this dynamic simulation scheme the column has been first designed using Aspen Plus which is then imported to Aspen Plus Dynamics in order to perform the dynamic simulation.

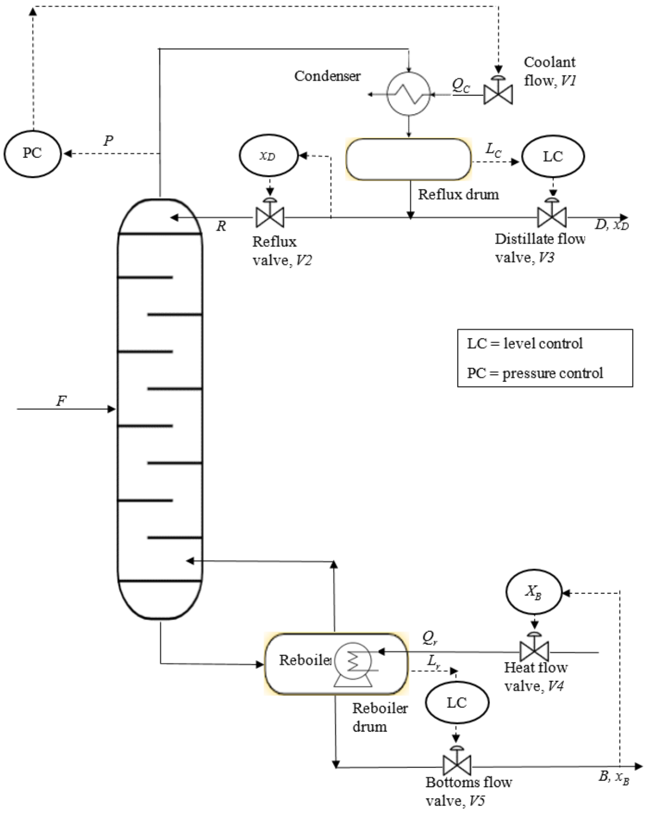

Fig. 1. Flowsheet of a binary distillation column

B. Control of Distillation Column

Generally, a column is designed to operate in the steady state at the values determined from design calculations during the normal operation. A column remains at energy and material balance (described by mesh equations) during the steady state condition. Material balance infers that the sum of products entering the column must be equal (approximately) to the sum of products leaving the column; and energy balance implies that the heat input to the column must be equal (approximately) to heat removed from the system. A column is said to be "stable" when it is under energy and material balance.

The flowsheet shown in Fig. 1 contains five control valves each of which can be used to independently vary the distillate flow rate, reflux flow rate, bottoms flow rate, condenser duty, and reboiler duty. Therefore, this column has five DoF.

The feed stream is considered being set by the upstream process; hence is considered to be a constant. Inventory loops in the case of the distillation column presented in Fig. 1 include liquid levels in the reflux drum and column base which must be controlled around a constant desired value to ensure the distillate and reflux flow, and bottoms flow and reboiler duty can be adjusted properly as the liquid flow requires pressure which depends on the liquid height. The column has been designed to operate under constant pressure hence the

TABLE II
CONTROL CONFIGURATION FOR A BINARY DC

Controlled variables	Manipulated variables	Control valve (Fig. 1)
Column pressure, P	Condenser duty, Q_c	Coolant flow (*V1*)
Distillate purity concentration, x_D	Reflux flow rate, R	Flux flow(*V2*)
Liquid level in reflux drum, L_c	Distillate flow rate,B	Distillate flow (*V3*)
Bottoms impurity concentration, x_B	Reboiler duty, Q_r	Heat flow (*V4*)
Liquid level in column base, L_R	Bottoms flow rate, B	Bottom flow (*V5*)

TABLE III
EMERGENCY SHUTDOWN THRESHOLD FOR EACH CONTROLLED VARIABLES

Controlled variables	Maximum	Minimum
Column pressure (atm)	20	–
Concentration of distillate	–	0.90
Liquid level (m)	1.00	0.05
Concentration of bottoms	0.10	–
Liquid level in column base (m)	1.00	0.05

pressure has to be controlled as excessive pressure can risk the mechanical integrity of the column. Therefore, including the quality requirement of the distillate and bottoms product, in total, there are five variables which has to be controlled using five inputs mentioned in Table II.

