Palleti *et al. Cybersecurity* (2021) 4:8
https://doi.org/10.1186/s42400-021-00071-z

Cybersecurity

RESEARCH Open Access

Cascading effects of cyber-attacks on interconnected critical infrastructure

Venkata Reddy Palleti[1*], Sridhar Adepu[2], Vishrut Kumar Mishra[2] and Aditya Mathur[2]

Abstract

Modern critical infrastructure, such as a water treatment plant, water distribution system, and power grid, are representative of Cyber Physical Systems (CPSs) in which the physical processes are monitored and controlled in real time. One source of complexity in such systems is due to the intra-system interactions and inter-dependencies. Consequently, these systems are a potential target for attackers. When one or more of these infrastructure are attacked, the connected systems may also be affected due to potential cascading effects. In this paper, we report a study to investigate the cascading effects of cyber-attacks on two interdependent critical infrastructure namely, a Secure water treatment plant (SWaT) and a Water Distribution System (WADI).

Keywords: Industrial Control Systems, Water treatment, Water distribution, Interconnected critical infrastructure, Cyber-attacks, Cascading effects

Introduction

Critical Infrastructure (CI) such as power grids, transportation networks, and water supply systems are considered vital to a nation's economy and prosperity[1]. In order to achieve real time monitoring and control, such systems couple computer control systems with the physical process. This coupling of physical and cyber systems forms a Cyber-Physical System (CPS). Such coupling often interjects vulnerabilities making it raising the possibility of damaging the physical system.

Further, several CI are interconnected and dependent on each other. For example, a water treatment or a water distribution plant requires power to operate and hence is connected to a power distribution source. Therefore, a random failure, or a cyber-attack, in a component of an interdependent system could cause cascading effects that can potentially collapse a component of or the entire system of interdependent CI. For example, the year 2003 blackout in the United States and Canada (U.S.-Canada 2004) was initiated to a large extent by the failure that initially occurred in the communication system.

Following are the types of interconnections between Critical Infrastructure (Rinaldi et al. 2002) that are useful when investigating the cascading effects of cyber-attacks on coupled CI.

- *Physical*: Physical reliance on material flow from one CI to another, e.g., an electric power grid supplies electric power for water treatment and distribution systems.
- *Cyber*: This refers to the reliance of two or more CI on each other for information transfer, also known as "Informational Interdependency." For example, the amount of treated water in a water treatment plant requires information regarding the demand from a water distribution system.
- *Geographic*: A local environmental event affects components across multiple CI due to physical proximity. This is also known as "Geospatial Interdependency."
- *Logical*: This dependency is due to mechanisms such as policy, legal, or regulatory regimes, that can link logically two or more CI.

*Correspondence: venkat_palleti.che@iipe.ac.in
[1]Indian Institute of Petroleum and Energy, 2nd Floor, AU Engg College Main Block, Andhra University, 530003 Visakhapatnam, India
Full list of author information is available at the end of the article

[1]In this work the terms critical infrastructure, plant, and system are used interchangeably.

While interdependencies among CI are often necessary to meet design specifications, they also lead to undesirable situations when a fault or attack occurs in one CI and escalates to other connected CI (Rinaldi et al. 2002). Such escalation may disrupt the operation of the involved CI and create subtle feedback loops that can initiate and propagate disturbances in unforeseen ways due to the complexity of the connected systems. In addition, the inclusion of cyber components such as SCADA workstations, HMI interfaces, and PLCs has made these systems vulnerable to cyber-attacks that could create cascading effects.

There exist interconnected systems in several application domains. For example, Vaidya et al. (2011) describes a security mechanism in a vehicle-to-grid infrastructure. The vulnerability assessment of interdependent systems is discussed in Lee et al. (2004). Resilience assessment of such systems is addressed in Ouyang and Wang (2015). A co-simulation approach for vulnerability analysis of such systems is proposed in Caire et al. (2013). A model for studying interdependency across CI has been proposed in Rozel et al. (2008). This work, though not directly related to cyber security, helps extract dependencies which then can be used in investigating the propagation of attacks across connected systems. A framework is introduced in Heracleous et al. (2017) based on open hybrid automata for modeling interdependency in CI. This model is used to investigate the cascading effects on three interconnected CI, namely, water, power, and telecommunication. Recent work (Zhang and Yagan 2018) shows how to model and analyze the dynamics of cascading failures on interdependent cyber-physical systems. In this work, failures in the system are assumed as a random attack on a certain fraction of nodes. A centralized approach is proposed in Heracleous et al. (2018) for monitoring and detection of failures for hybrid systems with nonlinear uncertain continuous-time dynamics and measurement noise. In Rueda and Calle (2017), presented a matrix analysis to mitigate attacks on an interconnected system namely, power grid and telecommunications networks. There has been a significant work in the area of networked control systems. For example, in Amin et al. (2013) and Amin et al. (2009), authors look into the security of networked control systems. Further, a survey of various network control techniques is explained in Liu and Zeng (2012).

In summary, critical infrastructure interdependency means that the behavior and reliability of one system on another system. Therefore, any attack on one system can spread to another system, leading to disruption of services or economic loss. To the best of the author's knowledge, the works reported on attacks on interconnected systems were carried out through a simulation environment. In contrast to the existing works, this paper emphasizes on experimental investigation of cyber-attacks on an interconnected system to showcase the cascading effects of one on the other system. The experiments were performed on a system that includes, namely, Secure Water Treatment (SWaT) plant and Water Distribution (WADI) system. The experiments are designed to understand the impact of single and multi-point cyber-attacks on a single system or two systems. Further, an invariant based approach was used to detect attacks within and across the systems. In this work, the invariants were derived based on the work in Adepu and Mathur (2016a). In addition to work in Adepu and Mathur (2016a), 'distributed-invariants' are also defined in "Invariants" section. To summarise, the contributions are listed as follows.

Contributions: (a) An experimental investigation of cyber-attacks on an interconnected system that includes a water distribution and a water treatment plant. (b) Identification of forward and backward cascading effects caused by cyber-attacks on one or both of the systems studied. (c) the application of an invariant-based approach (Adepu and Mathur 2016a) to interconnected CI for detecting process anomalies resulting from cyber-attacks.

Organization: The remainder of this paper is organized as follows. Interdependency among CI is described in "Interdependency among critical infrastructure" section. The architecture of SWaT and WADI testbeds and their dependency is explained in "Interconnected testbed" section. In "Design of experiments" section, the design of experiments and attack tools are described. Cascading effects between SWaT and WADI are discussed in "Cascading effects of attacks on SWaT and WADI" section. The related work is presented in "Related work" section. Conclusion and future works are explained in "Conclusions and future work" section.

Interdependency among critical infrastructure

Consider a plant CI that contains a finite set of components $\{c_1, c_2, ..., c_n\}$. These components are connected to each other via directed links denoting the flow of system resource or information. Thus, CI can be represented as a graph.

Now consider two interconnected systems, namely, CI_A and CI_B with component sets, respectively, as $\{c_{a1}, c_{a2}, \ldots, c_{an}\}$ and $\{c_{b1}, c_{b2}, \ldots, c_{bm}\}$. Consider components $c_{ai} \in CI_A$ and $c_{bj} \in CI_B$. CI_A and CI_B are considered dependent on each other if one of the following condition is satisfied.

1. The interconnected systems can have one or more inputs from another infrastructure. For example, the output of an electric power generation system is input to an electric power distribution system.
2. Both systems share one or more components, i.e., $c_{ai} = c_{bj}$ = water tank for some i and j, where systems share a tank for storing water. In this case

the amount of input available for both systems is shared. Consumption in one system affects the resource available for the other.

3. The flow of resource uses components in CI_A or CI_B, but not in both. An example of such dependency is a transport system where there exist multiple routes from point X to point Y and these different routes are dependent on each other.

Interconnected testbed

Two interceonnected testbeds, namely Secure Water Treatment (SWaT) and Water Distribution (WADI), were used in the experiments reported here. SWaT and WADI are described briefly in the following subsections.

SWaT

SWaT consists of six stages to purify raw water. Figure 1 represents the architecture of SWaT. It consists of a total of 12 Programmable Logic Controllers (PLCs) (six primary and six standby). Description of each stage, and the communications network, follows; details are in Mathur and Tippenhauer (2016).

Physical process: In stage 1 (P1) raw water to be treated is stored in a tank. This stage contains one tank, an on/off valve MV101 that controls the flow of water into the tank, and a pump P101 that transfers water to the ultra filtration (UF) tank T301 whose level is measured by sensor LIT301. In the pre-treatment stage (P2) the conductivity, pH, and Oxidation-Reduction Potential (ORP) are measured to determine the activation of chemical dosing pumps to maintain water quality. UF stage (P3) is used to remove the bulk of the feed water solids and colloidal material by using fine filtration membranes that let pass only small molecules. Any free chlorine in the filtered water is destroyed in stage 4, the dechlorination stage (P4), using an ultraviolet chlorine destruction unit and by dosing a solution of sodium bisulphite. The reverse osmosis (RO) stage (P5) is designed to reduce inorganic impurities by pumping the filtrated and dechlorinated water with a high pressure (pump P501) into RO containers. Stage P6 is used to clean the ultrafiltration unit in P3 using a backwash process.

Communication architecture: A multi-layer network enables communications across all components of SWaT.

