

METHOD AND SYSTEM FOR DETECTING ANOMALY IN A PHYSICAL PROCESS ASSOCIATED WITH A NETWORKED CONTROL SYSTEM

- 5 [0001] This application claims the benefit of priority of Singapore Patent Application No. 10202005543S, filed on 11 June 2020, the content of which being hereby incorporated by reference in its entirety for all purposes.

TECHNICAL FIELD

- 10 [0002] The present invention generally relates to a method and a system for detecting anomaly in a physical process associated with a networked control system, and more particularly, for detecting an attack on the networked control system.

BACKGROUND

- 15 [0003] An Industrial Control System (ICS) is a networked control system comprising sensors, actuators, controllers and communication networks configured to control one or more physical processes in an industry, such as water treatment, water distribution, smart grid, autonomous transportation, and so on. For example, connectivity in an ICS provides improved monitoring and operation of a physical process. Such advancements are helpful but also bring
20 about challenges of secure operation of the connected devices for the ICS to operate securely.

- [0004] For example, an ICS can be subject to cyber and/or physical attacks, which can be launched either remotely or locally. Attackers may tamper sensor reading or inject spoofing sensor data, and manipulate the actuators to cause anomaly of operations, which may eventually lead to physical damages to the ICS. However, traditional intrusion detection methods based
25 on network traffic cannot detect many low layer attacks originated in the physical domain, as there may be no abnormal network traffic.

- [0005] For example, sensor data may be transmitted to a Programmable Logic Controller (PLC) to perform an appropriate action based on the sensor measurement. In this regard, if an adversary can spoof sensor data in the digital or physical domain, the adversary can cause the
30 ICS to go to an unsafe state. The focus here is not on the confidentiality of the sensor data as in legacy computer security but the integrity and trustworthiness of the sensor data.

[0006] A need therefore exists to provide a method and a system for detecting anomaly in a physical process associated with a networked control system, that seek to overcome, or at least ameliorate, one or more problems relating to conventional method and a system for detecting anomaly in a physical process, and more particularly, enabling or improving anomaly detection (in particular, attack detection) in a physical process associated with a networked control system in an effective manner. It is against this background that the present invention has been developed.

SUMMARY

10 [0007] According to a first aspect of the present invention, there is provided a method of detecting anomaly in a physical process associated with a networked control system using at least one processor, the method comprising:

obtaining, for each process run of a plurality of process runs for a state process at a process state of the physical process, measured sensor data associated with the process run in relation to a physical state associated with the state process at the process state;

15 producing, for said each process run of the plurality of process runs, process offset data associated with the process run based on the measured sensor data associated with the process run and modelled sensor data in relation to the physical state associated with the state process, to obtain a plurality of process offset data associated with the plurality of process runs, respectively, in relation to the physical state associated with the state process;

determining process skew fingerprint information associated with the plurality of process runs based on the plurality of process offset data, the process skew fingerprint information comprising characteristic information associated with the plurality of process offset data; and

25 detecting anomaly in the physical process based on the process skew fingerprint information associated with the plurality of process runs for the state process at the process state of the physical process.

[0008] According to a second aspect of the present invention, there is provided a system for detecting anomaly in a physical process associated with a networked control system, the system comprising:

a memory; and

at least one processor communicatively coupled to the memory and configured to:

obtain, for each process run of a plurality of process runs for a state process at a process state of the physical process, measured sensor data associated with the process run in relation to a physical state associated with the state process at the process state;

5 produce, for said each process run of the plurality of process runs, process offset data associated with the process run based on the measured sensor data associated with the process run and modelled sensor data in relation to the physical state associated with the state process, to obtain a plurality of process offset data associated with the plurality of process runs, respectively, in relation to the physical state associated with the state process;

10 determine process skew fingerprint information associated with the plurality of process runs based on the plurality of process offset data, the process skew fingerprint information comprising characteristic information associated with the plurality of process offset data; and

15 detect anomaly in the physical process based on the process skew fingerprint information associated with the plurality of process runs for the state process at the process state of the physical process.

[0009] According to a third aspect of the present invention, there is provided a computer program product, embodied in one or more non-transitory computer-readable storage mediums, comprising instructions executable by at least one processor to perform the method of detecting anomaly in a physical process according to the above-mentioned first aspect of the present invention.
20

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Embodiments of the present invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:
25

FIG. 1 depicts a schematic flow diagram of a method of detecting anomaly in a physical process associated with a networked control system, according to various embodiments of the present invention

30 FIG. 2 depicts a schematic block diagram of a system for detecting anomaly in a physical process associated with a networked control system, according to various embodiments of the present invention, such as corresponding to the method of detecting anomaly in a physical process as described with reference to FIG. 1;

FIG. 3 depicts a schematic block diagram of an exemplary computer system which may be used to realize or implement the system as described with reference to FIG. 2;

FIG. 4 depicts a schematic drawing of a Secure Water Treatment Testbed (SWaT) Network Architecture, based on which the method of detecting anomaly in a physical process may be applied as an illustrative example, according to various example embodiments of the present invention for illustration purpose;

FIG. 5 depicts a schematic flow diagram illustrating an overview of a process skew based detection method according to various example embodiments of the present invention, such as corresponding to the method of detecting anomaly in a physical process as described with reference to FIG. 1;

FIG. 6 depicts a schematic drawing showing an abstraction of an industrial control system (ICS) in relation to a thread model;

FIGs. 7A and 7B depict a table (Table 1) providing a list of attacks on the SWaT testbed that may be carried out in experiments conducted, according to various example embodiments of the present invention;

FIG. 8 depicts a plot of level sensor (LIT-101) measurements in the SWaT testbed in stage 1 for a duration of a normal process (i.e., under normal operation);

FIG. 9 shows a table (Table 2) providing a list of example design parameters for each type of state process or control action, according to various example embodiments of the present invention;

FIGs. 10A to 10D depict four plots showing four possible state processes of a physical process, respectively, along with measured sensor data obtained with respect to the water level in a water tank (tank 1) as described with reference to Table 2, according to various example embodiments of the present invention;

FIG. 11 depicts a plot illustrating the concept of process offsets (or process skews) associated with a physical process, according to various example embodiments of the present invention;

FIG. 12 depicts a schematic diagram of an example physical system for stage 1 of the SWaT testbed, according to various example embodiments of the present invention;

FIGs. 13A to 13C depict process offset data obtained based on measured sensor data for different state processes at stage 1 of the SWaT testbed, according to various example embodiments of the present invention;

FIG. 14 depicts a plot of a plurality of process offset data obtained based on measured sensor data for the water filling process in stage 1 of the SWaT testbed, with a linear regression model fitted thereon, according to various example embodiments of the present invention;

FIGs. 15A to 15C depict process skew fingerprint distributions for eight state processes at three stages of the SWaT testbed, according to various example embodiments of the present invention;

FIG. 16 illustrates mutual information across the eight process skew fingerprints discussed with reference to FIGs. 15A to 15C, according to various example embodiments of the present invention;

FIG. 17 depicts a table (Table 3) showing the model accuracies for three stages of the SWaT and corresponding state processes used in experiments conducted (from the SWaT testbed), according to various example embodiments of the present invention;

FIG. 18 depicts a table (Table 4) showing example design and performance of a cumulative sum (CUSUM) detector on the normal operation data, according to various example embodiments of the present invention;

FIG. 19 depicts a plot of process offsets obtained based on measured sensor data on process runs in relation to tank 4 in stage 4 of the SWaT testbed, including a mixture of normal process runs and a few attacks, according to various example embodiments of the present invention;

FIGs. 20A and 20B depict plots in relation to an attack detection example for an outflow process in relation to level sensor LIT-401, according to various example embodiments of the present invention;

FIG. 21 depicts a table (Table 5) showing evaluation results of the process skew based detection method, according to various example embodiments of the present invention, on attack data from the SWaT testbed; and

FIGs. 22A and 22B show an example execution of a stealthy attack on stage 1 of the SWaT testbed, according to various example embodiments of the present invention.

DETAILED DESCRIPTION

[0011] Various embodiments of the present invention provide a method and a system for detecting anomaly in a physical process associated with a networked control system, and more particularly, for detecting an attack on the networked control system. For example, the networked control system may be implemented in any industries (industrial applications) as an

Industrial Control System (ICS) as desired or as appropriate that requires an industrial process control, such but not limited to, water treatment, chemical processing, power generation, oil and gas processing, and so on. The networked control system may comprise a sensor network comprising a plurality of sensors. A sensor network is known in the art and may comprise a plurality of sensors that are spatially positioned or installed in the networked control system, each being arranged or positioned for monitoring and collecting sensor data (e.g., measurements or readings, which may be referred to herein as measured sensor data) relating to one or more process states of one or more physical processes associated with the networked control system, such as relating to a physical condition or a physical property of a surrounding environment (e.g., in relation to a medium or an object), such as but not limited to, temperature, sound, pressure, fluid flow rate, fluid level and so on. The plurality of sensors may be communicatively coupled to a processor (e.g., a central processor or a sensor data processor, such as a Programmable Logic Controller (PLC)) based on any communications technologies known in the art, such as wired communications technologies or wireless communications technologies, and need not be described herein. It will be appreciated by a person skilled in the art that each sensor may be any type of sensor known in the art configured for capturing a physical condition or physical property of a surrounding environment and outputting corresponding measured sensor data in relation to the surrounding environment. It will be appreciated by a person skilled in the art that the plurality of sensors may be of the same type or may include a variety of sensors, depending on the aspects of (or in relation to) the one or more physical processes associated with the networked control system that are desired to be monitored. In various embodiments, an attack on the networked control system may refer to any type of security or malicious attack on the networked control system known in the art and need not be described herein, such as an attack on one or more sensors in the sensor network. Various possible types of attack on a networked control system are known in the art, and for illustration purpose, example types of attack will be described later below according to various example embodiments of the present invention.