The column dynamic model is linked to Simulink and the controllers are designed and tuned. PID controller is used to control each variable. The distillate purity concentration(x_D) and bottoms impurity concentration (x_B) set-points are selected as 0.98 and 0.01 respectively, the column pressure (P) is set at 14 atm and the liquid level set-point in the reflux drum (L_c) and reboiler (L_r) are selected at 0.75 m. Following that, the closed-loop control system in Simulink is integrated with the dynamic model in Aspen Plus Dynamics to perform the dynamic simulation of the DC.

C. Emergency shutdown

All five controlled variables are critical for the safe operation of the column following its performance specifications. Hence, it is necessary to include shutdown thresholds for each of these parameters to avoid operating the column if their values violated the thresholds. Table III summarizes the thresholds set for each of the five parameters for an emergency shutdown.

III. MATHEMATICAL MODELING OF CYBER ATTACKS

Mathematically modeling of a cyber attack provides a means of evaluating its effect on the dynamics of a physical plant with the aid of computer simulation. An ICS under different attacks is shown in Fig. 2 where the plant can be modeled as

$$\begin{aligned}\dot{x}(t) &= f(x(t), \widetilde{u}(t), t) + w(t)\\ y(t) &= g\left(x(t), t\right) + v(t)\end{aligned} \tag{1}$$

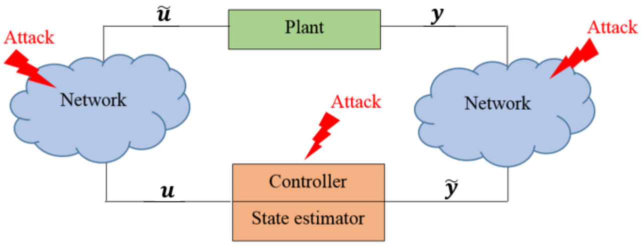

Fig. 2. Block level illustration of Cyber Physical System under attack

and the controller can be generally modeled as a dicrete-time nonlinear system

$$\begin{aligned}\dot{z}(k) =& p\left(z(k), \widetilde{y}(k), k\right)\\ u(k) =& q\left(z(k), \widetilde{y}(k), k\right)\end{aligned} \tag{2}$$

where $u \in \mathbb{R}^m$, $\widetilde{u} \in \mathbb{R}^m$, $y \in \mathbb{R}^o$, and $\widetilde{y} \in \mathbb{R}^o$ are the controller output, input to the plant actuators, output from the plant sensors, and controller input, respectively of a CPS, and $w(t)$ and $v(t)$ represent the process noise and measurement noise, respectively.

It should be noted that the plant is considered as a continuous time system and the controller as discrete time digital system, as, a controller can be viewed as a tailored computer en-tasked to control the plant. The sampling is done following the zero order hold model. If the network integrity is maintained, at every sampling instant k, the output from the plant should be available precisely at the input of the controller i.e. $\widetilde{y}(k) = y(t = k)$. and similarly the output from the controller should be available to the actuators precisely i.e. $\widetilde{\boldsymbol{u}} = \boldsymbol{u}$.

A. Sensor attack

For all attacks T_a represents the attack period, $y_i(t)$ and $y_i(t)$ are the the i-th sensor measurement and sensor reading to the controller, respectively. In case of these attacks the sensor measurements from the plant to controller $\widetilde{y}(t)$ for the ICS represented by (1) and (2) are corrupted by the attacker.

1) Scaling Attack: A scaling attack involves modifying true measurements to higher or lower values depending on the scaling attack parameter as:

$$\widetilde{y}_i\left(k\right) = \begin{cases} y_i\left(k\right) & k \notin T_a\\ \left(1+\lambda_s\right) y_i\left(k\right) & k \in T_a\end{cases} \tag{3}$$

where λ_s is a constant.