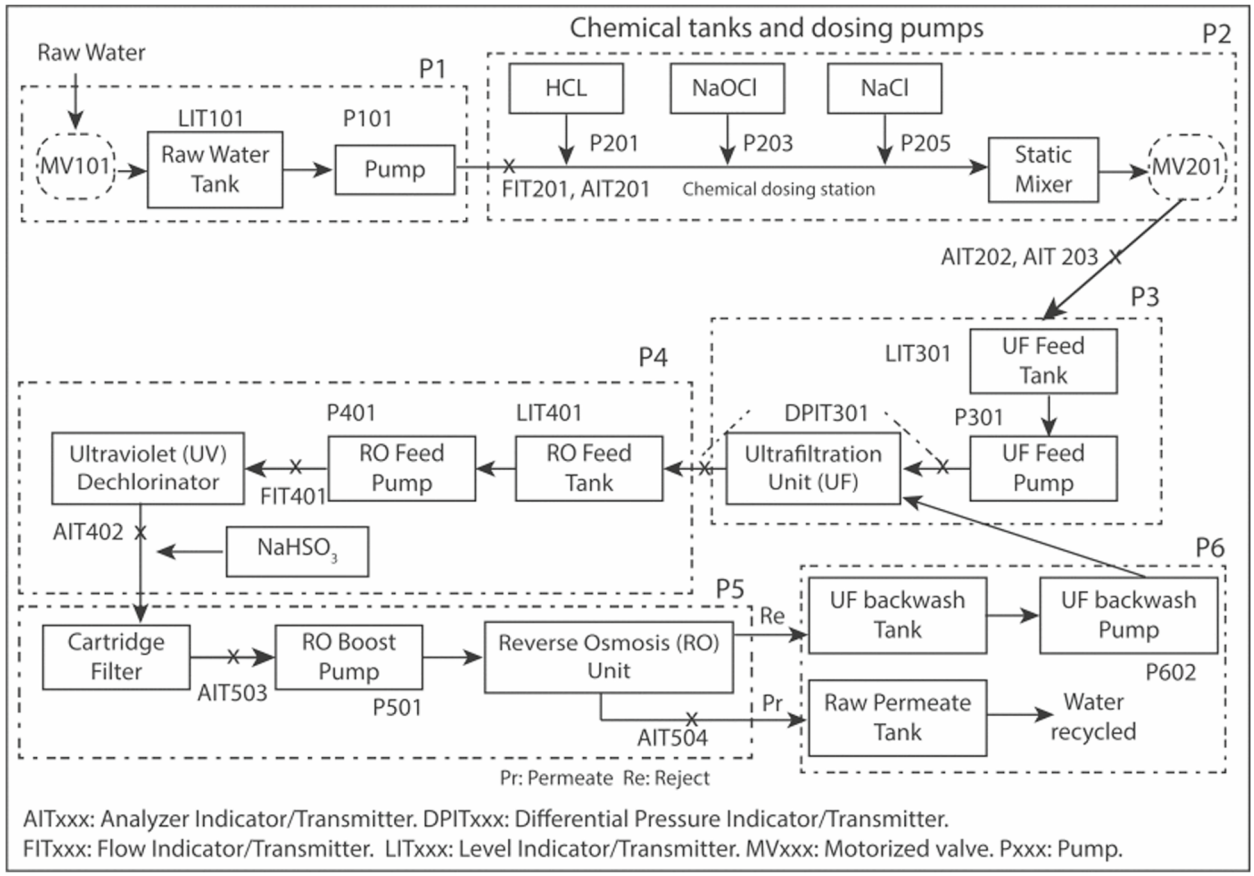

Fig. 1 Overview of the Secure Water Treatment (SWaT) plant

The ring network at each stage at level 0 enables PLCs to communicate with sensors and actuators at the corresponding stage. A star network at level 1 enables communications across PLCs, Supervisory Control and Data Acquisition (SCADA) system, the Human Machine Interface (HMI) and the Historian. Both wired and wireless options are available at level 1 and at level 0.

WADI

WADI is a scaled down version of a water distribution system found in cities (Ahmed et al. 2017). As shown in Fig. 2, WADI consists of three stages namely, primary stage (P1), secondary stage (P2) and return water stage (P3). P1 stage consists of two raw water tanks of 2500 liters each. There exists three incoming sources to the primary stage water tanks, namely, public utility water, SWaT treated water, and return water stage. Water quality is monitored before entering into the raw water tanks using sensors such as conductivity, turbidity, pH and ORP. A level sensor and flow meter are installed to monitor the level of the tanks and incoming flow into the tanks, respectively.

Stage P2 consists of two Elevated Reservoirs (ER) and six consumer tanks. A pump in P1 pumps water from raw water tanks to the ER tanks based on the set point levels of the tanks. Each consumer tank is assigned a preset demand pattern. Water flows from the ER to consumer tanks via gravity or booster station based on high or low demand consumption. Two water quality monitoring stations at upstream and downstream of ER tanks are installed to measure water quality properties. Once the consumer tanks are filled, water drains into the P3 stage. Further, based on the raw water tank level, water from P3 flows into stage P2.

Communication architecture: WADI consists of three Programmable Logic Controllers (PLCs), each PLC controls a different subprocess. These PLCs use National Instrument Compact RIO (Remote Input Output) devices. The communication network contains three layers, namely, layer-0 (L0), layer-1 (L1) and layer 2-(L2). L0 is at the process level and connects actuators/sensors and I/O modules via RS485-Modbus protocol. The second layer L1 is the plant control network where all PLCs are connected to a central node in a star topology. Communication among PLCs and Remote Terminal Units (RTUs) occurs over Ethernet switches using NIP/SP based on TCP and High Speed Packet Access (HSPA) cellular gateways using GPRS modem. The third layer L2 is a communication network between a touch panel HMI and the plant control network. This network is implemented using star topology and consists of PLCs and RTUs. A firewall isolates the enterprise network from the plant control network. A SCADA workstation provides an interface between the plant operators and PLCs for remote monitoring and control.

SWaT and WADI interconnection

SWaT and WADI are connected through a physical pipe. The treated water from the RO stage in SWaT can be made to flow through this pipe to WADI as shown in Fig. 3. The valve 1_MV_005 is responsible for the flow of treated water into the raw water tanks of P1 stage (WADI). When the raw water tank level (1_LT_001) falls below Low state (defined by the user), Stage-1 PLC sends a command to the valve 1_MV_004 to CLOSE and 1_MV_005 to OPEN. Further, this status of 1_MV_005 is sent to the RO stage in SWaT to turn ON pump P601. Similarly when the raw water tank level reaches high state, valve 1_MV_004 is set

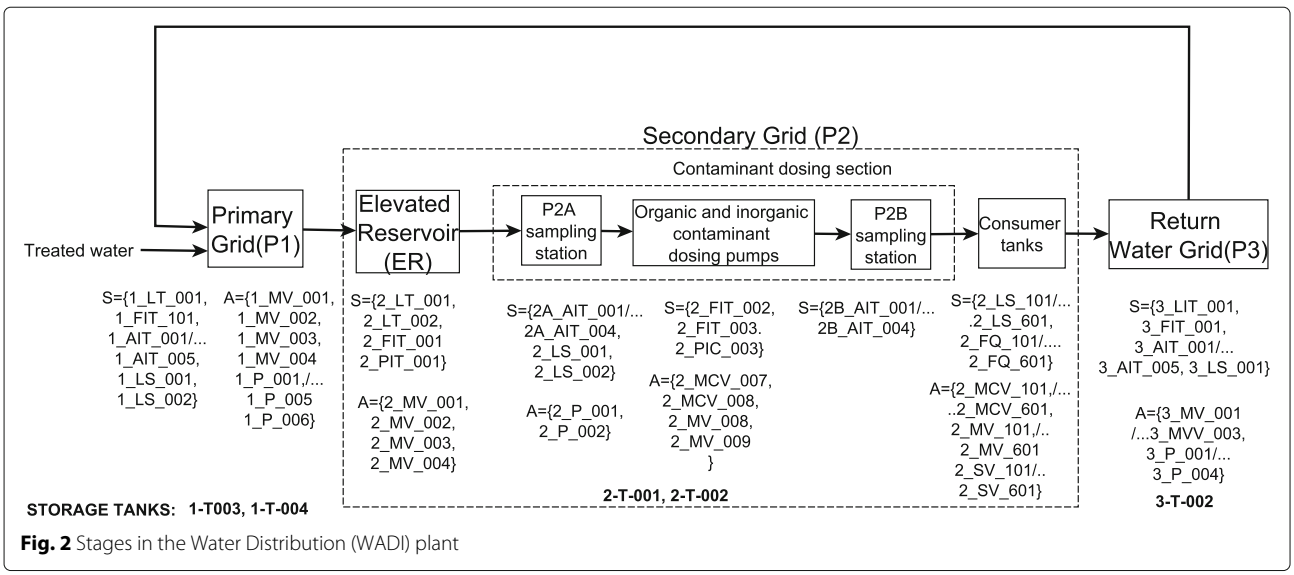

Fig. 2 Stages in the Water Distribution (WADI) plant

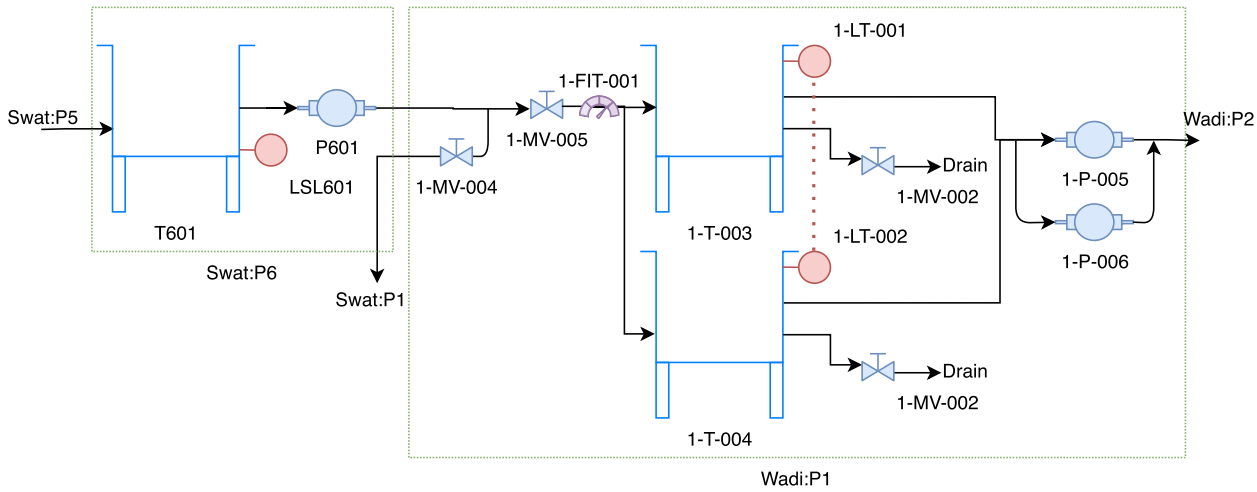

Fig. 3 Interconnection of SWaT and WADI via valve 1-MV-005. Opening 1-MV-005 causes the treated water to flow from SWaT to WADI

to OPEN, 1_MV_005 to CLOSE, and pump P601 is turned OFF. SWaT and WADI are clearly interdependent based on condition 1 (as discussed in "Interdependency among critical infrastructure" section), i.e. input of one system is the output of the other.

Design of experiments

Experiments were designed to investigate the cascading effects of cyber-attacks on SWaT and WADI. Design of such experiments includes, as described below, the design of attacks, choice of an attack detection mechanism, and the tools used to launch the attacks.

Attacker and attack models

We derive an attack model based on the attacker's intention. Initially, the attack model is developed for a single system and then extended to interconnected systems.

Let V_A denote a set of components that could serve as potential attack targets.

$$V_A = \{v_{a1}, v_{a2}, \ldots, v_{an}\}, V_A \subseteq CI_A \quad (1)$$

Let us assume that an attacker wishes to realize intention I and formulates the best approach (AP) to realize it. Hence, we define an attack as a pair:

$$A = \{AP, I\}. \quad (2)$$

An attack procedure is a sequence of steps executed on one or more stages of a CI. Thus, AP is defined as an ordered sequence of attacks written as

$$AP = \{AS_1, AS_2, \ldots, AS_n\} \quad (3)$$

where AS_i is a the i^{th} attack step. Each attack step AS_i is defined as a tuple consisting of attack points (ap) and an attack function (af).

$$AS_i = \{ap, af\} \quad (4)$$

Here af is the attack function that captures the manner of launching an attack on ap. For the attack to be possible, $ap \in V$.

As an example, let us define an attack A where the attacker intends to empty tank 1 (Fig. 4) while remaining undetected. Here the set of attack targets V includes all sensors and actuators in the system such that $V = \{$*Flow Meter*, *Tank 1*, *Valve In 1*, *Valve Out 1*, *Level Sensor 1*, *Tank 2*, *Valve In 2*, *Valve Out 2*, *Level Sensor 2*, *Pump*$\}$. The intention of this attack is defined as $I_A =$ *Empty Tank 1*. First step, AS_1, in this attack A is represented as AS_{1A}. In this step, the attacker spoofs the value of *Level Sensor 1* so that the controller is unable to determine the actual level of water in tank 1. ap for AS_{1A} is *Level Sensor 1* and af for AS_{1A} is spoofing the value of ap. Next, the attacker opens *Valve Out 2*. This is the second step of attack referred to as AS_{2A}. This is followed by the third step AS_{3A} which is to start the *Pump*.