[0012] As described in the background, an ICS can be subject to cyber and/or physical attacks, which can be launched either remotely or locally. Attackers may tamper sensor reading or inject spoofing sensor data and may manipulate the actuators, which may result in anomaly of operations and eventually lead to physical damages to the ICS. However, traditional intrusion detection methods based on network traffic cannot detect many low layer attacks originated in the physical domain, as there may be no abnormal network traffic. For example, sensor data

may be transmitted to a PLC to perform an appropriate action based on the sensor measurement. In this regard, if an adversary can spoof sensor data in the digital or physical domain, the adversary can cause the ICS to go to an unsafe state. Therefore, the integrity and trustworthiness of the sensor data are important for the ICS to operate securely.

5 **[0013]** Accordingly, various embodiments of the present invention provide a method and a system for detecting anomaly in a physical process associated with a networked control system, that seek to overcome, or at least ameliorate, one or more problems relating to conventional method and a system for detecting anomaly in a physical process, and more particularly, enabling or improving anomaly detection (in particular, attack detection) in a physical process
10 associated with a networked control system in an effective manner.

[0014] FIG. 1 depicts a schematic flow diagram of a method 100 of detecting anomaly in a physical process associated with a networked control system using at least one processor, according to various embodiments of the present invention. The method 100 comprises: obtaining (at 102), for each process run of a plurality of process runs for a state process at a
15 process state of the physical process, measured sensor data associated with the process run in relation to a physical state associated with the state process at the process state; producing (at 104), for the above-mentioned each process run of the plurality of process runs, process offset data associated with the process run based on the measured sensor data associated with the process run and modelled sensor data in relation to the physical state associated with the state
20 process, to obtain a plurality of process offset data associated with the plurality of process runs, respectively, in relation to the physical state associated with the state process; determining (at 106) process skew fingerprint information associated with the plurality of process runs based on the plurality of process offset data, the process skew fingerprint information comprising characteristic information associated with the plurality of process offset data; and detecting (at
25 108) anomaly in the physical process based on the process skew fingerprint information associated with the plurality of process runs for the state process at the process state of the physical process.

[0015] In various embodiments, in relation to 102, the measured sensor data associated with a process run may be obtained from one or more sensors of the sensor network of the networked
30 control system. For example, a physical process associated with a network control system may comprise one or more process states, and for each process state, there may be one or more state processes (i.e., one or more types of state processes) that may be performed (or may occur) at the process state. Furthermore, for each state process, a plurality of process runs (or process

instances) for the state process may be performed (or may occur). By way of an example only and without limitation, in relation to a water treatment plant, there may be a plurality of process stages, such as a raw water storage stage to hold the raw water for treatment, a chemical dosing stage to treat the water, an ultra-filtrating stage, and so on. For example, in relation to the raw water storage stage, there may be an associated physical process comprising a plurality of process states, such as a water emptying state, a water filling state and a water filling and emptying state. In this regard, the one or more types of processes performed at each process state may thus be one or more state processes (i.e., one or more types of state processes) at the process state. Furthermore, for a state process (e.g., water emptying process) at a process state (e.g., water emptying state), a plurality of process runs (e.g., hundreds of process runs (or process instances) of the water emptying process over time) may be performed (or may occur), and measured sensor data associated with each of the plurality of process runs in relation to a physical state (e.g., water level in a water tank) associated with the state process may thus be obtained, to produce a plurality of measured sensor data associated with the plurality of process runs in relation to the physical state associated with the state process. In various embodiments, the networked control system may be configured to perform or control a physical process, and each process stage of the networked control system may thus be configured to perform or control an associated physical sub-process.

[0016] In various embodiments, in relation to 104, the modelled sensor data in relation to the physical state associated with the state process may be sensor data in relation to the physical state that is expected or intended (e.g., configured or designed to be) based on design parameters associated with the state process. For example, in the case of the physical state associated with the state process being the water level in a water tank during the water emptying process, the modelled sensor data in relation to the water level during the water emptying process may be sensor data in relation to the water level that is expected over time during the water emptying process based on design parameters associated with water emptying process in relation to the water tank. As will be described later below, according to various embodiments, sensor data in relation to a physical state that is expected may be determined by estimating the sensor data in relation to the physical state based on a system model.

[0017] In various embodiments, in relation to 106, characteristic information associated with the plurality of process offset data associated with the plurality of process runs for the state process may be determined (e.g., extracted) so as to produce the process skew fingerprint information associated with the plurality of process runs. As will be described later below,

according to various embodiments, the characteristic information may be a slope parameter associated with a linear regression model applied to the plurality of process offset data.

[0018] In various embodiments, in relation to 108, using the process skew fingerprint information associated with the process runs for the state process, whether there is an anomaly in the physical process at that state process may then be detected.

[0019] It will be understood by a person skilled in the art that the method 100 of detecting anomaly in the physical process for additional one or more other state processes at the process state of the physical process, or at one or more other process states of the physical process may be performed in the same or similar manner as described herein in relation to the above-mentioned state process at the above-mentioned process state of the physical process. It will also be understood by a person skilled in the art that the method 100 of detecting anomaly in additional one or more physical processes associated with the networked control system may also be performed in the same or similar manner as described herein in relation to the above-mentioned state process at the above-mentioned process state of the physical process.

[0020] Accordingly, the method 100 of detecting anomaly in a physical process is based on a plurality of process offset data (e.g., which may be referred to herein as a plurality of process skew data) associated with a plurality of process runs for a state process at a process state of the physical process. Therefore, the method 100 of detecting anomaly in a physical process is advantageously based on inaccuracies (e.g., deviations due to an attack) in the physical process itself, and thus is based on physical process dynamics. Furthermore, a plurality of process skew data associated with a plurality of process runs for a state process of a physical process is produced and used to fingerprint the plurality of process runs for the state process, so as to produce process skew fingerprint information for detecting anomaly in the state process of the physical process. Such a technical approach in detecting anomaly in the physical process has been found to enable or improve anomaly detection (in particular, attack detection) in a physical process associated with a networked control system in an effective manner. These advantages or technical effects, and/or other advantages or technical effects, will become more apparent to a person skilled in the art as the method 100 of detecting anomaly, as well as corresponding system for detecting anomaly, is described in more detail according to various embodiments and example embodiments of the present invention.

[0021] In various embodiments, the method 100 further comprises determining the modelled sensor data in relation to the physical state associated with the state process, comprising estimating sensor data in relation to the physical state associated with the state

process based on a system model representing the state process and one or more design parameters associated with the state process.

[0022] In various embodiments, the above-mentioned producing (at 104), for the above-mentioned each process run of the plurality of process runs of the state process at the process state, process offset data associated with the process run comprises: determining, for each time step of a plurality of time steps, a process offset between the measured sensor data associated with the process run obtained at the time step and the modelled sensor data at the time step in relation to the physical state associated with the state process, to obtain a plurality of process offset information associated with the process run at the plurality of time steps, respectively. In this regard, the process offset data associated with the process run comprises the plurality of process offset information associated with the process run.

[0023] In various embodiments, the above-mentioned determining, for the above-mentioned each time step of the plurality of time steps, the process offset comprises determining, for the above-mentioned each time step of the plurality of time steps, a difference between the measured sensor data associated with the process run obtained at the time step and the modelled sensor data at the time step in relation to the physical state associated with the state process, to obtain the plurality of process offset information associated with the process run at the plurality of time steps, respectively.

[0024] In various embodiments, the above-mentioned determining (at 106) the process skew fingerprint information associated with the plurality of process runs comprises determining a slope parameter associated with the plurality of process offset data associated with the plurality of process runs in relation to the physical state associated with the state process. In this regard, the process skew fingerprint information comprises the slope parameter.

[0025] In various embodiments, the above-mentioned determining the slope parameter associated with the plurality of process offset data comprising applying a linear regression model to the plurality of process offset data to obtain a regression coefficient. In this regard, the slope parameter comprises the regression coefficient.

[0026] In various embodiments, the above-mentioned detecting (at 108) anomaly in the physical process comprises detecting anomaly in the physical process based on the process skew fingerprint information associated with the plurality of process runs for the state process at the process state of the physical process and a reference process skew fingerprint information associated with the state process at the process state of the physical process.