2) Ramp attack: In this attack, the true sensor measurements are modified by adding a ramp function which gradually increases/decreases with time based on the gradient of ramp denoted by λ_r, as follows:

$$\widetilde{y}_i\left(k\right) = \begin{cases} y_i\left(k\right) & k \notin T_a\\ y_i\left(k\right) + \lambda_r & k \in T_a\end{cases} \tag{4}$$

3) Random attack: This attack involves the addition of randomly generated positive attack values generated by a uniform random variable [5], [26] as:

$$\widetilde{y_i}\left(k\right)=\begin{cases} y_i\left(k\right) & k\ \notin T_a \\ y_i\left(k\right)+rand(a,b) & k\ \in T_a \end{cases} \tag{5}$$

where a and b are the minimum and maximum value of the random signal respectively.

4) False data injection (FDI) attack: In this attack, the injection attack can be modeled as

$$\widetilde{y_i}(k)=\begin{cases} y_i\left(k\right) & k\ \notin T_a \\ y_a(k) & k\ \in T_a \end{cases} \tag{6}$$

where $y_a(k)$ is the injected false sensor measurement during attack.

IV. Attack surface identification for DC

The paper assumes that the attacker has breached the IT security configurations and firewall settings and has access to the hardware linked to the physical plant. Identification of the attack surface is the first step towards designing attack detection, diagnostics, recovery and elimination tools for cyber physical systems.

As stated, the column is under energy and mass balance during normal operation. Any attack can cause violation to mass and energy balances. It is assumed that each of the feedback control loop is networked. The attacks can intend to deviate the quality of the output product beyond their specified requirement which will cause financial loss. Crude oil is highly flammable hence the attackers can target the liquid level control loops to upset the mass balance by increasing liquid level in either tanks causing a spillage thus posing fire hazard. Besides that the attackers can target the column pressure threatening the integrity of the column with the aim of imparting environment damage, monetary loss and loss of human lives.

V. State estimation based attack detection

In this paper, a bank of observers is developed for sensor attack detection and isolation where each observer is only designed to estimate one output. Fig. 3 presents the proposed scheme for cyber-attack detection and isolation algorithm.

A. Luenberger Observer design

A linear model of the column is generated around the stable operating point during steady state using Aspen Plus Dynamics based on the step response. The aim is to design an observer to estimate small changes in states around the equilibrium point. Based on the reduced linear system model the state space representation of the full order observer or Luenberger observer is given as follows:

$$\begin{aligned} \dot{\hat{x}}_\delta(t) &= A\hat{x}_\delta(t)+Bu(t)+K(y_\delta(t)-\hat{y}_\delta(t)) \\ \dot{\hat{y}}_\delta(t) &= C\hat{x}_\delta(t)+Du_\delta(t) \end{aligned} \tag{7}$$

where $\hat{x}_\delta$, $\hat{y}_\delta$, $\hat{y}_\delta$, and K are estimated state, estimated output, output measurement, and observer gain respectively. The actual output estimate is computed from the observer output estimate as following:

$$\hat{y}(t)=\hat{y}_\delta(t)+y_{eq} \tag{8}$$

where $\hat{y}(t)$ is the estimated output and y_{eq} is the output value used during linearization.

B. Residual based attack detection and isolation

The detection scheme relies on discrepancy between the sensor measurements and predicted output during attack scenario which can be computed as a residual. During normal operation the residual will remain small and during the attack, the residual value exceeds the threshold. The residuals are as follows: $r_{Lc}=|\hat{L}_C(t)-\widetilde{L}_C(t)|$, $r_{Lr}=|\hat{L}_r(t)-\widetilde{L}_r(t)|$, $\widetilde{P}=|\hat{P}(t)-\widetilde{P}(t)|$, $r_{xD}(t)=|\hat{x}_D(t)-\widetilde{x}_D(t)|$, and $r_{xB}(t)=|\hat{x}_B(t)-\widetilde{x}_B(t)|$ which correspond to the liquid levels (m) in the reflux drum and the reboiler drum, the column pressure at the top (atm), the distillate purity and bottoms impurity at the controller side, respectively. Any parameter $\hat{z}$ implies value of parameter z estimated by the observer. The threshold values for the residuals r_{Lc}, r_{Lr}, r_P, r_{xD}, and r_{xB} are set to 0.2 m, 0.2 m, 5 atm, .01 and .01, respectively.