Next, we extend the attack procedure described above for single system to interconnected systems. Consider two interconnected systems CI_A and CI_B. This combination leads to two sets of potential attack targets, namely, V_A and V_B. The attack model can be defined as proposed above for the interconnected system by combining them into one set such that $V = V_A \cup V_B$. Once the new V is defined, we define AP using the steps above. The other steps follow in a similar manner.

For example, in Fig. 5, let us define an attack ***Ad*** where the attacker intent is to drain Tank A. Here the set of components for system A is $V_A = \{$*Tank A*, *Pump A*$\}$, and set of components of system B is $V_B = \{$*Valve In B*, *Tank B*, *Level B*, *Valve Out B*, *Valve Drain B*$\}$. So the final $V = V_A \cup V_B$. To realize the intention, first the attacker OPENS *Valve In B*. This is the first step AS_{1Ad} in the attack procedure AP_{Ad}. The next step AS_{2Ad} is to turn *Pump A* ON. Last

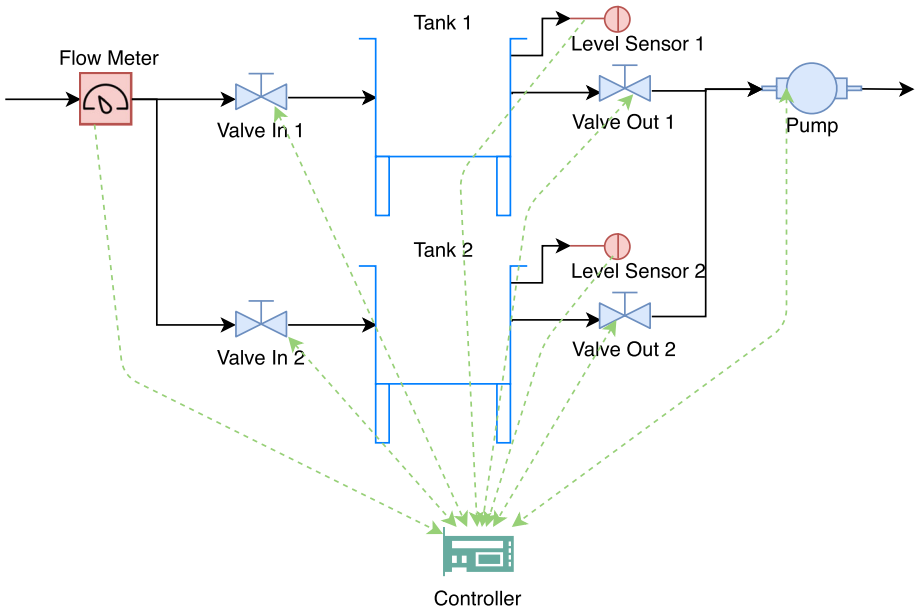

Fig. 4 Example of a Cyber-Physical Infrastructure

step AS_{3Ad} is to OPEN *Valve Drain B* when *Level B* reaches High while keeping *Pump A* ON and *Valve In B* OPEN.

Invariants

An invariant is a physical condition that must hold true in a given state of a process (Adepu and Mathur 2016a). There are many ways to derive invariants in a process like material balance, energy balance, and reaction stoichiometry (Gadewar et al. 2002; 2001; Kumar and Kaistha 2019). Data driven machine learning approaches can also be used to derive invariants (Chen et al. 2018; Feng et al. 2019). However, these methods assume process anomaly arising from component failure or defective operation. In contrast to the existing methods, Adepu and Mathur (2016a) works concerned with the strategic manipulation of sensor measurements and actuators while an attacker can maintain the invariants to satisfy but cause the process to move into an abnormal state. Therefore, in this paper, the works (Adepu and Mathur 2016a) were used as basis to derive the invariants for detecting cyber-attacks across the systems. An invariant captures dependence across state variables such as pH, pressure, and tank level. Invariants serve as the basis for detecting process anomalies, i.e., deviations from the normal process behavior. In this paper, invariants are derived from the process design. As an example, consider Fig. 4 in which 'Level Sensor 1' measures the water level in 'Tank 1' and is made available to the 'Controller.' 'Valve In 1' and 'Valve Out 1' are inlet and outlet valves, respectively, for 'Tank 1.' The states of 'Level Sensors 1' are defined as L(ow) and H(igh) and the states of 'Valve In 1', 'Valve Out 1' and 'Pump' are defined as OPEN/CLOSE or ON/OFF. An invariant that

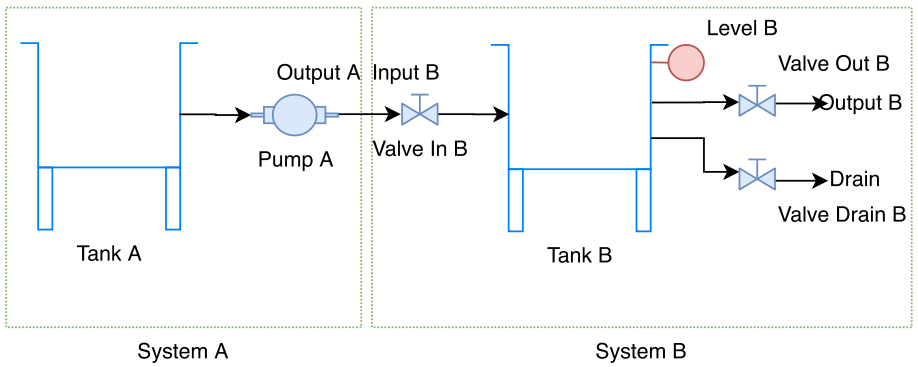

Fig. 5 Example of a Interconnected System

captures relationships across the valves and the pump can be defined as follows.

$$\text{Level Sensor 1} \leq \text{L} \Rightarrow \text{Valve In 1} = \text{OPEN} \wedge \text{Valve Out 2} = \text{CLOSE} \wedge \text{Pump=OFF} \quad (5)$$

When the level sensor reaches the L(ow) state, the inlet and outlet valves should be in the OPEN and CLOSE states, respectively, and the pump must be turned OFF. This condition must hold at all times. Violation of this invariant is considered as a process anomaly. Further, this approach can be extended to multiple systems. This extension is done by deriving *distributed invariants* that include state variables from across two or more connected systems. Distributed invariants are invariants defined using states from different systems and relationship that must hold between two systems that are interconnected. Depending on how the two systems are interconnected (condition of dependency), these relationship may differ as mentioned in "Interdependency among critical infrastructure" section. These invariants are derived by using the condition of dependency between the multiple interconnected systems. For example, from Fig. 5 we can see that if *Pump A* is ON, *Valve In B* has to be OPEN. This is the 'condition of dependency' for this interconnection.

$$\text{Pump A} = \text{ON} \Rightarrow \text{Valve In B} = \text{OPEN} \quad (6)$$

Also, if Tank B is getting filled, it should not be getting drained at the same time and vice versa. This condition can be represented by the following invariants. These invariants are invariants from system B.x

$$\text{Valve In B} = \text{OPEN} \Rightarrow \text{Valve Drain B} = \text{CLOSE} \quad (7)$$

$$\text{Valve Drain B} = \text{OPEN} \Rightarrow \text{Valve In B} = \text{CLOSE} \quad (8)$$

we can combine Invariant 6 with 7 and 8 to get a set of distributed invariants 9 and 10 as follows.

$$\text{Pump A} = \text{ON} \Rightarrow \text{Valve Drain B} = \text{CLOSE} \quad (9)$$

$$\text{Valve Drain B} = \text{OPEN} \Rightarrow \text{Pump A} = \text{OFF} \quad (10)$$

The distributed invariants 9 and 10 can be used to detect attack *Ad* described in "Attacker and attack models" section.

In this study, we derived such invariants for both SWaT and WADI and distributed invariants across the two systems.

Attack tools

Attacks were designed manually and launched using two tools developed in iTrust. These tools are described below.

Attack tool for SWaT: To support research and experiments in SWaT, iTrust engineers have developed a flexible scripting tool named SWaTAssault (Urbina et al. 2016a)). This tool enables one to programmatically override and manipulate control signals between PLCs, sensors, and actuators. SWaTAssault was used to simulate the behavior of compromised sensors and actuators, and launch attacks on SWaT.

Attack tool for WADI: A multi-layered network comprising multiple protocols is deployed in WADI. National Instruments Publish-Subscribe Protocol (NI-PSP) was used WADI network. The components of NI-PSP include a server called the Shared Variable Engine that hosts values, timestamps, and other shared variable information (LabVIEW 2019). Shared Variable Engine is a software framework and provides access to all shared variables over a network. A tool named NiSploit (Adepu et al. 2017) was used in the experiments to launch attacks on WADI. NiSploit uses custom LabVIEW Virtual Instruments (VIs) that can communicate with shared variables located in different PLCs using NI-PSP.

Based on the attack model mentioned above, several attacks were designed and launched (Table 1) The attacks were launched to study the forward and backward cascading effects on the SWaT and WADI interconnected system. A description of the attacks and their impact is in "Cascading effects of attacks on SWaT and WADI" section.

Cascading effects of attacks on SWaT and WADI

In a system, the direction of the flow of commodities or information determines the direction of the system. If the commodities or information flows from point A to point B then point A and point B are said to be upstream and downstream respectively. During an attack, if the attack point is downstream and the impact is observed upstream, it is called the backward cascading effect. Similarly, when an attack point is upstream and the impact is observed downstream it is called the forward cascading effect. For example, from Fig. 3 that treated water obtained from the SWaT is fed into the water distribution system. Therefore, SWaT is an input to the WADI system and it can be stated that SWaT is upstream and WADI is downstream in the interconnected system. If an attacker launches an attack only on the SWaT system and the attack propagates to the WADI system. As a result, the impact of the attack can be observed in the WADI system. This type of attack propagation i.e, from SWaT to WADI is defined as a forward cascading effect. In contrast to this, if the attack occurs on the WADI system and the impact is observed on the SWaT system, then it can be defined as a backward cascading effect between SWaT and WADI.

In this paper, the backward and forward cascading effects were demonstrated experimentally using attacks A_3 and A_4 respectively (refer Table 1). Once the system reaches an undesirable state due to the actions of an

Table 1 Attacks launched on SWaT and WADI

Attack design			
Attack	**Intention**	**Target CI and Procedure**	
		SWaT	**WADI**
A_1	RO permeate tank overflow	Pump P601	Attack sequence: 1. Stealthy attack on 1_LT_001 2. Replay attack on 1_FIT_001
A_2	Damage P501	Increase speed of P501 to meet the demand	Increase consumer tank m demand in stage P2
A_3	Drain the RO permeate tank in SWaT	-	Attack on water quality sensors in P1 stage
A_4	Cut-off water supply to the consumer tanks in WADI	Attack sequence: 1. Attack on P-601, LS601 2. Attack on P-501 3. Attack on P-401, LT-401	-

attacker, the attack is said to be realized. Let us consider the interconnected system in Fig. 5. If the attack is performed on System A and System B reaches an undesirable state, it is termed as a forward cascading attack. Similarly, if the attack is performed on System B and System A reached an undesirable state, it is termed as a backward cascading attack.

Attacks on SWaT and WADI

A set of cyber-attacks were designed to understand how an attack in one system affects the process in another. These attacks were launched on SWaT and WADI and their effects monitored via several sensors. In this work, we choose the attack points that were either immediately downstream or upstream of the interconnection link.