- [0027] In various embodiments, the method 100 further comprises determining the reference process skew fingerprint information associated with the state process at the process state of the physical process, comprising: obtaining, for each reference process run of a plurality of reference process runs for the state process at the process state of the physical process, measured sensor data associated with the reference process run in relation to the physical state associated with the state process at the process state; producing, for said each reference process run of the plurality of reference process runs, reference process offset data associated with the reference process run based on the measured sensor data associated with the reference process run and the modelled sensor data in relation to the physical state associated with the state process, to obtain a plurality of reference process offset data associated with the plurality of reference process runs, respectively, in relation to the physical state associated with the state process; and determining the reference process skew fingerprint information associated with the plurality of reference process runs based on the plurality of reference process offset data, the reference process skew fingerprint information comprising characteristic information associated with the plurality of reference process offset data. In various embodiments, the reference process skew fingerprint information, the plurality of reference process runs and the plurality of reference process offset data may refer to that obtained under normal operating conditions (e.g., without attack and breakdown), that is, reference with respect to normal operating conditions.
- [0028] In various embodiments, the above-mentioned reference process skew fingerprint information associated with the state process may be determined in the same or similar manner as the above-mentioned process skew fingerprint information associated with the state process determined at 106, except that the above-mentioned reference process skew fingerprint information is determined based on measured sensor data associated with the plurality of reference process runs for the state process.
- [0029] In various embodiments, the above-mentioned detecting anomaly in the physical process comprises detecting an attack on the networked control system based on the process skew fingerprint information associated with the plurality of process runs for the state process at the process state of the physical process.
- [0030] FIG. 2 depicts a schematic block diagram of a system 200 for detecting anomaly in a physical process associated with a networked control system, according to various embodiments of the present invention, such as corresponding to the method 100 of detecting anomaly in a physical process associated with a networked control system as described

hereinbefore with reference to FIG. 1 according to various embodiments of the present invention. The system 200 comprises: a memory 202; and at least one processor 204 communicatively coupled to the memory 202 and configured to: obtain, for each process run of a plurality of process runs for a state process at a process state of the physical process, measured sensor data associated with the process run in relation to a physical state associated with the state process at the process state; produce, for the above-mentioned each process run of the plurality of process runs, process offset data associated with the process run based on the measured sensor data associated with the process run and modelled sensor data in relation to the physical state associated with the state process, to obtain a plurality of process offset data associated with the plurality of process runs, respectively, in relation to the physical state associated with the state process; determine process skew fingerprint information associated with the plurality of process runs based on the plurality of process offset data, the process skew fingerprint information comprising characteristic information associated with the plurality of process offset data; and detect anomaly in the physical process based on the process skew fingerprint information associated with the plurality of process runs for the state process at the process state of the physical process.

[0031] It will be appreciated by a person skilled in the art that the at least one processor 204 may be configured to perform various functions or operations through set(s) of instructions (e.g., software modules) executable by the at least one processor 204 to perform various functions or operations. Accordingly, as shown in FIG. 2, the system 200 may comprise a measured sensor data module (or a measured sensor data circuit) 206 configured to obtain, for each process run of a plurality of process runs for a state process at a process state of the physical process, measured sensor data associated with the process run in relation to a physical state associated with the state process at the process state; a process offset data producing module (or a process offset data producing circuit) 208 configured to produce, for the above-mentioned each process run of the plurality of process runs, process offset data associated with the process run based on the measured sensor data associated with the process run and modelled sensor data in relation to the physical state associated with the state process, to obtain a plurality of process offset data associated with the plurality of process runs, respectively, in relation to the physical state associated with the state process; a process skew fingerprint information determining module (a process skew fingerprint information determining circuit) 210 configured to determine process skew fingerprint information associated with the plurality of process runs based on the plurality of process offset data, the process skew fingerprint information

comprising characteristic information associated with the plurality of process offset data; and an anomaly detection module (or an anomaly detection circuit) 212 configured to detect anomaly in the physical process based on the process skew fingerprint information associated with the plurality of process runs for the state process at the process state of the physical process.

5 [0032] It will be appreciated by a person skilled in the art that the above-mentioned modules are not necessarily separate modules, and one or more modules may be realized by or implemented as one functional module (e.g., a circuit or a software program) as desired or as appropriate without deviating from the scope of the present invention. For example, two or more of the measured sensor data module 206, the process offset data producing module 208,
10 the process skew fingerprint information determining module 210 and the anomaly detection module 212 may be realized (e.g., compiled together) as one executable software program (e.g., software application or simply referred to as an “app”), which for example may be stored in the memory 202 and executable by the at least one processor 204 to perform various functions/operations as described herein according to various embodiments of the present
15 invention.

[0033] In various embodiments, the system 200 corresponds to the method 100 of detecting anomaly as described hereinbefore with reference to FIG. 1, therefore, various functions or operations configured to be performed by the least one processor 204 may correspond to various steps or operations of the method 100 of detecting anomaly as described herein according to
20 various embodiments, and thus need not be repeated with respect to the system 200 for detecting anomaly for clarity and conciseness. In other words, various embodiments described herein in context of the methods are analogously valid for the corresponding systems, and vice versa.

[0034] For example, in various embodiments, the memory 202 may have stored therein the measured sensor data module 206, the process offset data producing module 208, the process
25 skew fingerprint information determining module 210 and/or the anomaly detection module 212, which respectively correspond to various steps (or operations or functions) of the method 100 of detecting anomaly as described herein according to various embodiments, which are executable by the at least one processor 204 to perform the corresponding functions/operations as described herein.

30 [0035] A computing system, a controller, a microcontroller or any other system providing a processing capability may be provided according to various embodiments in the present disclosure. Such a system may be taken to include one or more processors and one or more computer-readable storage mediums. For example, the system 200 described hereinbefore may

include a processor (or controller) 204 and a computer-readable storage medium (or memory) 202 which are for example used in various processing carried out therein as described herein. A memory or computer-readable storage medium used in various embodiments may be a volatile memory, for example a DRAM (Dynamic Random Access Memory) or a non-volatile memory, for example a PROM (Programmable Read Only Memory), an EPROM (Erasable PROM), EEPROM (Electrically Erasable PROM), or a flash memory, e.g., a floating gate memory, a charge trapping memory, an MRAM (Magnetoresistive Random Access Memory) or a PCRAM (Phase Change Random Access Memory).

5 [0036] In various embodiments, a “circuit” may be understood as any kind of a logic implementing entity, which may be special purpose circuitry or a processor executing software stored in a memory, firmware, or any combination thereof. Thus, in an embodiment, a “circuit” may be a hard-wired logic circuit or a programmable logic circuit such as a programmable processor, e.g., a microprocessor (e.g., a Complex Instruction Set Computer (CISC) processor or a Reduced Instruction Set Computer (RISC) processor). A “circuit” may also be a processor
10 executing software, e.g., any kind of computer program, e.g., a computer program using a virtual machine code, e.g., Java. Any other kind of implementation of the respective functions which will be described in more detail below may also be understood as a “circuit” in accordance with various alternative embodiments. Similarly, a “module” may be a portion of a system according to various embodiments in the present invention and may encompass a
15 “circuit” as above, or may be understood to be any kind of a logic-implementing entity therefrom.
20

[0037] Some portions of the present disclosure are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations
25 are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise
30 manipulated.

[0038] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, description or discussions utilizing terms such as “obtaining”, “producing”, “determining”, “detecting”, “estimating” or the like, refer to

the actions and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

5 **[0039]** The present specification also discloses a system (e.g., which may also be embodied as a device or an apparatus), such as the system 200, for performing various operations/functions of various methods described herein. Such a system may be specially constructed for the required purposes, or may comprise a general purpose computer or other device selectively activated or reconfigured by a computer program stored in the computer. The
10 algorithms presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose machines may be used with computer programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform various method steps may be appropriate.

[0040] In addition, the present specification also at least implicitly discloses a computer
15 program or software/functional module, in that it would be apparent to the person skilled in the art that individual steps of various methods described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure
20 contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the scope of the invention. It will be appreciated by a person skilled in the art that various modules described herein (e.g., the measured sensor data module 206, the process offset data producing module 208, the process skew fingerprint
25 information determining module 210 and/or the anomaly detection module 212) may be software module(s) realized by computer program(s) or set(s) of instructions executable by a computer processor to perform the required functions, or may be hardware module(s) being functional hardware unit(s) designed to perform the required functions. It will also be appreciated that a combination of hardware and software modules may be implemented.

30 **[0041]** Furthermore, one or more of the steps of a computer program/module or method described herein may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage

devices suitable for interfacing with a general purpose computer. The computer program when loaded and executed on such a general-purpose computer effectively results in an apparatus that implements the steps of the methods described herein.

5 **[0042]** In various embodiments, there is provided a computer program product, embodied in one or more computer-readable storage mediums (non-transitory computer-readable storage medium(s)), comprising instructions (e.g., the measured sensor data module 206, the process offset data producing module 208, the process skew fingerprint information determining module 210 and/or the anomaly detection module 212) executable by one or more computer processors to perform the method 100 of detecting anomaly in a physical process associated
10 with a networked control system, as described herein with reference to FIG. 1 according to various embodiments. Accordingly, various computer programs or modules described herein may be stored in a computer program product receivable by a system therein, such as the system 200 as shown in FIG. 2, for execution by at least one processor 204 of the system 200 to perform various functions.