VI. Simulation Result

The simulation results for sensor attacks using the proposed detection and isolation scheme are presented in this section. It should be mentioned that there exists discrepancy between the observer outputs and the sensor measurement at the beginning of the simulation which is due to initial transient response of the observers. The convergence time of the observers are around 0.5 hours during simulation. Hence all attacks are injected after $t=1$ hours. The controller samples the measurements with sampling time of 0.01 hour.

A. Sensor attack

1) Scaling attack: The value of λ_s is set to 0.5 for the sensor attack on the reflux drum liquid level measurements as shown in Fig. 4. Fig. 5 presents the residual signals corresponding to this attack. As can be seen from this figure, only the residuals corresponding to this measurement exceeds the threshold and other residuals remain below the threshold. Hence, this sensor attack is detected and isolated in 0.01 hour.
2) FDI attack: The attack vector is generated using continuous time pulse with a period of 0.1 hour and pulse width of 20% biased by multiplying with a uniformly distributed random variable between $(0.8, 0.9)$ for this attack and fed to the reboiler liquid level measurements which is shown in Fig. 6. The attack resulted in feeding liquid level data which is lower than the true liquid level in the reboiler drum. Hence, the controller reduces the bottoms product flow rate which results in increasing the true level of liquid in the reboiler and consequently an emergency shutdown. Fig. 7 shows the residual signals corresponding to this attack scenario. Results show that r_{Lr} detects the attack in .02 hour before the emergency shutdown and the remaining residuals do not

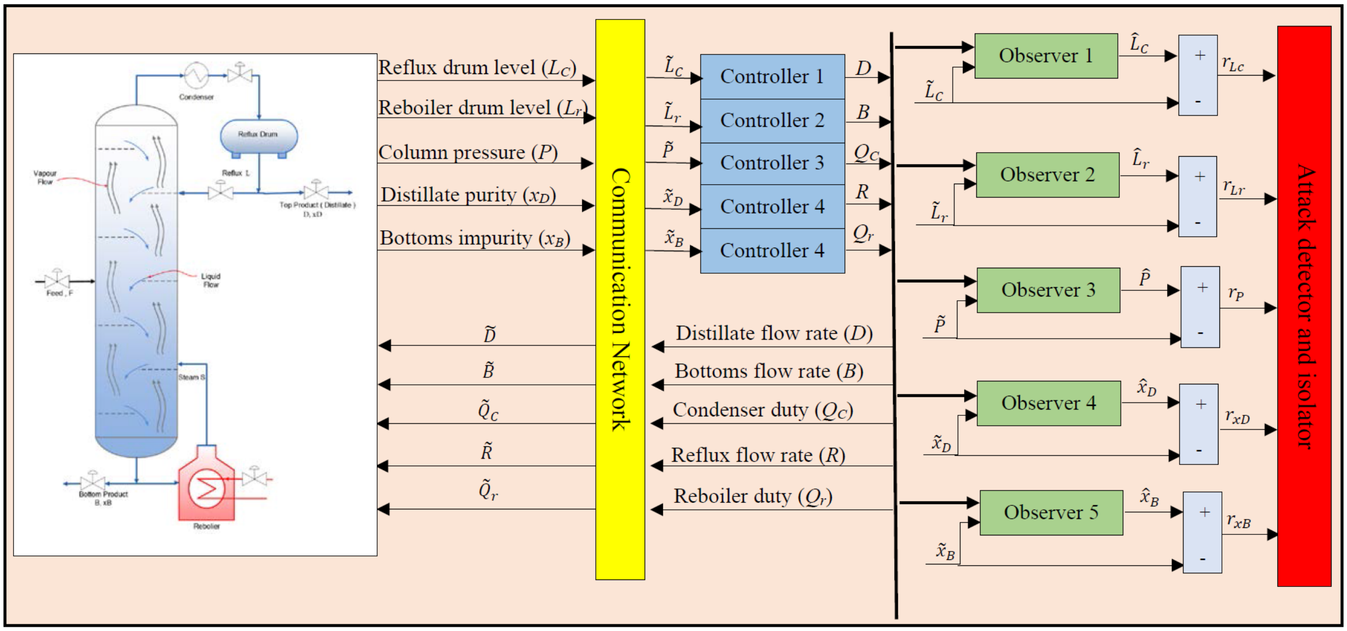

Fig. 3. Attack detection and isolation scheme using Observer based state estimation.