Invariants for SWaT and WADI, as well as those across the two systems, were implemented in the two systems for detecting any process anomaly resulting from each attack. The attacks are summarized in Table 1. Description of each attack, its impact, and detection are described next.

Attack A_1: In this attack, the attacker's intention is to overflow the RO permeate tank in SWaT. Based on the attacker's capabilities and knowledge, the attack can be launched in two ways: 1) attack on SWaT ($A_{1.1}$) and 2) simultaneous, i.e. coordinated, attack on SWaT and WADI ($A_{1.2}$). Initially the attack was launched only on SWaT to study the propagation of its effects to WADI. This was followed by the simultaneous attack on SWaT and WADI.

$A_{1.1}$: Attack on SWaT: The intention of this attack is to overflow the RO permeate tank in SWaT ($I_{A_{1.1}}$). The intention can be realized through the level 0 attack in SWaT by switching pump P601 OFF. This is a level 0 Man in the Middle attack (MITM) attack where packets from a PLC are modified and the modified packets sent to one or more physical processes such as actuators and sensors ($AS_{1A_{1.1}}$). The communications protocol used in this case is Ethernet IP. The steps to launch AS_1 are described below.

SWaT network topology: The network topology used in level 0 is a ring configuration where all the nodes are connected to two other nodes as shown in Fig. 6. There are two PLC's, one primary and the other secondary, RIO (Remote Input/Output Unit) and ETAP (EThernet Access Point). As shown in Fig. 6, a bridge is setup with an attacker device in between the PLC and RIO using bridge controls. Once the bridge setup is verified the packets are modified using a dissector built using the SCAPY tool (Biondi 2010).

As shown in Fig. 7, the attack starts at 2247 second mark. The impact of this attack can be observed in WADI as described next. Figures 8 and 9 show the status of primary grid water tank level (1_LT_001) and flow meter (1_FIT_001), respectively, in WADI. Note the High and Low set points of 1_LT_001 are 65% and 60% of the tank height, respectively. The attack on P601 in SWaT started when 1_LT_001 reaches the Low set point, i.e. at the 2247 second mark. At this time instant, it can be seen in Fig. 9 that valve 1_MV_004 moves from ON to OFF position. As a result, 1_MV_005 turns ON and enables flow of water from the RO tank to the primary grid tank. However, 1_FIT_001 reading is zero as shown in Fig. 9. It can therefore be concluded that there is no inflow into the primary grid tanks. As a result the RO tank level in SWaT starts to overflow at approximately 4050 second mark as observed in Fig. 7. Further, the level in the primary grid tank decreases continuously and reaches at 30% mark as shown in Fig. 8 thus realizing the attacker intent.

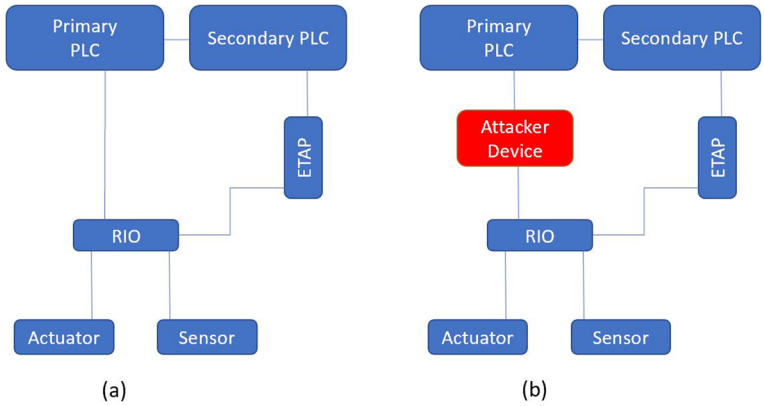

Fig. 6 a Example ring topology in SWaT and (**b**) with an attacker inserted as Man-in-the-Middle. In this configuration, the attacker can eavesdrop and manipulate all traffic between RIO and the primary PLC

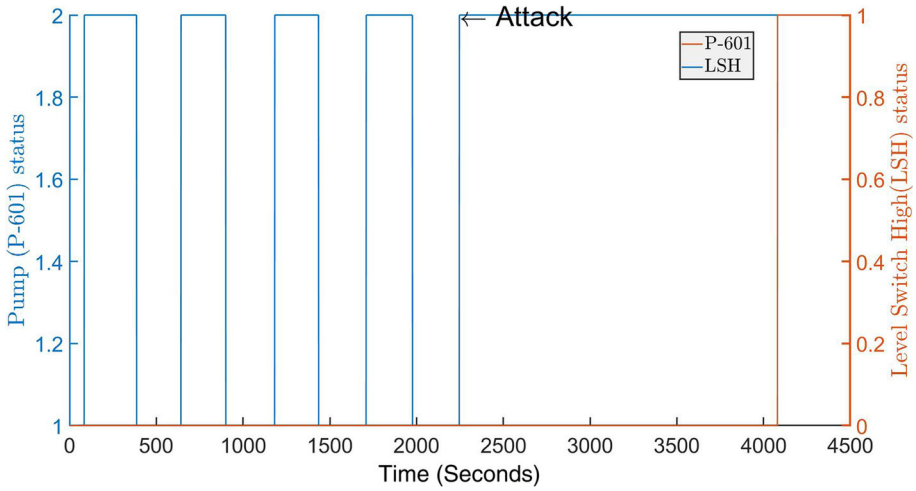

Fig. 7 Left and right axes show the P-601 and LSH status in SWaT respectively

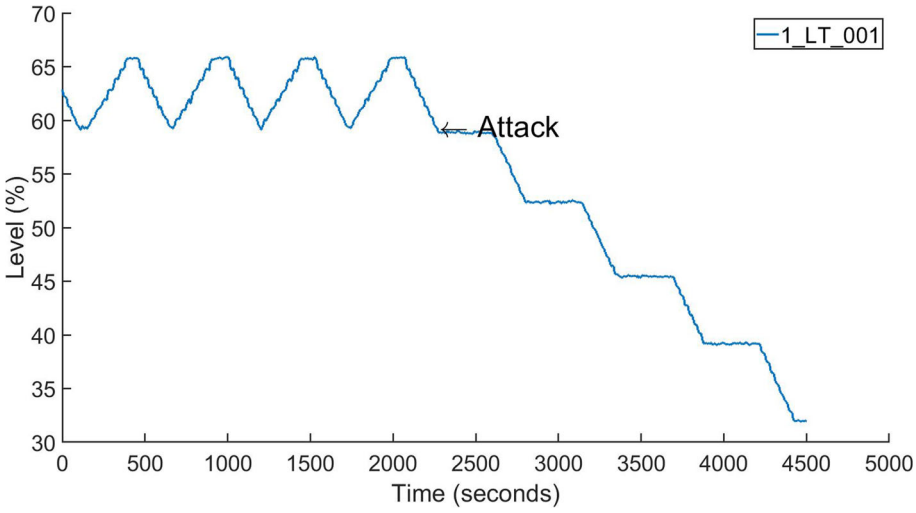

Fig. 8 1_LT_001 level status in primary grid of WADI

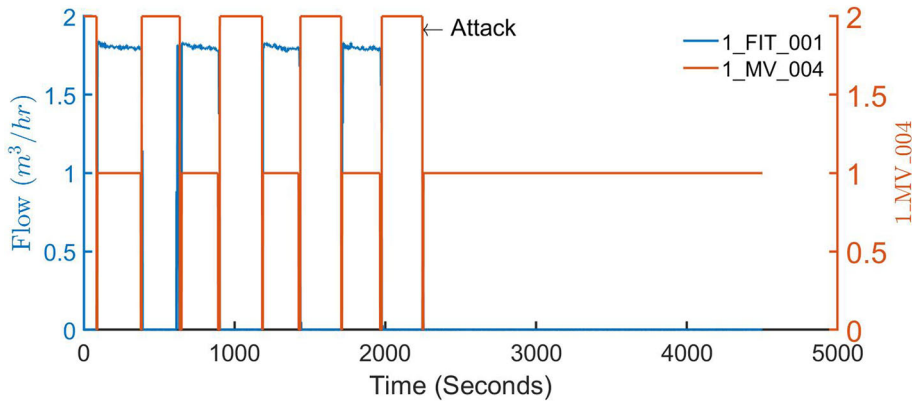

Fig. 9 1_LT_001 level status in primary grid of WADI

Attack detection: Three invariants, listed below, are of interest in detecting attack $A_{1.1}$. Invariant 11 is derived for WADI whereas Invariants 12 and 13 denote the distributed invariants across SWaT and WADI. Invariant 11 represents the condition between the level of raw water tank in stage 1 of WADI, status of 1_MV_004, and that of 1_MV_005. Invariant 12 describes the condition that determines when pump P601 should be ON. Whenever P601 is ON and 1_MV_004 is CLOSED, there should be an inflow to the raw water tank that is indicated by the flow meter 1_FIT_001. This condition is captured as Invariant 13. From Figs. 7 and 9 it can be observed that after the attack is launched pump P601 is ON and valve 1_MV_004 is in CLOSED position though the 1_FIT_001 reading is recorded as zero. This observation is adequate to conclude that Invariant 13 is violated and hence the process anomaly detected.

$$1\_LT\_001{=}L \Rightarrow 1\_MV\_004{=}CLOSE \wedge 1\_MV\_005{=}OPEN \tag{11}$$

$$1\_MV\_004 {=}CLOSE \wedge \neg LSL601 \Rightarrow P601{=}ON \tag{12}$$

$$P601{=}ON \wedge 1\_MV\_004{=}CLOSE \Rightarrow 1\_FIT\_001 > 0.001 \tag{13}$$

$A_{1.2}$*: Simultaneous attacks on SWaT and WADI*: The attacker's intention remains as in the previous attack, i.e. to overflow the RO permeate tank in SWaT ($I_{A_{1.2}}$). The steps for launching simultaneous attack on SWaT and WADI are as follows. First, the attack is launched on WADI. Attacking WADI requires a replay attack on 1_FIT_001 ($AS_{1A_{1.2}}$) and a stealthy attack on 1_LT_001 ($AS_{2A_{1.2}}$). This is followed by an attack on SWaT ($AS_{3A_{1.2}}$). The steps for attacking SWaT are the same as in $A_{1.2}$ ($AS_{3A_{1.2}} = AS_{1A_{1.1}}$). Note that even though $AS_{1A_{1.1}}$ and $AS_{2A_{1.1}}$ are launched before $AS_{3A_{1.2}}$, they remain active until after $AS_{3A_{1.2}}$ is inactive. The sequence of attacks among $AS_{1A_{1.1}}$ and $AS_{2A_{1.1}}$ does not impact the outcome.