15 **[0043]** Software or functional modules described herein may also be implemented as hardware modules. More particularly, in the hardware sense, a module is a functional hardware unit designed for use with other components or modules. For example, a module may be implemented using discrete electronic components, or it can form a portion of an entire electronic circuit such as an Application Specific Integrated Circuit (ASIC). Numerous other
20 possibilities exist. Those skilled in the art will appreciate that the software or functional module(s) described herein can also be implemented as a combination of hardware and software modules.

[0044] In various embodiments, the system 200 may be realized by any computer system (e.g., desktop or portable computer system) including at least one processor and a memory,
25 such as a computer system 300 as schematically shown in FIG. 3 as an example only and without limitation. Various methods/steps or functional modules (e.g., the measured sensor data module 206, the process offset data producing module 208, the process skew fingerprint information determining module 210 and/or the anomaly detection module 212) may be implemented as software, such as a computer program being executed within the computer
30 system 300, and instructing the computer system 300 (in particular, one or more processors therein) to conduct various functions or operations as described herein according to various embodiments. The computer system 300 may comprise a computer module 302, input modules, such as a keyboard and/or a touchscreen 304 and a mouse 306, and a plurality of output devices

such as a display 308, and a printer 310. The computer module 302 may be connected to a computer network 312 via a suitable transceiver device 314, to enable access to e.g., the Internet or other network systems such as Local Area Network (LAN) or Wide Area Network (WAN). The computer module 302 in the example may include a processor 318 for executing various instructions, a Random Access Memory (RAM) 320 and a Read Only Memory (ROM) 322. The computer module 302 may also include a number of Input/Output (I/O) interfaces, for example I/O interface 324 to the display 308, and I/O interface 326 to the keyboard 304. The components of the computer module 302 typically communicate via an interconnected bus 328 and in a manner known to the person skilled in the relevant art.

10 [0045] It will be appreciated by a person skilled in the art that the terminology used herein is for the purpose of describing various embodiments only and is not intended to be limiting of the present invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, 15 specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0046] Any reference to an element or a feature herein using a designation such as "first", "second" and so forth does not limit the quantity or order of such elements or features, unless 20 stated or the context requires otherwise. For example, such designations may be used herein as a convenient way of distinguishing between two or more elements or instances of an element. Thus, a reference to first and second elements does not necessarily mean that only two elements can be employed, or that the first element must precede the second element. In addition, a phrase referring to "at least one of" a list of items refers to any single item therein or any combination 25 of two or more items therein.

[0047] In order that the present invention may be readily understood and put into practical effect, various example embodiments of the present invention will be described hereinafter by way of examples only and not limitations. It will be appreciated by a person skilled in the art that the present invention may, however, be embodied in various different forms or 30 configurations and should not be construed as limited to the example embodiments set forth hereinafter. Rather, these example embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the present invention to those skilled in the art.

[0048] In particular, for better understanding of the present invention and without limitation or loss of generality, unless stated otherwise, various example embodiments of the present invention will now be described with respect to attack detection on a networked control system for a water treatment plant. However, it will be understood by a person skilled in the art that the present invention is not limited to being applied to or implemented in a networked control system for a water treatment plant, and may be applied to or implemented in any industry as desired or as appropriate that may require an industrial process control, such but not limited to, chemical processing, power generation, oil and gas processing, and so on.

[0049] In an ICS, its complex network of sensors, actuators and controllers have raised security concerns. In this regard, various example embodiments provide a method (or technique), which may be referred to herein as a process skew based detection method, that uses process offsets (which may also be referred to as process skews, e.g., small deviations) in the ICS process for anomaly detection (e.g., attack detection). In various example embodiments, the process skew based detection method (e.g., corresponding to the method 100 of detecting anomaly in a physical process associated with a networked control system, as described herein according to various embodiments) may be based on fingerprinting a physical process for anomaly detection (i.e., determining process skew fingerprint information (i.e., process skew based fingerprint information), which may be simply referred to herein as a process skew fingerprint). In this regard, various example embodiments determine the process skew fingerprint based on noise in sensor measurements due to the process fluctuations (or process offsets). Various example embodiments found that a process skew fingerprint determined such a manner is unique to a physical process due to the intrinsic operational constraints of the physical process, and is hard to be forged even for a powerful attacker knowing the process operation. As will be described later below, the process skew based detection method was validated using data from a real-world water treatment testbed. In this regard, experimental results obtained demonstrate that the process skew based detection method effectively detected anomaly in a physical process associated with a networked control system (e.g., detected process anomaly with a very low false-positive rate), as well as demonstrate that the process skew based detection method can effectively identify a process (e.g., a state process at a process state of the physical process) based on the process skew fingerprint.

[0050] An ICS is a networked control system comprising sensors, actuators, controllers and communication networks configured to control one or more physical processes in an industry. For example, connectivity in an ICS provides improved monitoring and operation of a physical

process. Such advancements are helpful but also bring about challenges of secure operation of the connected devices for the ICS to operate securely.

[0051] For example, as discussed in the background, an ICS can be subject to cyber and/or physical attacks, which can be launched either remotely or locally. Attackers may tamper sensor reading or inject spoofing sensor data, and manipulate the actuators to cause anomaly of operations, which may eventually lead to physical damages to the ICS. However, traditional intrusion detection methods based on network traffic cannot detect many low layer attacks originated in the physical domain, as there may be no abnormal network traffic.

[0052] For example, sensor data may be transmitted to a PLC to perform an appropriate action based on the sensor measurement. In this regard, if an adversary can spoof sensor data in the digital or physical domain, the adversary can cause the ICS to go to an unsafe state. Therefore, according to various example embodiments, the focus is not on the confidentiality of the sensor data as in legacy computer security but the integrity and trustworthiness of the sensor data.

[0053] Furthermore, an open problem with conventional attack detection methods is that it is not possible to localize the source of attacks. This is especially an issue associated with conventional machine learning-based methods that use raw data from a process and feed them to well-known machine learning models. In this regard, various example embodiments note that, in contrast to the process skew based detection method, these conventional attack detection methods are not aware of or do not take into account process dynamics, and thus, they are unable to determine or locate the physical state where the attack occurred.

[0054] Accordingly, in various example embodiments, there is provided a process skew based detection method (e.g., corresponding to the method 100 of detecting anomaly in a physical process associated with a networked control system, as described herein according to various embodiments) configured to identify a physical process (e.g., a state process of the physical process) and detect data integrity attacks in an ICS in an effective manner. In various example embodiments, the process skew based detection method uses deviations (e.g., small deviations) in a physical process (in particular, deviations in measured sensor data associated with the physical process) with respect to a modelled physical process (in particular, modelled sensor data of the physical process) modelled based on design parameters (e.g., which may be referred to as process offsets or process skews) for fingerprinting the physical process so as to obtain a process skew fingerprint associated with the physical process (in particular, a process fingerprint associated with the measured sensor data associated with the physical process). For

example, these deviations in the physical process may be noise that appears in sensor measurements due to the process fluctuations (or process offsets). Advantageously, uniqueness in the process skew fingerprint obtained can be achieved due to the specified operational constraints of the physical process.

5 [0055] Accordingly, various example embodiments create a process skew fingerprint by extracting process offset information (or process skew information) from the sensor measurements. In this regard, various example embodiments note that for a physical process, due to inaccuracies in the physical process, it would have a skew from what it is designed for. An example is that of a water pipe delivering water to fill a tank. Pipes and tanks of two different
10 sizes would take/store a different amount of water. Even if the pipes are of the same size, two different amounts of pumping force would result in a different amount of water flowing or being stored. In this example, the flow of water in a pipe and water storage in a tank are examples of state processes of a physical process. At the design stage, these state processes may be designed to meet certain operational requirements (i.e., based on design parameters). However, various
15 example embodiments note that when these state processes are running, they show small deviations or offsets from the designed parameters due to the physical inaccuracies in the state processes, for example, no two water pipes can have the same diameter at a micro-scale due to manufacturing imperfections. Therefore, the process skew based detection method according to various example embodiments advantageously makes use of inaccuracies in the physical
20 process itself. Moreover, the process skew based detection method does not depend on the specific state of the system (e.g., does not need to wait for the process to be static) and uses the dynamics of the physical process (or a state process thereof) to create a system model, and uses process skews (or process offsets) for fingerprinting the physical process (or a state process thereof) so as to obtain a process skew fingerprint associated with the physical process (or a
25 state process thereof). Accordingly, the process skew based detection method advantageously provides a distinctive way of passively fingerprinting processes, by using process skews to determine a process skew fingerprint to detect attacks.

[0056] Accordingly, in various example embodiments of the present invention, there are provided a method of utilizing process skews to fingerprint a physical process, a method of
30 analyzing the effects of stealthy attacks on a process skew based detection method, and a method of detecting sensor attacks under a multitude of adversarial scenarios.