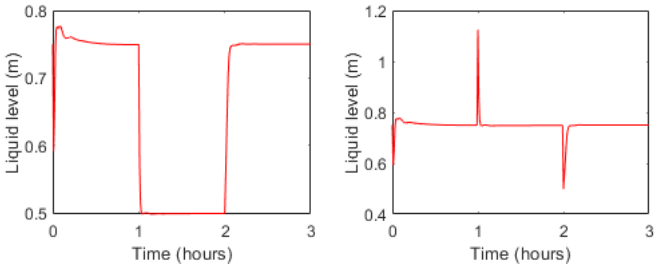

Fig. 4. Actual vs injected reflux drum liquid level during for a scaling attack vs time.

exceed their thresholds and hence the attack can be both detected and isolated.

Table IV summarizes the performance and results obtained for different control loops using the detection and isolation scheme for the proposed sensor attacks. It should be noted that these results have been obtained for specific values of attack parameters hence variation in the attack parameters may cause the results to differ although the scheme will still remain functional.

TABLE IV
SUMMARY OF RESULTS FOR THE PROPOSED SENSOR ATTACKS USING THE OBSERVER BASED DETECTION AND ISOLATION SCHEME.

Attack name	Attacked parameter	Detection time	Attack isolation (Y/N)
Scaling attack	Distillate purity	.03	Y
	Bottoms impurity	.02	Y
	Liquid level in reflux drum	.01	Y
	Liquid level in reboiler drum	.01	Y
	Pressure	.02	Y
Ramp attack	Distillate purity	.01	Y
	Bottoms impurity	.04	Y
	Liquid level in reflux drum	.02	Y
	Liquid level in reflux drum	.01	Y
	Pressure	.01	Y
Random attack	Distillate purity	.17	Y
	Bottoms impurity	.20	Y
	Liquid level in reflux drum	.06	Y
	Liquid level in reflux drum	.08	Y
	Pressure	.58	Y
FDI attack	Distillate purity	.64	Y
	Bottoms impurity	.53	Y
	Liquid level in reflux drum	.04	Y
	Liquid level in reflux drum	.02	Y
	Pressure	.03	Y

VII. Conclusion

A hybrid model of a closed loop controlled DC has been presented in the paper. The proposed control configuration for the DC is able to marginalize the effect of coupling between inputs and outputs. State estimation technique based on Luenberger observer has been used for attack detection. The isolation scheme has been designed using a bank of observer utilizing the fact that the proposed control configuration is able to decouple the relationship between inputs and outputs; hence a sensor attack will only affect the performance of the corresponding feedback loop it is part of. The modeled sensor attacks have been injected to the different control loops of the hybrid model of the DC and the results show that the proposed