1. ***Attacking WADI:*** Attacks on WADI are described in the following.
   (a) $AS_{1A_{1.1}}$ ***Replay attack***: This attack is launched on 1_FIT_001. The attacker observes and records the data for certain time duration and replays the recorded measurements during the attack. The recorded measurements are replayed when valve 1_MV_004 is in CLOSED position, i.e., valve 1_MV_005 is in OPEN position. Whereas, when 1_MV_004 is in OPEN position, i.e., 1_MV_005 is in CLOSED position, 0 is replayed instead of the recorded data. Figure 10 shows the valve (1_MV_004) position and flow meter readings (1_FIT_001) during the replay attack. The attacker launches the replay attack at 3443 second mark and ends at 6228 second mark as shown in the figure.
   (b) $AS_{2A_{1.1}}$***: Stealthy attack*:** In order to launch a stealthy attack it is assumed that the attacker has the knowledge of the physical model of the plant and the anomaly detection mechanism, and can secretly manipulate the sensor readings. The dynamics of the water tank level can be derived from first principles. The relationship between the water height and the inlet and outlet flow rate is captured below.

$$A\frac{dh}{dt} = Q_{in} - Q_{out} \tag{14}$$

where A is the cross-sectional area of the water tank, and Q_{in} and Q_{out} are inlet and outlet flow rates, respectively. The following Linear Time Invariant model can be derived assuming a discrete time interval 1 second.

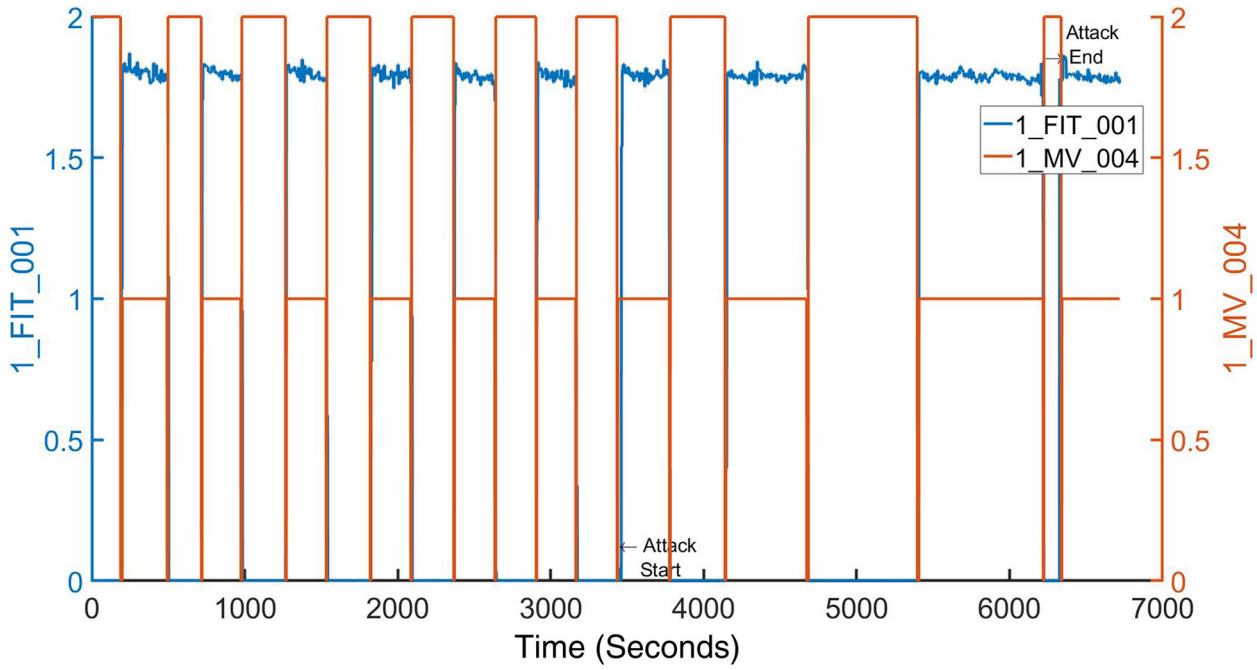

Fig. 10 Replay attack on 1_FIT_001

$$h_{k+1} = h_k + \frac{Q_{in} - Q_{out}}{A} \tag{15}$$

The change in the level during the attack is estimated using Equation 15. Further, the replayed value of 1_FIT_001 is used as the inlet flow rate Q_{in} in the above Equation. Figure 11 shows the stealthy attack start and end points on level sensor 1_LT_001.

2. Attack on Pump P601 ($AS_{3A_{1.2}} = AS_{1A_{1.1}}$): As explained in "SWaT and WADI interconnection" section, pump P601 turns ON/OFF based on the status of valve 1_MV_004. To perform this attack on P601 the attacker must synchronize with the status of valve 1_MV_004. Whenever 1_MV_004 is in CLOSED position, pump P601 should be ON. To overflow the RO tank, the attacker needs to launch the attack to turn OFF the pump as explained above. When 1_MV_004 is in OPEN state, PLC P6 sends a command to turn OFF P601. Therefore, the attacker must end the attack at this time. This cycle is repeated until the RO tank overflows. Figure 12 shows the different start and end points for the attack on P601. It can be observed from Fig. 13 that the level switch LSH601 status reaches the high set point when the attack ends.

Attack Detection: First, the distributed invariants derived in Eqs. 11, 12 and 13 are applied. Due to the replay attack on WADI, these invariants are not violated, indicating that the attack is not detected. An attack detection framework, based on Linear Time Invariant model of WADI together with the CUSUM detector (Ahmed et al. 2017) is used on level sensor 1_LT_001. As shown in Fig. 14, the CUSUM residuals are within the limits. Hence CUSUM is also unable to detect the attack on 1_LT_001. Therefore, it can be concluded that the attacker achieves the goal by successfully launching replay and stealthy attacks.

Attack A_2: The attacker's intention is to damage pump P501 in SWaT(I_{A_2}). This can be achieved by increasing the demand from the consumer tanks in WADI (AS_{1A_2}). The attacker increases the demand of the consumers as shown in Fig. 15. To meet this demand pump P501 speed is increased (AS_{2A_2}) as can be observed from Fig. 16. The attacker continues to increase the demand i.e, AS_{1A_2} and AS_{2A_2} are launched in a loop continuously until the pump reaches its maximum speed. The attack was removed shortly after due to the safety of the pump. However, if this attack continues for a longer period, it will damage the pump.

Attack A_3: This attack demonstrates how an attacker can impact SWaT by launching an attack on WADI and that there is a *backward cascading effect* between SWaT and WADI. The attacker intends to drain the RO permeate tank in SWaT (I_{A_3}) and hence selects water quality sensors in stage P1 as the target. As shown in Fig. 17, the attacker increases the conductivity reading from 5 to 500 at 4000

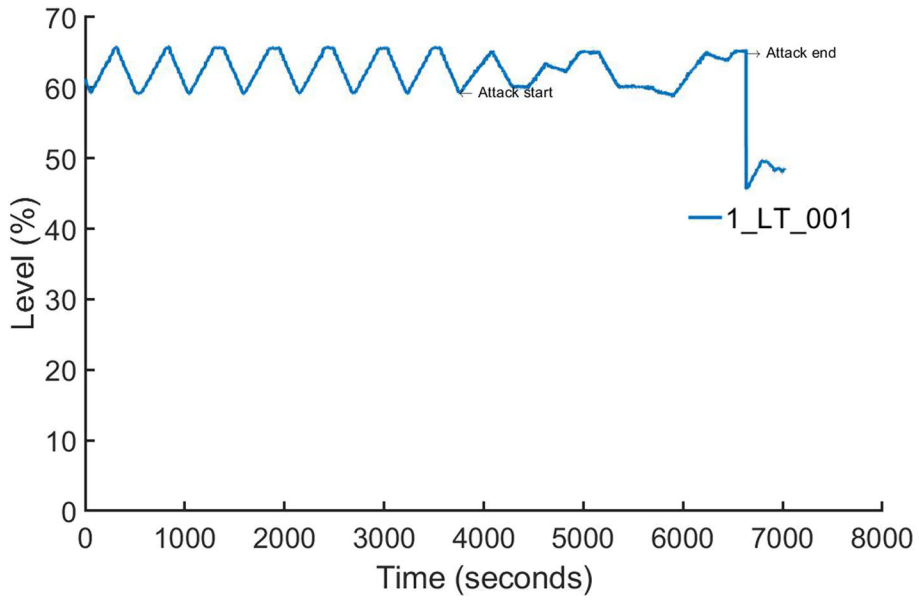

Fig. 11 1_LT_001 level indicator during simultaneous attack on SWaT and WADI

second (AS_{1A_3}) mark. Consequently the PLC assumes that the water quality is not within the acceptable range. This leads to the opening of valves 1_MV_002 and 1_MV_003 to drain the water in the raw water tank. When the level reaches the Low mark, water from the RO tank will be supplied. Due to this attack, water supply from the RO tank is not adequate to meet the raw water tank requirements. Consequently the RO tank level reaches the Low mark triggering LS601 at 7500 second as shown in Fig. 18.

Attack Detection: As the water flows from SWaT to WADI, it is expected that the water quality in stage 5 of SWaT and stage 1 of WADI should be the same. Also, if the