[0057] By way of an example only for illustration purpose and without limitation, the Secure Water Treatment Testbed (SWaT) at the Singapore University of Technology and

Design will now be described as an example ICS, along with an example implementation of the process skew based detection method thereto for detecting an attack, according to various example embodiments of the present invention.

[0058] ICS is a broad domain of connected industrial systems. A particular example of a water treatment industrial process, and more particularly, the SWaT, is considered. The SWaT is a fully functional testbed and is open for researchers to use. A brief introduction of the SWaT is provided below, but is described in detail in A. P. Mathur and N. O. Tippenhauer, "SWaT: a water treatment testbed for research and training on ICS security," *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, 2016, pp. 31-36, doi: 10.1109/CySWater.2016.7469060. The SWaT testbed produces purified water and it is a scaled-down version of a real water treatment process. FIG. 4 depicts a schematic drawing of the SWaT Test-bed Network Architecture 400. In FIG. 4, it can be seen that the testbed is distributed and there are different stages, where each stage is labeled as P_n where n is the n^{th} stage. There are six stages in the SWaT testbed, namely, $P1$ through $P6$. Each stage is equipped with a set of sensors and actuators. Sensors include water quantity measures, such as level, flow, and pressure and water quality measures, such as pH, ORP and conductivity. Actuators are different motorized valves and electric pumps. Stage 1 is a raw water stage configured to hold the raw water for the treatment and stage 2 is a chemical dosing stage configured to treat the water depending on the measurements from the water quality sensors. Stage 3 is an ultra-filtration stage. Stage 4 includes a de-chlorinator and stage 5 is equipped with reverse osmosis filters. Stage 6 is configured to hold the treated water for distribution. In the SWaT, data from the sensors and actuators are communicated to the PLCs using a level 0 network and PLC communicates to each other over a level 1 network as shown in FIG. 4.

[0059] According to various example embodiments, process skews (or process offsets) are extracted from measured sensor data. FIG. 5 depicts a schematic flow diagram illustrating an overview of a process skew based detection method 500 according to various example embodiments of the present invention (e.g., corresponding to the method 100 of detecting anomaly in a physical process associated with a networked control system, as described herein according to various embodiments). The method 500 comprises extracting (at 504) measurements (i.e., measured sensor data) for a specific state of the physical process (i.e., a process state of the physical process). For example, measured sensor data associated with each process state of the physical process may be obtained. In this regard, based on the actuator data, it is possible to determine the process state of the physical process. For example, if the inlet

pump is switched on, then the water is being filled in a tank, and thus, by knowing the state of the inlet pump, it is possible to know the process state of the physical process (e.g., in this case, the process state is that of the tank being filled with water, and the state process is a process at that process state, such as, the process of the water filling the tank). However, such state information from the sensors and actuators may be spoofed by an attacker.

5 [0060] Next, at 508, based on the state process at the process state of the physical process, a system model, along with the design parameters associated with the state process at the process state of the physical process, is used to model (e.g., estimate based on modelling) the physical state associated with the state process to obtain estimated sensor data (which may be referred to as modelled sensor data since the estimated sensor data is obtained based on a system model) in relation to the physical state associated with the state process at the process state (e.g., in the above-mentioned case, the physical state may be the water level in a tank).

10 [0061] At 512, the difference between the estimate (modelled sensor data) and real sensor measurement (measured sensor data) establishes an offset value (or a process offset), which corresponds to an amount by which the physical process (or state process) is offset from what it should be, as designed. This process offset data may be obtained for each process run of a plurality of process runs for a state process at the process state of the physical process, thereby obtaining a plurality of process offset data associated with the plurality of process runs, respectively, in relation to the physical state associated with the state process. Furthermore, for each process run, the difference between the modelled sensor data and the measured sensor data associated with the process run may be obtained or determined at each time step of a plurality of time steps, thereby obtaining a plurality of process offsets (or a plurality of process offset information) associated with the process run at the plurality of time steps, respectively. In this regard, the process offset data associated with the process run comprises the plurality of process offset information associated with the process run.

20 [0062] The plurality process offset data associated with the plurality of process runs for a state process, when accumulated over time, reveal the process skews associated with the plurality of process runs. Various example embodiments note that the plurality of process offset data associated with the plurality of process runs for a state process obtained may have fluctuations, for example, due to sensor noise. In this regard, various example embodiments apply (at 516) a linear regression model to the plurality of process offset data to obtain the best fit for the state process, so as to determine process skew fingerprint information (which may simply be referred to herein as a process skew fingerprint) associated with the plurality of

25 30

process runs. In various example embodiments, the process skew fingerprint may be obtained by calculating the rate of change of linear regression on the plurality of process offset data with respect to time. According to various example embodiments, a theoretical proof based on the calculated entropy of the process skew fingerprint is used to establish the uniqueness of the process skew fingerprint obtained. At 520, an anomaly detector (e.g., a CUSUM detector) may be used to detect attacks on the networked control system (e.g., the SWaT) based on the process skew fingerprint. The process skew based detection method 500 will be described in further details later below according to various example embodiments of the present invention.

[0063] In an ICS, sensors play an important role by sending physical measurements (measured sensor data) to a controller to execute an appropriate control action. However, an adversary can spoof sensor measurements either through cyber domain or physical domain intrusions. Accordingly, it is important to detect or authenticate whether the data is originating from the real physical process or is being modified in some manner. For example, various example embodiments note that due to computational limitations and legacy compliant equipment, it is not feasible to rely on cryptographic methods. Accordingly, various example embodiments provide a process skew based detection method 500 to achieve a process skew based authentication of a physical process. In this regard, various example embodiments seek to identify a physical process (or a state process of the physical process) based on its physical dynamics. In various example embodiments, specific cyber attacks are also considered on sensor measurements in a water treatment plant. FIG. 6 depicts a schematic drawing showing an abstraction of an ICS 600 in relation to a thread model, whereby $\bar{y}_k$ may or may not be attacked sensor measurement. In FIG. 6, it can be seen that an attacker can modify a rightful sensor measurement by an attack value δ_k . For illustration purpose, example types of attacks launched on the SWaT in experiments conducted will be described later below. In general, the attacker model encompasses the attacker's intentions and capabilities. For example, the attacker may choose its goals from a set of intentions, including performance degradation, disturbing a physical property of the system, or damaging a component. In the experiments conducted according to various example embodiments, a range of attacks are considered from already published attack scenarios in the literature.

[0064] An example attacker model will now be described. In the example attacker model, it is assumed that the attacker has access to the sensor's measurements. For example, a powerful attacker can arbitrarily change sensor measurements to the desired sensor value. A malicious insider may be an attacker with physical access to the plant and thus to its devices, such as level

sensors. However, an attacker who can physically replace or tamper sensors may not necessarily be an insider, because critical infrastructures, e.g., for water and power, are generally distributed across large areas. An outsider, for example, an end user, may also carry out a physical attack on sensors, such as smart energy monitors.

5 **[0065]** For example, in data injection attacks, an attacker injects or modifies the real sensor measurement. In general, for a complex ICS, there may be many possible attack scenarios. For illustration purpose, various example embodiments consider a generic attack to show the performance of the process skew based detection method 500 according to various example embodiments of the present invention. Accordingly, it will be appreciated by a person skilled
10 in the art that the present invention is not limited to any particular or specific type of attack. However, a stealthy attack may be a worst case scenario for a model based detection technique where an adversary tries to deceive the detection mechanism by creating attack vectors δ_k based on working principle of the attack detection technique. In various example embodiments, the following types of data injection attack scenarios are considered.

15 **[0066]** A type of data injection attack scenario is a generic sensor spoofing attack. In this regard, the process skew based detection method 500 was evaluated for a range of network attack scenarios from benchmark attacks on the SWaT testbed. These benchmark attacks cover a wide range of 36 attacks on both sensors and actuators. Since the process skew based detection method 500 extracts process skew information for various physical properties, attacks on
20 chemical sensors are thus excluded, resulting in a total of 25 attacks remaining as summarized in Table 1 shown in FIGs. 7A and 7B. In particular, Table 1 provides a list of attacks on the SWaT testbed carried out in experiments conducted according to various example embodiments of the present invention. In general, an attack vector may be defined as:

$$\bar{y}_k = y_k + \delta_k,$$

25 Equation (1)

where y_k are the real sensor measurement (measured sensor data), $\bar{y}_k$ is sensor measurement with a possible attack and δ_k is the data injected by an attacker at time step k . Details about each δ_k (attack vector) is described in Table 1 shown in FIGs. 7A and 7B, where it can be seen that it ranges from an abrupt injection of data to a more slow/stealthy change in sensor
30 measurements.

[0067] Another type of data injection attack scenario is stealthy attacks for model based techniques. These attacks are designed to be stealthy by changing sensor measurements such that the system model based detection mechanism would fail. Since model based detectors use

a system model, a Kalman filter and a statistical detector, an attacker who wants to remain stealthy may try to choose injected readings so as not to exceed the detector threshold. To do this, an attacker may learn the system model and the detector parameters. In this regard, various example embodiments assume that an attacker has the ability to do so, but does not possess the process skew knowledge.