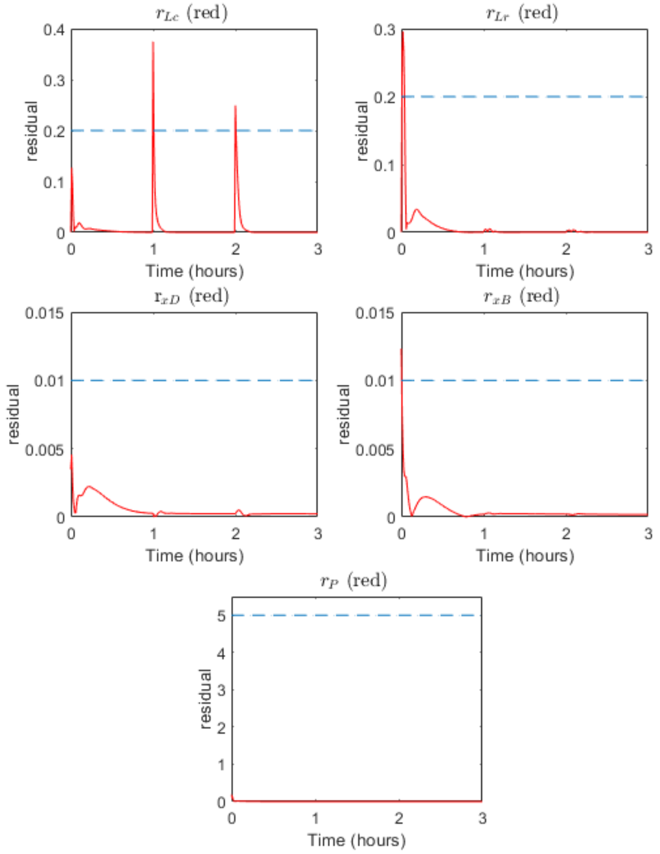

Fig. 5. Residual signals corresponding to scaling attack in the reflux drum liquid level sensor.

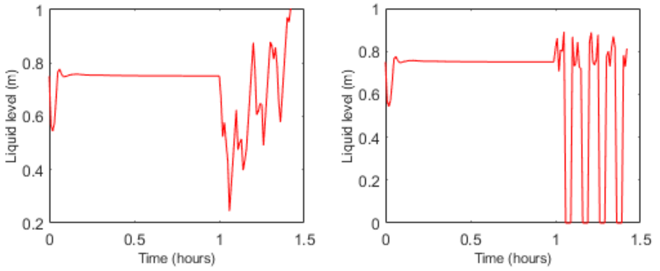

Fig. 6. Actual vs injected reboiler drum liquid level during for a FDI attack vs time.

scheme based on state estimation is able to detect attacks successfully. Besides that only observer outputs associated to the feedback loop under attack are corrupted by attack hence validating the isolation scheme.

Acknowledgment

This publication was made possible by the Graduate Sponsorship Research Award (GSRA) award (GSRA4-2- 0518-17083) from the Qatar National Research Fund (QNRF), a member of the Qatar Foundation. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of QNRF.

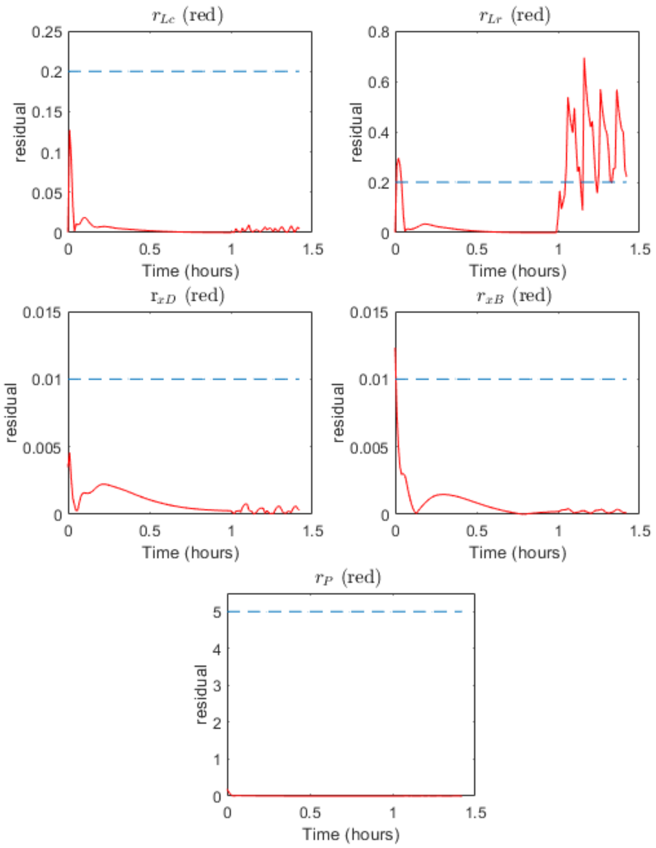

Fig. 7. Validation of attack detection and isolation scheme for FDI attack on the liquid level in the reboiler drum.

References

[1] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, Feb 2015.

[2] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, pp. 2715–2729, 2012.

[3] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *IJSN*, vol. 6, pp. 2–13, 04 2011.

[4] Y. Wadhawan, A. Almajali, and C. Neuman, "A comprehensive analysis of smart grid systems against cyber-physical attacks," *Electronics*, vol. 7, 10 2018.