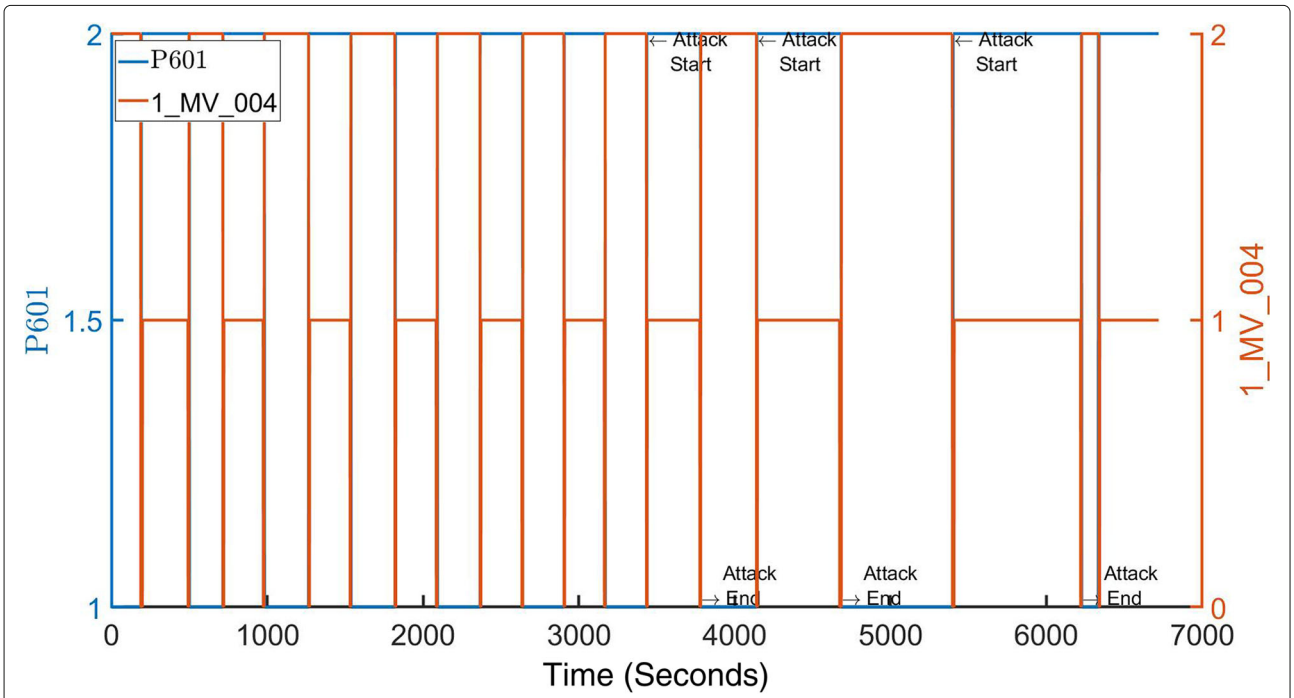

Fig. 12 Pump and valve statuses in SWaT and WADI respectively

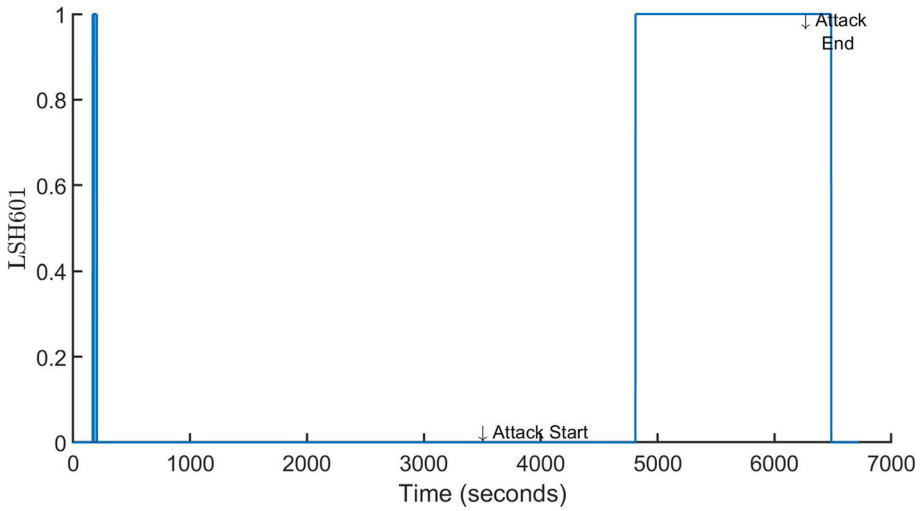

Fig. 13 RO permeate tank High Level switch status in SWaT

water conductivity is less than 20 $\mu s/cm$, the drain valve for tanks in raw water stage (stage 1) of WADI should be closed. Therefore, the distributed Invariant 16 can be used to detect this attack. Moreover, when the water flows from SWaT to WADI the raw water tanks should not be draining. This condition is represented as Invariant 17.

$$\text{AIT504} < 20 \Rightarrow \text{1\_MV\_002=CLOSE} \wedge \text{1\_MV\_003=CLOSE} \quad (16)$$

$$\text{P601=ON} \Rightarrow \text{1\_MV\_002=CLOSE} \wedge \text{1\_MV\_003=CLOSE} \quad (17)$$

Attack A4: In this attack, the attacker's intention is to cut-off water supply to consumer tanks in WADI (I_{A_4}). To realise the intention the attacker targets P501 pump in SWaT (AS_{1A_4}). This attack also demonstrates the *forward cascading effect* between SwaT and WADI. in this attack, the attacker launches an attack only on SWaT system and the impact can be observed in WADI system. As shown in Fig. 19, the attacker switches OFF the pump at 3000 second mark. This attack is continued until the water supply to consumers cuts-off. This happens between 12000 and 14000 second marks as evident from Fig. 20. It is observed that not all the consumer tanks are

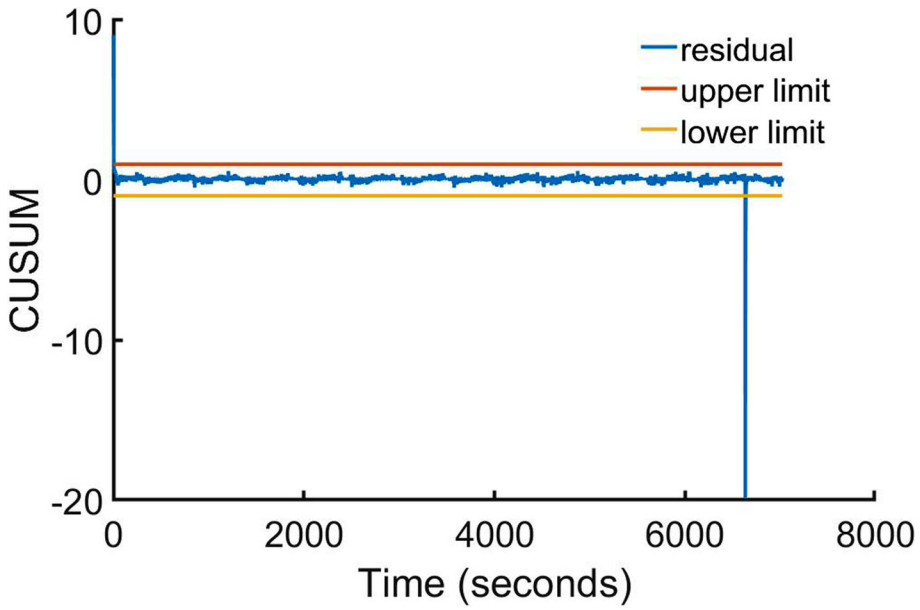

Fig. 14 Residual estimate of level sensor 1_LT_001

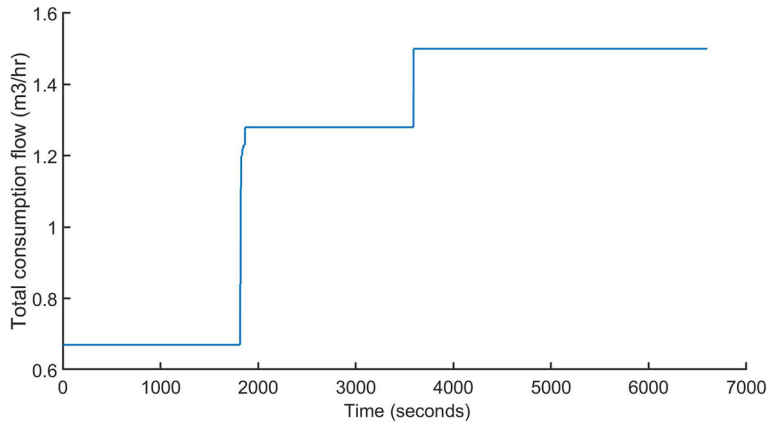

Fig. 15 Total consumption flow rate of consumer tanks in WADI

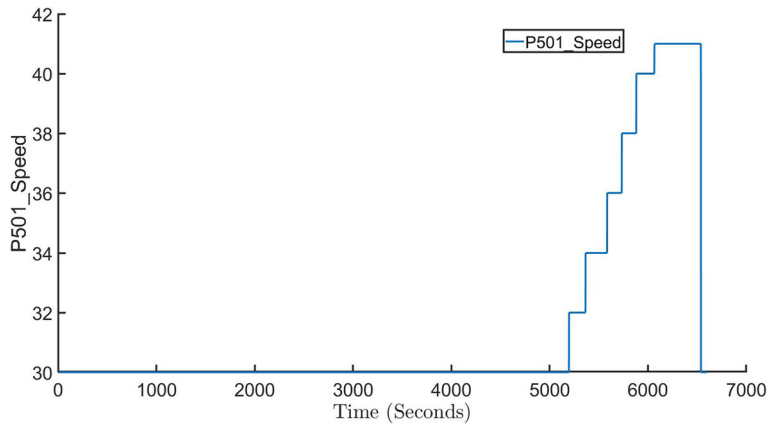

Fig. 16 Pump P501 speed in SWaT

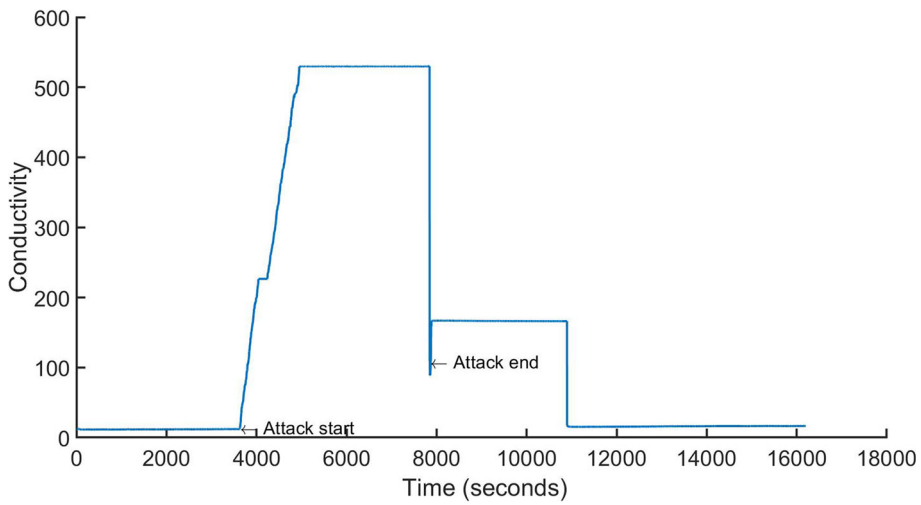

Fig. 17 Attack on conductivity sensor in WADI

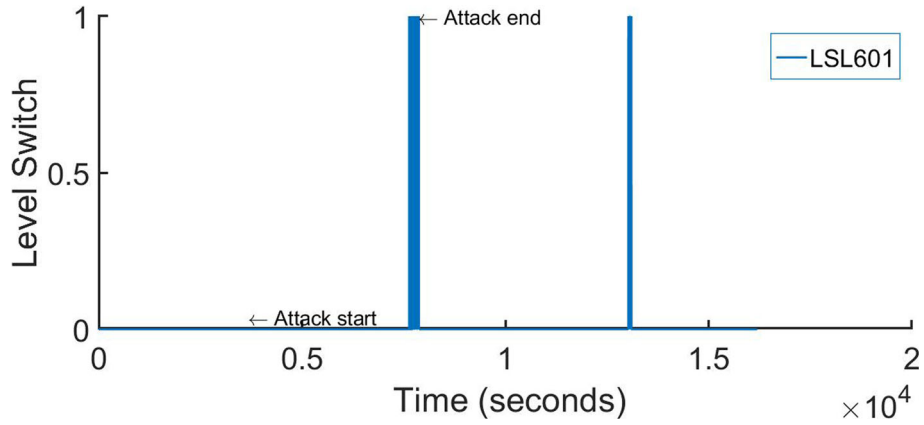

Fig. 18 RO tank Low level switch status in SWaT

simultaneously cut-off from water supply. This is due to the difference in spatial location of the consumer tanks.

Attack detection: In SWaT pump P501 should be ON when in stage 4 pump P401 is ON, the dechlorinator UV401 is ON, and flow meter FIT401 reading is above the LowLow (LL) set point. This condition is captured in Invariant 18. It is clear from the data that all three conditions are met but P501 remains OFF during the attack period. Hence, the anomaly resulting from this attack is detected.

$$\text{P401=ON} \wedge \text{UV401=ON} \wedge \text{FIT401} > \text{LL} \Rightarrow \text{P501=ON} \tag{18}$$

Discussion

Next, we point to key observations and challenges that would be faced by an attacker while designing and launching the attacks on interconnected systems.

Realizing attackers intention: Observations from the experiments conducted indicate that a cyber-attack on one system will likely impact the connected system. SWaT and WADI are interconnected in such a way that the output of SWaT flows into WADI as input. Experiments were designed to show attacks on interconnected systems, the forward and backward cascading effects. In these experiments attack A_4 shows the forward cascading effect on WADI when the attack is launched on SWaT. The attack on P501 cuts off water supply to WADI. Attack A_3 shows the backward cascading effect between SWaT and WADI. A different type of interconnection might have a different type of cascading effect. For example, if two systems are connected in a loop there is a possibility of a looped cascading effect. Such attacks/cascading effects are not performed in this paper as the testbeds used are not built in such a configuration.