[0068] In relation to attack execution, all the attacks which are obtained from the SWaT dataset disclosed in Goh J., et al., “A Dataset to Support Research in the Design of Secure Water Treatment Systems”, In Critical Information Infrastructures Security, Grigore Havarneanu, Roberto Setola, Hypatia Nassopoulos, and Stephen Wolthusen (Eds.), Springer International Publishing, Cham, pages 88-99, 2017, are executed by compromising the Supervisory Control and Data Acquisition (SCADA) system. An attack toolbox was used to inject an arbitrary value for real sensor measurement.

[0069] The process skew based detection method 500 will now be described in further details according to various example embodiments of the present invention.

[0070] A method of extracting state processes (or process states) of a physical process will now be described according to various example embodiments of the present invention. An example from the SWaT testbed is considered. FIG. 8 depicts a plot of level sensor (LIT-101) measurements in the SWaT testbed in stage 1 labeled as LIT-101 for a duration of a normal process (i.e., under normal operation). In particular, FIG. 8 shows multiple runs for a state process at a process state, e.g., water filling, water flowing out, both or none of the previous process. Each of these possible state processes in the water tank are labeled as S1 to S4, respectively, and their descriptions are provided in Table 2 shown in FIG. 9. The design parameters in Table 2 indicate the design for the inflow and outflow processes and which state process is present in a particular process state. The tank 1 in stage 1 of the SWaT testbed has one inlet valve labeled as MV-101 and one outlet pump labeled as P-101. There is also a secondary backup pump at the outlet labeled as P-102. Accordingly, there can be four possible state processes for the water level (physical state) in tank 1 based on input and output flow processes, namely, output flow process is present but no input flow process (S1), neither input nor output flow processes (S2), input flow process is present but no output flow process (S3), both input and output flow processes are present (S4).

[0071] In experiments conducted, the water treatment plant was operated for seven days continuously and measured sensor data for normal operations (e.g., without attack and breakdown) of the water treatment plant were collected. FIGs. 10A to 10D depict four plots

showing four possible state processes of a physical process, respectively, along with measured sensor data obtained with respect to the water level in a water tank (tank 1) as described with reference to Table 2. The level sensor in the SWaT testbed in stage 1 is labeled as LIT-101 under normal operations. Accordingly, the measured sensor data shown in FIGs. 10A to 10D present the particular state processes extracted from the seven days of normal operations. As shown, for each state process, there may be a plurality of occurrences (or process runs), for example, hundreds of occurrences. For example, for the water emptying process (S1) shown in FIG. 10A, there may be hundreds of occurrences (hundreds of process runs) of the water empty process during the observation period. From FIGs. 10A to 10D, the effects of noise (e.g., deviations or fluctuations) on the measured sensor data obtained in the plurality of process runs noted according to various example embodiments of the present invention can be seen.

[0072] Each physical process (or state process of the physical process) is expected to behave according to design parameters, such as shown in Table 2 in FIG. 9. However, as can be observed in FIGs. 10A to 10D, there are deviations due to the process noise. For example, in FIG. 10A, a first state process S1 shows different process runs of the water emptying process from the tank 1. In this regard, the variations in each process run due to the sensor noise can be observed in FIG. 10A. This can also be observed from the static (S2) and water filling (S3, S4) state processes. In this regard, according to various example embodiments of the present invention, based on these deviations (e.g., due to noise) in the state processes, variations due to process offsets in the state processes from those expected based on corresponding design parameters are determined. In various example embodiments, to quantify the amount of process skews associated with these state processes, the process dynamics for these state processes based on the design parameters (e.g., under the designed set points) are learned or determined.

[0073] A design based system model according to various example embodiments will now be described

[0074] FIG. 11 depicts a plot illustrating the concept of process skews associated with a physical process, according to various example embodiments of the present invention. In FIG. 11, the sensor measurements (measured sensor data) with respect to the water level for the water filling process and estimated sensor value (modelled sensor data) based on design parameters are shown. The difference between the measured sensor data and the modelled sensor data at each time step may be referred to as a process offset. In FIG. 11, the accumulated process offsets over time are also labelled for illustration purpose and better understanding.

[0075] For illustration purpose, FIG. 12 depicts a schematic diagram of an example physical system 1200 for stage 1 according to various example embodiments of the present invention, for modelling the physical process with respect to the level sensor in a tank (Tank 1) 1204. In the example physical system 1200, the tank 1204 in stage 1 of the SWaT testbed is being used as a running example to demonstrate the process skew based detection method 500 according to various example embodiments of the present invention. In FIG. 12, as shown, the water level in the tank 1204 is measured using a level sensor 1208 and the inflow and outflow of the water are controlled by the motorized valve (MV-101) 1212 at the input and pump (P-101) 1216 at the output, respectively. Various example embodiments model this inflow and outflow by considering the physical principles and the design parameters associated with the physical process. In particular, process skew information associated with the measured sensor data is extracted based on determining process dynamics drift from the design due to process noise. For example, for a tank, the rate of change of water inside the tank is equal to the difference between water flowing into the tank and water flowing out from the tank with respect to time. Accordingly, the rate of change of water inside the tank may be represented using a mass-balance equation, such as,

$$\frac{dV}{dt} = Q_{in} - Q_{out}$$

$$\frac{dh}{dt} = \frac{Q_{in} - Q_{out}}{A} \text{ since } V = A \times h$$

Equation (2)

where V denotes the volume of the tank, A denotes the cross-sectional area of the tank, and h denotes the height of the water inside the tank. Equation (2) provides a linear equation, and thus, the expression $[Q_{in} - Q_{out}]$ represents the water flow which depends on the PLC control actions implemented via the valve (MV-101) 1212 and the pump (P-101) 1216.

[0076] Accordingly, from FIG. 12, it can be seen that using the height and diameter of the tank from design documents, it is possible to determine the volume and the cross-sectional area of the tank. Assuming that the physical state of the physical process corresponds to the height of water (i.e., water level) inside the tank 1204, then the solution of Equation (2) produces the following result, $[x_{k+1} = x_k + u_k]$, where u_k is the PLC control action. In this regard, x_k represents water level in the tank at time k , and the control action u_k can be either open/close (for the motorized valve 1212) or on/off (for the pump 1216). Furthermore, by defining the sensor state, the following set of system equations can be obtained:

$$\begin{cases} x_{k+1} = Ax_k + Bu_k, \\ y_k = Cx_k \end{cases}$$

Equation (3)

where y_k is the sensor measurement (measured sensor data) driven by the control action u_k , and matrices A , B and C are the state-space matrices of appropriate dimensions.

5 [0077] From Equation (3), it can be seen that for a system state value at time k , and given the PLC control u_k , the next state at time $k + 1$ can be predicted. Table 2 in FIG. 9 shows a list of example design parameters for each type of control action. For example, for state process S4, the valve MV-101 1212 is controlled to be in an open state and the pump P-101 1216 is controlled to be in an activated (switched on) state. For example, based on these control
10 information from the PLC, various example embodiments estimate the sensor data of the physical state of the state process based on design parameters associated with the state process (e.g., estimated water level in the tank based on design parameters). However, as explained hereinbefore and further described below, for example due to the process noise, there are deviations between the measured sensor data and the estimated sensor data (or modelled sensor
15 data) with respect to the physical state.

[0078] A method of extracting process offsets in measured sensor data will now be described according to various example embodiments of the present invention. Using the process design parameters and the system of equations in Equation (3), process offsets (or process skews) may be extracted, for example, how much the real process dynamics are offset
20 from the designed physical process. For example, in FIGs. 13A to 13C to be described later below, the process offsets associated with the measured sensor data with respect to the level of the water in the above-mentioned tank 1204 for the three different state processes, namely S1, S3 and S4, can be seen.

[0079] In various example embodiments, for each time step, the process offset at the time
25 step may be defined as a deviation of the process dynamics due to the process inaccuracies from the design at the time step. For example, for each time step over a time period (e.g., the duration while a process run is active, which may be referred to as a process activity time frame), the process offset associated with the process run may be calculated or determined. All the process offsets associated with the process run may then be accumulated over the time period, to obtain
30 process offset data (including the process offsets accumulated over the time period) associated with the process run. A plurality of process offset data may thus be obtained for a plurality of process runs for a state process (e.g., for the plurality of process runs of the water emptying process (S1) as shown in FIG. 13A). Process skew fingerprint information associated with the

plurality of process runs for the state process may then be determined or extracted based on the plurality of process offset data obtained.

[0080] In various example embodiments, the process skew fingerprint information associated with a plurality of process runs may be determined based on a slope of the plurality of process offset data obtained on the plurality of process runs.