[5] T. Meraj, S. Sharmin, and A. Mahmud, "Studying the impacts of cyber-attack on smart grid," in *2015 2nd International Conference on Electrical Information and Communication Technologies (EICT)*, Dec 2015, pp. 461–466.

[6] T. Zhang, Y. Wang, X. Liang, Z. Zhuang, and W. Xu, "Cyber attacks in cyber-physical power systems: A case study with gprs-based scada systems," in *2017 29th Chinese Control And Decision Conference (CCDC)*, May 2017, pp. 6847–6852.

[7] S. Hasan, A. Ghafouri, A. Dubey, G. Karsai, and X. Koutsoukos, "Vulnerability analysis of power systems based on cyber-attack and defense models," in *2018 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2018, pp. 1–5.

[8] H. Nishino and H. Ishii, "Distributed detection of cyber attacks and faults for power systems," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 11 932 – 11 937, 2014, 19th IFAC World Congress.

[9] A. Dagoumas, "Assessing the impact of cybersecurity attacks on power systems," *Energies*, vol. 12, p. 725, 02 2019.

[10] A. Aldairi and L. Tawalbeh, “Cyber security attacks on smart cities and associated mobile technologies,” *Procedia Computer Science*, vol. 109, pp. 1086–1091, 12 2017.

[11] S. Adepu and A. Mathur, “An investigation into the response of a water treatment system to cyber attacks,” in *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, Jan 2016, pp. 141–148.

[12] D. T. Ramotsoela, G. P. Hancke, and A. M. Abu-Mahfouz, “Attack detection in water distribution systems using machine learning,” *Human-centric Computing and Information Sciences*, vol. 9, no. 1, p. 13, Apr 2019.

[13] I. Shames, F. Farokhi, and T. H. Summers, “Security analysis of cyber-physical systems using $\mathcal{H}_2$h2 norm,” *IET Control Theory Applications*, vol. 11, no. 11, pp. 1749–1755, 2017.

[14] Y. Yan, P. Antsaklis, and V. Gupta, “A resilient design for cyber physical systems under attack,” in *2017 American Control Conference (ACC)*, May 2017, pp. 4418–4423.

[15] C.-Z. Bai, F. Pasqualetti, and V. Gupta, “Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs,” *Automatica*, vol. 82, pp. 251 – 260, 2017.

[16] Y. Mo, S. Weerakkody, and B. Sinopoli, “Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs,” *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, Feb 2015.

[17] C. Kwon, W. Liu, and I. Hwang, “Security analysis for cyber-physical systems against stealthy deception attacks,” in *2013 American Control Conference*, June 2013, pp. 3344–3349.

[18] Y. Liu, P. Ning, and M. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Trans. Inf. Syst. Secur.*, vol. 14, p. 13, 01 2011.

[19] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using kalman filter,” *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, Dec 2014.

[20] Y. Nakahira and Y. Mo, “Dynamic state estimation in the presence of compromised sensory data,” in *2015 54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 5808–5813.

[21] M. S. Chong, M. Wakaiki, and J. P. Hespanha, “Observability of linear systems under adversarial attacks,” in *2015 American Control Conference (ACC)*, July 2015, pp. 2439–2444.

[22] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, “Secure state estimation against sensor attacks in the presence of noise,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 49–59, March 2017.

[23] Y. Shoukry and P. Tabuada, “Event-triggered projected luenberger observer for linear systems under sparse sensor attacks,” in *53rd IEEE Conference on Decision and Control*, Dec 2014, pp. 3548–3553.

[24] Y. Shoukry, M. Chong, M. Wakaiki, P. Nuzzo, A. L. Sangiovanni-Vincentelli, S. A. Seshia, J. P. Hespanha, and P. Tabuada, “Smt-based observer design for cyber-physical systems under sensor attacks,” in *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, April 2016, pp. 1–10.

[25] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, “Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach,” *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 4917–4932, Oct 2017.

[26] M. Lv, W. Yu, Y. Lv, J. Cao, and W. Huang, “An integral sliding mode observer for cps cyber security attack detection,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, p. 043120, 04 2019.