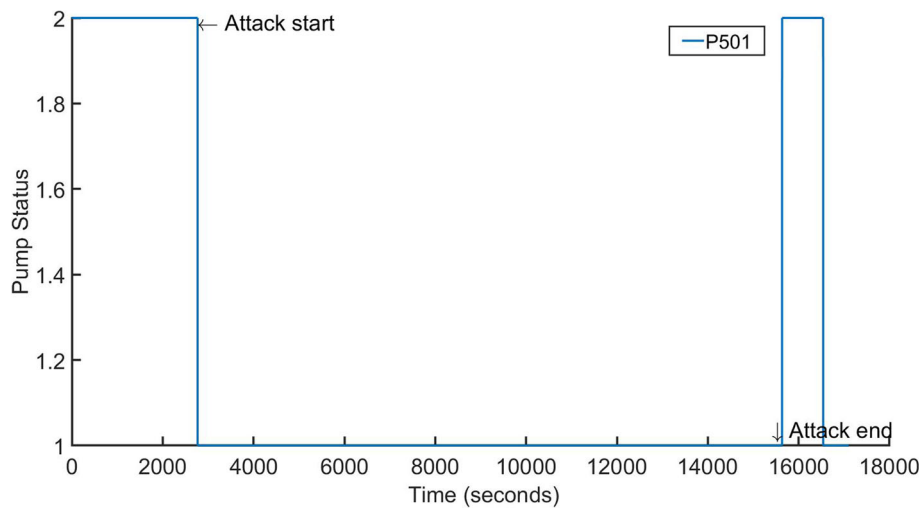

Fig. 19 Attack on the pump P501

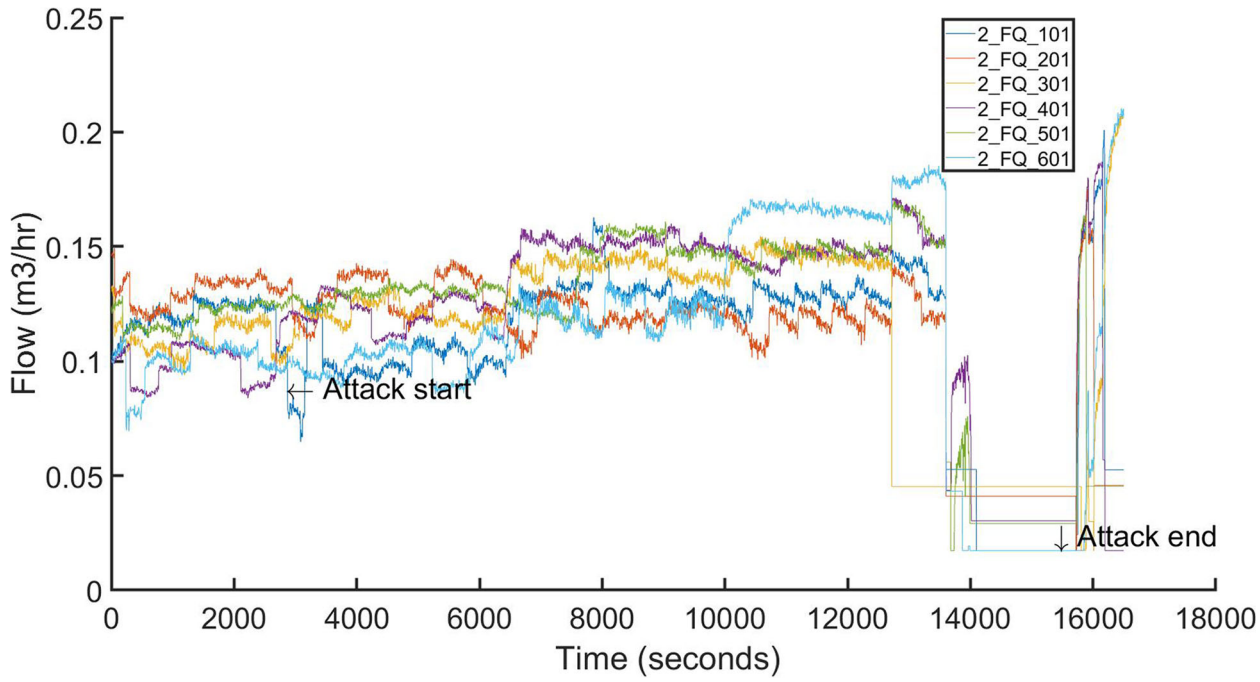

Fig. 20 Consumer tank input flow rates in WADI

Attack A_2 demonstrate how the attacker can launch attacks on both systems simultaneously in order to realise his/her intentions. It is to be noted that the attacker can also realise the intention by attacking only one system. However, such attacks can be detected in another system easily when there is a dependency. For example, in attack A_1, the attacker can realise the intent by targeting only SWaT. However, the distributed invariants can detect the attacks easily. To successfully hide the attack the attacker needs to target both systems.

It is to be noted that the designed invariants can detect the attacks once an actuator (valve) state is stabilized i.e, valve is in either open or closed position, but not in the transition state. However, water treatment and distribution systems dynamics evolve slowly, therefore, it is assumed that if an attack occurs during the transition period, the detection mechanism can still detect the attack before the system reaches to an unsafe state.

Design of experiments: It is observed that for an attacker it is important to choose the right set of sensors and actuators for an attack. To select such components and the appropriate attack point, the attacker needs to have prior knowledge of the systems and their dependency.

In our experiments the attacks were designed based on the attacker's intention. The attack points were chosen either in one system or in both in order to realise the intention. It is to be noted that the attack points were chosen either immediately downstream or upstream of the interconnection link. In general, the attacker may have a good knowledge of the immediate up-stream and downstream points of the interconnection link. Therefore, he/she tries to choose these points as potential attack points. However, the attack can propagate much further downstream in another system.

In attack A_4, the attack point P501 was chosen which is immediately downstream of the RO tank. The impact is observed in consumer tanks located towards the end of stage 2 of WADI as shown in Fig. 2. It is worth mentioning that by choosing such attack points the impact can be observed sooner. It is also possible to choose attack points in P1, P2, or P3 stages of SWaT. However, the intention may take longer to be realised. These points were chosen for the ease of experimentation.

Challenges in launching attacks: At least two attackers are required to launch some of the attacks designed in our experiments. Moreover, the attackers need to be communicating with each other to successfully launch the attack. For example, attack A_1 was performed on both SWaT and WADI. This attack required two attackers, one in SWaT and another in WADI. The attack on WADI was started before the attack on SWaT was launched. Uninterrupted communication was required between the attackers until the intention was achieved.

To successfully realize the attack on the interconnected system, the attacker needs information about all the different systems and how they are interconnected to each other. Lack of this knowledge will lead to either an unsuccessful attack or easy detection of the attack.

Applicability to other systems: The interconnected SWaT and WADI testbeds are based on real water treatment and distribution systems. However, they are scaled-down. The complexity of a real system is greater as there are large number of possible attack points, large numbers of interconnection links and the control logic between the interconnected variables will be more complex. Even though the methods used in this paper are scalable, creating invariants with many variables will be more challenging compared to the ones created in this paper.

On the other hand, for attackers, synchronizing between all the attack points for successful attacks, most of which will be on different networks, will be a challenging task. Also, as there are more interconnection links, an attacker has a wider choice of attack points that are immediate upstream or downstream of the interconnection links.

Related work

Significant research exists in modeling cyber-attacks and assessing their impact on CPS. In Berman and Butts (2012) the authors make an attempt to characterize cyber-attacks on an Industrial Control System. However, the characterization in Berman and Butts (2012) does not include several aspects of attacks such as start and end states, intents, and attack points. Attacks have been modeled as noise in sensor data (Kwon et al. 2013). Such attacks have also been referred to as state attacks or output attacks (Pasqualetti et al. 2011) and are often referred to as formal attack models. These attack modeling approaches consider a linear state model of the CPS control mechanism and add noise to either the state and/or to the control. The model so derived is then used to answer questions related to attack detectability and identification. Textbooks (Stamp 2011) on cyber security generally describe these attacks. These attacks include a variety of deception attacks including surge and bias (Stamp 2011). Several other graph based modeling techniques also exist and are derived from research in network security (Chen et al. 2011). Textual attack models have been proposed based on the CERT security incident taxonomy (Wasicek 2013). Control theoretic models (Kwon et al. 2013) reduce the entire attack space to a mathematically tractable noise and abstract the physical aspects whereas the attacks designed in this paper are from a cyber physical attacker model (Adepu and Mathur 2016b) and affords an opportunity to widen the attack surface. The investigation of attacks (Kang et al. 2016; Adepu et al. 2017; Adepu et al. 2020) and automatic generation of attacks (Chen et al. 2019) have been studied.

Petri net based models (Chen et al. 2011) capture the dynamics between the behavior of an attacker and the attack detection or defense mechanism in a CPS. The models account for failure types of a CPS and survivability. The attack model proposed here is useful in the design of cyber-attacks while a Petri net, as well as other graph models, are useful in analyzing the impact of an attack. Capability centric models (Teixeira et al. 2012) make use of the attacker's knowledge and capabilities in designing and launching attacks. This aspect is covered in the attack model proposed here in terms of the attack procedures though not as explicitly as in the literature. Thus, for example, the cyber-physical attack space in Teixeira et al. (2012) captures the different types of traditional network-based attacks, the domain model in this chapter captures the key elements of a CPS that might be an attacker's target. The information flow disruption attacks (Howser and McMillin 2014), as in the case of Stuxnet, can be modeled.

Single point attacks are similar to those in Cardenas et al. (2011) and Urbina and et al. (2016b), however, the attacks investigated in this paper are multi-point attacks where an attacker manipulate multiple data points. In Urbina and et al. (2016b) the authors have proposed a metric to capture the maximum deviation per unit time in sensor readings resulting from undetected attacks, and the expected time between false alarms. This metric is not suitable in the case of multi-point coordinated attacks involving multiple actuators and sensors. Further, attacks in the case study as in "Cascading effects of attacks on SWaT and WADI" section were launched on a larger scale than those in Urbina and et al. (2016b). Researchers have also explored false data injection attacks in electric power grids using simulation (Liu et al. 2011); these attacks are also single-point; and not coordinated as in our study. The Weaselboard (Mulder et al. 2013) uses PLC backplane to get the sensor, actuator values and analyses them to prevent zero day vulnerabilities. The use of invariants for detecting attacks on CPS has been proposed by several researchers. The work that relates most closely to the techniques used in DAD is in Gamage et al. (2010), Paul et al. (2011), and Rosich et al. (2014). In another work (Ahmed et al. 2018), the model from the plant dynamics and unsupervised learning was used for attack detection. Evaluated cascading impact of attacks on resilience of industrial control systems (Hau et al. 2020). In another work, zero residual attacks on industrial control systems are presented (Ghaeini et al. 2019).

Conclusions and future work

An experimental study was conducted to investigate the cascading effects of cyber-attacks on interconnected critical infrastructure. Experiments were designed and carried out on two operational testbeds namely, a water treatment and a water distribution system. Forward and backward cascading effects were studied to understand how an attack can propagate and impact these systems. An invariant-based approach was used for attack detection. Distributed invariants were derived across the interdepen-

dent systems to detect process anomalies resulting due to cascading effects of a cyber attack.