[0081] In FIGs. 13A to 13C, the accumulative process offsets for three different state processes, namely, S1, S3 and S4, respectively, can be seen. State process S1 is a water emptying process at the water emptying state (i.e., water outflow from the tank). In this regard, the negative slope indicates that the real process is actually slower than designed (i.e., based on design parameters). State process S2 is a static process corresponding to the process state of being static (i.e., there is no inflow or outflow), and thus, this state process is actually missing so no process offset exists. State process S3 is a water filling process at the water filling state (i.e., only the inflow is present). In this regard, the positive slope indicates that the real process is actually faster than designed. State process S4 is a water filling and emptying process at the water filling and emptying state (i.e., both the inflow and outflow are present). In this regard, the negative slope indicates that the real process is actually slower than designed. All these state processes (or process states) scenarios may be different state processes (or process states) of the same physical process, that is, with respect to the water tank 1204 in stage 1 of the SWaT testbed. In this regard, although they may be different state processes (or process states) of the same physical process, it can be observed that based on the corresponding process offsets obtained, all the state processes (or process states) of the physical process can be distinguished from each other. Accordingly, the method of extracting the process offsets in measured sensor data according to various example embodiments of the present invention advantageously establishes a process skew fingerprint, that is, fingerprinting the process runs for a process state based on process skews to obtain a corresponding process skew fingerprint.

[0082] Various example embodiments note that, as can be observed in FIGs. 13A to 13C, the process offsets obtained are noisy, for example, due to the sensor noise. In this regard, various example embodiments seek to remove, or at least mitigate, the sensor noise effect without disturbing the process offsets. Accordingly, in various example embodiments, process skew fingerprint information associated with a plurality of process runs for a state process is derived based on the plurality of process offset data produced for the plurality of process runs in the following manner.

[0083] Consider the linear time invariant model of the system with sensor and process noise as:

$$\begin{cases} x_{k+1}^* = Ax_k^* + Bu_k + v_k, \\ y_k^* = Cx_k^* + \eta_k, \end{cases}$$

5 Equation (4)

where y_k^* is the sensor measurement with the measurement noise η_k and x_{k+1}^* is the system state.

[0084] At each time step, the difference between sensor measurements given by Equation (4) and sensor measurement estimate given by Equation (3) is calculated to obtain the process offset as, $y_{k+1} - y_{k+1}^* = CA[O_k] - Cv_k - \eta_{k+1}$, where $O_k = x_k - x_k^*$.

10

[0085] Without wishing to be bound by theory, a proof for the above derivation of the process offset is provided as follows. The difference between Equations (4) and (3) may be expressed as:

$$y_{k+1} - y_{k+1}^* = Cx_{k+1} - Cx_{k+1}^* - \eta_{k+1}$$

15 Equation (5)

$$y_{k+1} - y_{k+1}^* = CAx_k + CBu_k - CAx_k^* - CBu_k - Cv_k - \eta_{k+1}$$

Equation (6)

$$y_{k+1} - y_{k+1}^* = CA(x_k - x_k^*) - Cv_k - \eta_{k+1}$$

Equation (7)

[0086] As the process offset is defined as the difference the real system state and the estimated state of the system ($x_k - x_k^*$), it produces,

20

$$y_{k+1} - y_{k+1}^* = CA[O_k] - Cv_k - \eta_{k+1}$$

Equation (8)

Accordingly, it can be seen from Equation (8) that the process offset (O_k) can be extracted at each time step.

25

[0087] From Equation (8), it can be observed that the process offset includes the noise from the sensor. In this regard, various example embodiments apply a linear regression model on the plurality of process offset data to obtain a regression coefficient, which corresponds to the process skew fingerprint information. For example, a straight line may be fitted onto the plurality of process offset data to determine the slope of the plurality of process offset data.

30

Accordingly, for each state process (e.g., each of the three state processes shown in FIGs. 13A to 13C), a straight line may be fitted onto the plurality of process offset data associated with the plurality of process runs for the state process in relation to the physical state (e.g., water level)

to determine the slope thereof, which may represent the process skew fingerprint information associated with the plurality of process runs for the state process at the process state of the physical process. Accordingly, various example embodiments apply a linear regression model on the plurality of process offset data obtained for each state process. For example, from FIG. 5 13A to 13C, it can be observed that the process offsets obtained for each state process are generally linear in time.

[0088] In various example embodiments, to establish the linearity between the time and the progression of the process offsets, correlation coefficients are used. Correlation calculates the level of the linear relationship between variables. For example, a high correlation between two 10 variables indicates that the values for the variables increase or decrease in a linear relationship. However, uncorrelated variables may still be dependent on each other, just that the relationship may be nonlinear. For example, for N scalar values of two variables, the Pearson correlation coefficient may be defined as:

$$15 \quad \rho(X, Y) = \frac{\sum_{i=1}^N (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^N (X_i - \bar{X})^2} \sqrt{\sum_{i=1}^N (Y_i - \bar{Y})^2}}$$

Equation (9)

where $\bar{X}$ denotes the mean of the variable X , and $\bar{Y}$ denotes the mean of the variable Y . In this regard, various example embodiments found that the process data is linearly correlated with the time as the process is linearly increasing or decreasing in time. In various example embodiments, 20 a linear regression approach is adopted to obtain a data model describing the relationship between variables in a mathematical form. In various example embodiments, a least squares fit is applied to obtain the model for a set of n observed values of X and Y given by $X = (x_1, x_2, \dots, x_n)$ and $Y = (y_1, y_2, \dots, y_n)$, respectively. These values for a system of linear equations may be represented in matrix form as:

$$25 \quad \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & x_1 \\ 1 & x_2 \\ \vdots & \vdots \\ 1 & x_n \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix}$$

which may be simplified to:

$$Y = \beta_0 + \beta_1 X + \epsilon,$$

Equation (10)

where β_0 is the y-intercept, β_1 is the slope/regression coefficient and ϵ is the model error.

[0089] FIG. 14 depicts a plot of a plurality of process offset data for the water filling process in stage 1 of the water treatment system, with a linear regression model fitted thereon, according to various example embodiments of the present invention. The linear regression model is used to find the slope that defines process skew fingerprint information representing the process
 5 skews associated with the plurality of process runs. For example, the accuracy of the linear regression model can be seen in FIG. 14. To quantify the goodness of a system model, mean square error (MSE) may be used as a metric. In particular, one minus the root mean square error (RMSE) defines the estimation accuracy or best fit of a model,

$$RMSE = \sqrt{\frac{\sum_{i=1}^n (y_i - \hat{y}_i)^2}{n}}$$

10

Equation (11)

[0090] MSE is the difference between measured sensor data and estimated sensor data (or modelled sensor data) squared, and in general, provides the distance between measured and estimated value, in other words, how far the estimated value is from the measured value. The model accuracies for the three stages of the SWaT testbed and corresponding state processes
 15 used in the experiments conducted (from the SWaT testbed) are shown in Table 3 in FIG. 17. It can be seen that the obtained system model is very accurate, with almost zero mean error for all the process runs of a plurality of state processes. Table 3 in FIG. 17 shows the mean of models created for all the process runs of the plurality of state processes. Accordingly, from Table 3, the use of the linear regression model to find a good fit for the plurality of process
 20 offset data to determine the corresponding process skew fingerprint information is validated. In various example embodiments, the process offsets accumulated for a process run of a state process may be expressed as:

$$O_{accum} = \sum_{k=1}^n (O_k)$$

Equation (12)

25 and the corresponding process skew fingerprint information ($Process_{skew}$) may be determined as:

$$Process_{skew} = \frac{d(O_{accum})}{dt}$$

Equation (13)

[0091] The uniqueness of the process skew fingerprint information obtained will now be
 30 described according to various example embodiments of the present invention. FIG. 15A

depicts a plot of three process skew fingerprint information obtained with respect to three state processes, respectively, at stage 1 of the SWaT testbed, FIG. 15B depicts a plot of three process skew fingerprint information obtained with respect to three state processes, respectively, at stage 3 of the SWaT testbed, and FIG. 15C depicts a plot of two process skew fingerprint information obtained with respect to two state processes, respectively, at stage 4 of the SWaT testbed. Accordingly, FIGs. 15A to 15C depict process skew fingerprint distribution for eight state processes at three stages of the SWaT testbed. From FIGs. 15A to 15C, it can be observed that all of the eight state processes can be uniquely distinguished based on the process skew fingerprint profile, according to various example embodiments of the present invention. Therefore, FIGs. 15A to 15C show a visual analysis for process skew fingerprint uniqueness. In addition, without wishing to be bound by theory, a mathematical proof for the process skew fingerprint uniqueness will now be described. For example, demonstrating that fingerprints are information-theoretically unique helps to negate the possibility of impersonation attacks. Let $w(t)$ be the signal corresponding to a process skew fingerprint. In order to present an information-theoretic analysis, justification of two important criteria are provided:

(1) mutual information between process skew fingerprints as recorded for the same process, that is, in successive operations should be high, ≈ 1 , and

(2) conditional entropy of process skew fingerprints with other process skew fingerprints should be very low, $\ll 1$.

[0092] In order to investigate these relations, mutual information, $I(\cdot)$, for process i is defined as $I(w_{ij}, w_{ik}) = H(w_{ij}) - H(w_{ij}|w_{ik})$, where $i \in 1 : S, j \in 1 : N, H(w_{ij})$ is entropy of j^{th} attempt by a process i and $H(w_{ij}|w_{ik})$ is conditional entropy of i^{th} process for j^{th} attempt, given the features of k^{th} attempt. For high recall, mutual information for each of the process skew fingerprints should be close to 1 (normalized). Similarly, an ICS process i should not have access to any extra information about process t given observations of its own. Mathematically this can be quantified in condition entropy as $H(w_{ij}|w_{tk})$ for $i \in 1 : S$ and $j, k \in 1 : N$. Entropy measure and mutual information were evaluated for each of the process skew fingerprints. As can be seen in FIG. 16, mutual information across the above-mentioned eight process skew fingerprints are fairly low (less than 0.1), which demonstrates the uniqueness of the process skew fingerprints obtained. Entropy of each of the process skew fingerprints was recorded to be ≥ 0.94 . In addition, investigation of conditional entropy across different processes of the ICS system reveals that features are independent.