The experiments in this work showcase the impact of cascading effects on interconnected systems. It was observed that to perform an attack on critical interconnected infrastructure, the attacker needs to know how the target infrastructure is linked to other infrastructure. A weak, or a critical node, may be found in these systems to serve as an attack target and cause more damage to the system. For example, in attack A_4, it is observed that attacking the pump in SWaT can cause significant inconvenience to the consumers by disrupting water services. Invariants derived from the design of individual systems are unable to detect such attacks; distributed invariants become a necessity. For example, in attack A_1, Invariant 7, a distributed invariant, is violated but not Invariant 5 which is derived from only WADI.

Further work is needed to study the impact of cascading effects of electric power failures on water systems when power and water systems are interconnected and study the investigation of safety and security integrated models (Sabaliauskaite and Adepu 2017) across interconnected systems. The case study presented in this paper is a step towards realizing a safe and secure interconnected system. A procedure to derive a complete set of attacks and invariants can also be pursed as a future research work.

Author's contributions

VR performed the experiments, analysed the results, and wrote the first draft of this paper. SA also helped in performing experiments and helped in shaping up the draft. VKM and AM provided technical feedback throughout the work. All authors reviewed the final manuscript. All authors read and approved the final manuscript.

Funding

This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2015NCR-NCR003-001) and administered by the National Cybersecurity R&D Directorate.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Indian Institute of Petroleum and Energy, 2nd Floor, AU Engg College Main Block, Andhra University, 530003 Visakhapatnam, India. [2]Singapore University of Technology and Design, 8 Somapah Road, 487372 Singapore, Singapore.

Received: 20 August 2020 Accepted: 4 January 2021
Published online: 01 March 2021

References

Adepu S, Mathur A (2016a) Distributed detection of single-stage multipoint cyber attacks in a water treatment plant. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. Association for Computing Machinery, New York. pp 449–460

Adepu S, Mathur A (2016b) Generalized attacker and attack models for Cyber-Physical Systems. In: Proc. of the 40th IEEE COMPSAC. IEEE, Atlanta

Adepu S, Mishra G, Mathur A (2017) Access control in water distribution networks: A case study. In: 2017 IEEE International Conference on Software Quality, Reliability and Security (QRS). IEEE, Prague. pp 184–191

Adepu S, Palleti VR, Mishra G, Mathur A (2020) Investigation of cyber attacks on a water distribution system. In: Applied Cryptography and Network Security Workshops. Springer International Publishing, Cham. pp 274–291. arXiv preprint arXiv:1906.02279

Adepu S, Prakash J, Mathur A (2017) Waterjam: An experimental case study of jamming attacks on a water treatment system. In: 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE. pp 341–347

Ahmed CM, Murguia C, Ruths J (2017) Model-based attack detection scheme for smart water distribution networks. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17). ACM, New York. pp 101–113

Ahmed CM, Palleti VR, Mathur AP (2017) Wadi: A water distribution testbed for research in the design of secure cyber physical systems. In: Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWATER '17). Association for Computing Machinery, New York. pp 25–28

Ahmed CM, Zhou J, Mathur AP (2018) Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in cps. In: Proceedings of the 34th Annual Computer Security Applications Conference. pp 566–581

Amin S, Cardenas AA, Sastry SS (2009) Safe and secure networked control systems under denial-of-service attacks. In: Hybrid Systems: Computation and Control. Proc. 12th Intl. Conf. (HSCC), LNCS, Vol. 5469, Springer-Verlag. Springer Berlin Heidelberg, Berlin. pp 31–45

Amin S, Schwartz GA, Sastry SS (2013) Security of interdependent and identical networked control systems. Automatica 49(1):186–192

Berman D, Butts J (2012) Towards characterization of cyber attacks on industrial control systems: emulating field devices using gumstix technology. In: 2012 5th International Symposium on Resilient Control Systems. IEEE press, Salt Lake City. pp 63–68

Biondi P (2010) Scapy documentation (!). Release. https://scapy.readthedocs.io/en/latest/backmatter.html. Accessed 23 Feb 2020

Caire R, Sanchez J, Hadjsaid N (2013) Vulnerability analysis of coupled heterogeneous critical infrastructures: A co-simulation approach with a testbed validation. In: IEEE PES ISGT Europe 2013. IEEE, PES ISGT Europe. pp 1–5

Cardenas A, Amin S, Lin Z, Huang Y, Huang C, Sastry S (2011) Attacks against process control systems: Risk assessment, detection, and response. In: 6th ACM Symposium on Information, Computer and Communications Security. Association for Computing Machinery, New York. pp 355–366

Chen Y, Poskitt C, Sun J (2018) Learning from mutants: Using code mutation to learn and monitor invariants of a cyber-physical system:648–660. https://doi.org/10.1109/SP.2018.00016

Chen Y, Poskitt CM, Sun J, Adepu S, Zhang F (2019) Learning-guided network fuzzing for testing cyber-physical system defences. In: 2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE press, San Diego. pp 962–973

Chen TM, Sanchez-Aarnoutse JC, Buford J (2011) Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans Smart Grid 2(4):741–749

Feng C, Palleti VR, Mathur A, Chana D (2019) A systematic framework to generate invariants for anomaly detection in industrial control systems. In: NDSS. The Internet Society, San Diego

Gadewar SB, Doherty MF, Malone MF (2001) A systematic method for reaction invariants and mole balances for complex chemistries. Comput Chem Eng 25(9):1199–1217

Gadewar SB, Doherty MF, Malone MF (2002) Reaction invariants and mole balances for plant complexes. Ind Eng Chem Res 41(16):3771–3783

Gamage TT, McMillin BM, Roth TP (2010) Enforcing information flow security properties in cyber-physical systems: A generalized framework based on compensation. In: Computer Software and Applications Conference Workshops (COMPSACW), IEEE 34th Annual. IEEE, Seoul. pp 158–163

Ghaeini HR, Tippenhauer NO, Zhou J (2019) Zero residual attacks on industrial control systems and stateful countermeasures. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. pp 1–10

Hau Z, Castellanos JH, Zhou J (2020) Evaluating Cascading Impact of Attacks on Resilience of Industrial Control Systems: A Design-Centric Modeling Approach. Association for Computing Machinery, New York

Heracleous C, Keliris C, Panayiotou CG, Polycarpou MM (2018) Centralized fault detection of complex uncertain hybrid systems. IFAC-PapersOnLine 51(7):76–81

Heracleous C, Kolios P, Panayiotou CG, Ellinas G, Polycarpou MM (2017) Hybrid systems modeling for critical infrastructures interdependency analysis. Reliab Eng Syst Saf 165:89–101. https://doi.org/10.1016/j.ress.2017.03.028

Howser G, McMillin B (2014) A modal model of stuxnet attacks on cyber-physical systems: A matter of trust. In: 2014 Eighth International Conference on Software Security and Reliability (SERE). IEEE press, San Francisco. pp 225–234
Kang E, Adepu S, Jackson D, Mathur AP (2016) Model-based security analysis of a water treatment system. In: In Proceedings of 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems (in Press; SEsCPS'16). IEEE, Austin
Kumar V, Kaistha N (2019) Invariants for optimal operation of a reactor-separator-recycle process. J Process Control 82:1–12
Kwon C, Liu W, Hwang I (2013) Security analysis for cyber-physical systems against stealthy deception attacks. In: American Control Conference (ACC), 2013. IEEE press, Washington, DC. pp 3344–3349
LabVIEW (2019). http://www.ni.com/labview/. Accessed 15 Mar 2020
Lee EE, Mitchell JE, Wallace WA (2004) Assessing vulnerability of proposed designs for interdependent infrastructure systems. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004. IEEE Computer Society, Los Alamitos. p 8
Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur (TISSEC) 14(1):13
Liu J, Zeng F (2012) Research on Conceptual Design Method for Marine Power Plant Based on QFD. In: Computational Intelligence and Design (ISCID), 2012 Fifth International Symposium On, vol. 1. Hangzhou. pp 246–249
Mathur AP, Tippenhauer NO (2016) SWaT: A water treatment testbed for research and training on ICS security. In: International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater). IEEE, USA. pp 31–36
Mulder J, Schwartz M, Berg M, Van Houten JR, Mario J, Urrea MAK, Clements AA, Jacob J (2013) Weaselboard: Zero-day exploit detection for Programmable Logic Controllers. Technical report, SAND2013-8274, Sandia National Laboratories
Ouyang M, Wang Z (2015) Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. Reliab Eng Syst Saf 141:74–82
Pasqualetti F, Dörfler F, Bullo F (2011) Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In: 2011 50th IEEE Conference on Decision and Control and European Control Conference. IEEE press, Orlando. pp 2195–2201
Paul T, Kimball JW, Zawodniok M, Roth TP, McMillin B (2011) Invariants as a unified knowledge model for cyber-physical systems. In: IEEE International Conference on Service-Oriented Computing and Applications (SOCA). IEEE, Irvine. pp 1–8
Rinaldi SM, Peerenboom J, Kelly TK (2002) Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Syst IEEE 21:11–25
Rosich A, Voos H, Darouach M (2014) Cyber-attack detection based on controlled invariant sets. In: European Control Conference (ECC). IEEE, Strasbourg. pp 2176–2181
Rozel B, Viziteu M, Caire R, Hadjsaid N, Rognon J-P (2008) Towards a common model for studying critical infrastructure interdependencies. In: 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century. IEEE, Pittsburgh. pp 1–6
Rueda DF, Calle E (2017) Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks. Int J Crit Infrastruct Prot 16:3–12. https://doi.org/10.1016/j.ijcip.2016.11.004
Sabaliauskaite G, Adepu S (2017) Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE). IEEE press, Singapore. pp 41–48
Stamp M (2011) Information Security: Principles and Practice. Wiley Publishing, San Jose
Teixeira A, Pérez D, Sandberg H, Johansson KH (2012) Attack models and scenarios for networked control systems. In: Proceedings of the 1st International Conference on High Confidence Networked Systems. Association for Computing Machinery, New York. pp 55–64
U.S.-Canada, Power System Outage, Task Force (2004) Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. https://www.energy.gov/oe/downloads/us-canada-power-system-outage-taskforce-final-report-implementation-task-force. Accessed 14 Mar 2020
Urbina D, Giraldo J, Tippenhauer N, Cardenas A (2016a) Attacking fieldbus communications in ICS: applications to the SWaT testbed. In: Proceedings of the Singapore Cyber-Security Conference (SG-CRC). vol. 14. IOS press, Singapore. pp 75–89
Urbina DI, et al. (2016b) Limiting the impact of stealthy attacks on industrial control systems. In: Proceedings of the 2016 ACM CCS. Association for Computing Machinery, New York. pp 1092–1105
Vaidya B, Makrakis D, Mouftah HT (2011) Security mechanism for multi-domain vehicle-to-grid infrastructure. In: 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011. IEEE, Houston. pp 1–5
Wasicek A (2013) Attack modeling in Ptolemy: Towards a secure design for Cyber-Physical systems. http://chess.eecs.berkeley.edu/pubs/1039/wasicek_AttackModeling_PtolemyMiniConf2013.pdf
Zhang Y, Yagan O (2018) Modeling and Analysis of Cascading Failures in Interdependent Cyber-Physical Systems. arXiv e-prints:4731–4738. Miami Beach

Publisher's Note