[0093] An example anomaly detector according to various example embodiments of the present invention will now be described. As described hereinbefore, the process offsets for different runs of a particular state process at a process state (e.g., a water filling process) are accumulated. In various example embodiments, a process skew vector (determined based on the corresponding process skew fingerprint information) is provided as an input to the anomaly detector, which for example, may be a cumulative sum (CUSUM) detector and known as the stateful detector. The input (process skew vector) to the CUSUM procedure may be considered as a distance measure, that is, a measure of how far the estimated measurements is from the expected measurements. In various example embodiments, a dedicated anomaly detector for each process state may be designed. The index i denotes the process, $i \in I := \{1, 2, \dots, m\}$, where m is the number of processes in each stage of the plant. Process skew fingerprint is denoted as $r_{k,i}$ for easy reference, where k is the time step. The standard CUSUM procedure (e.g., as described in D.C. Montgomery, Introduction to Statistical Quality Control, Wiley, 2009) is explained using the following equations.

15

CUSUM: $S_{0,i}^- = \bar{T}_i$, $S_{0,i}^+ = \bar{T}_i$, $\tilde{k}_i^+ = 0$, $\tilde{k}_i^- = 0$,

$$\begin{cases} S_{k,i}^+ = \max(\bar{T}_i, S_{k-1,i}^+ + r_{k,i} - \bar{T}_i - \kappa_i), & \text{if } S_{k-1,i}^+ \leq \tau_i^+, \\ S_{k,i}^+ = \bar{T}_i \text{ and } \tilde{k}_i^+ = \tilde{k}_{i-1}^+ + 1, & \text{if } S_{k-1,i}^+ > \tau_i^+. \end{cases}$$

Equation (14)

$$\begin{cases} S_{k,i}^- = \min(\bar{T}_i, S_{k-1,i}^- + r_{k,i} - \bar{T}_i + \kappa_i), & \text{if } S_{k-1,i}^- \geq \tau_i^-, \\ S_{k,i}^- = \bar{T}_i \text{ and } \tilde{k}_i^- = \tilde{k}_{i-1}^- + 1, & \text{if } S_{k-1,i}^- < \tau_i^-. \end{cases}$$

20

Equation (15)

Design parameters: Bias $\kappa_i > 0$; threshold $\tau_i > 0$.

Output: Alarm(s) = $\tilde{k}_i^+ + \tilde{k}_i^-$.

[0094] From Equations (14) and (15), it can be observed that $S_{k,i}^+$ and $S_{k,i}^-$ accumulate the distance measure $r_{k,i}$ over time to measure how far are the values of the residual from the target mean ($\bar{T}_i$). To tune the CUSUM detector, there is also a slack variable κ chosen to be $\frac{1}{2} * \sigma_i$ in this experiment conducted. $\tau_i = \pm \Gamma * \sigma_i$, where Γ is a multiplier to the standard deviation (σ) and may typically be between 3 and 5. In various example embodiments, an alarm is raised when this accumulation becomes greater or less than a predetermined threshold τ_i . For example, based on a threshold that is derived from the process skew fingerprint information obtained under normal operation, an alarm may be raised when the accumulation crosses the threshold.

30

The sequence $S_{k,i}$ is reset to the target mean value each time it becomes negative or larger than τ_i . If $r_{k,i}$ is tightly bounded and κ_i is not sufficiently large, the CUSUM sequence $S_{k,i}$ grows unbounded until the threshold τ_i is reached, no matter how large τ_i is set. In order to prevent such drifts, the slack variable κ_i is selected properly based on the statistical properties of the distance measure. Once κ is chosen, the threshold τ_i must be selected to achieve a required false alarm rate $\mathcal{A}_i^*$. $\mathcal{A}_i \in [0, 1]$ denotes the false alarm rate for the CUSUM procedure defined as the expected proportion of observations which are false alarms.

[0095] To demonstrate the effectiveness of the process skew based detection method according to various example embodiments, the process skew based detection method is evaluated in a real water treatment testbed. For example, the following metrics are used for performance evaluation. TP_i denotes true positive for class c_i when it is rightly classified based on the ground truth, FN_i denotes false negative for class c_i when it is wrongly rejected, FP_i denotes false positive for class c_i when it is wrongly accepted, and TN_i denotes true negative for class c_i when it is rightly rejected. The True Positive Rate (TPR) and False Positive Rate (FPR) are defined as follows:

$$\text{True Positive Rate (TPR)} = \frac{TP}{TP+FN} = 1 - FNR, \quad \text{Equation (16)}$$

$$\text{False Positive Rate (FPR)} = \frac{FP}{FP+TN} = 1 - TNR. \quad \text{Equation (17)}$$

[0096] Ideally, FPR should be as small as possible and TPR as high as possible. Both TPR and FPR being a ratio ranging between 0 and 1.

[0097] In experiments conducted, normal operation data (or reference operation data, e.g., without attack or breakdown) from the SWaT testbed is collected for a period of seven days. During normal operations, the water treatment plant was run continuously under normal conditions and as it was designed to operate. The operating conditions from the design are presented in Table 2 in FIG. 9. For all the possible state processes, measured sensor data is extracted. Process offsets (e.g., corresponding to the plurality of reference process offset data as described hereinbefore according to various embodiments) are extracted for each state process in stage 1, stage 3 and stage 4 of the SWaT testbed. Stage 2 and stage 5 relate to chemical sensors and reverse osmosis process, respectively, and therefore, these two stages are not considered in the experiments. The experiments are focused on examining the physical properties of the process. During the seven days, water filling or emptying process occurred

hundreds of times (i.e., hundreds of process runs for this process state, e.g., corresponding to the plurality of reference process runs as described hereinbefore according to various embodiments). Process offsets are determined for each of these process runs. As explained hereinbefore, process offsets are noisy due to noise from the sensors. In this regard, a linear regression model is fitted on the plurality of process offset data obtained associated with the plurality of process runs to address the noise in the signal. After the linear regression model is fitted, a straight line is obtained for the accumulated process offsets associated with the plurality of process runs over a process time frame. The rate of change of these process offsets (corresponding to the slope of the straight line) may then be defined as the process skew fingerprint (e.g., corresponding to the reference process skew fingerprint information as described hereinbefore according to various embodiments) associated with the plurality of process runs.

[0098] For example, as described hereinbefore, FIGs. 13A to 13C show the process offsets for different state processes of the stage 1 of the SWaT testbed. FIG. 14 shows an example of linear model fitting for the process offsets. The obtained linear model may thus be used to calculate the process skew fingerprint. The process skew fingerprints obtained under normal operating conditions (which may be referred to as normal or reference process skew fingerprints) may then be used by an anomaly detector (e.g., the CUSUM detector) for detecting an anomaly in a physical process. The CUSUM parameters for all the stages in SWaT are shown in Table 4 in FIG. 18. In particular, Table 4 shows the design and performance of the CUSUM detector on the normal operation data. All the thresholds and other parameters are designed to have a desired false alarm rate of less than 5%. Table 4 shows bias parameter κ , threshold τ , mean μ and standard deviation σ for the process skew fingerprints. In the last two rows of Table 4 in FIG. 18, performance of the CUSUM detector under the normal operating conditions are shown using the design parameters specified. It can be observed that for all the cases the desired false alarm rate is below 5%.

[0099] Table 4 in FIG. 18 shows a high true negative rate, which indicates that it is possible to identify each state process (or process state) with a high accuracy based on the process skew fingerprint. A physical process goes through different state processes (or process states) during the operation of the process plant. For example, for the process of a fluid tank, either fluid is flowing out, flowing in, both or in a static state. Since different state processes have different process skew fingerprints according to various example embodiments of the present invention,

it is possible to uniquely identify each state process (or process state) based on its associated process skew fingerprint.

[00100] In experiments conducted, a particular process, for example, a water filling process started at different initial states depending on the control logic. The results presented in Table 4 in FIG. 18 is a combination of all possible initial conditions of a particular process and a process skew fingerprint is created with respect to all the process runs for the process state. It can be seen from Table 4 in FIG. 18 that the process skew based fingerprint is stable over a range of process start and end conditions making it robust for application in a real-world system.

[00101] The performance of the process skew based detection method 500 as an attack detection method is evaluated under a range of attack data collected from SWaT testbed. The SWaT testbed was subject to different attack scenarios for four days. In particular, over the four days, there were many process runs of normal operation and then there were attack instances in between. A complete list of attacks is shown in Table 1 in FIGs. 7A and 7B. An example of process offsets (or process skews) obtained for the process runs in relation to tank 4 in stage 4 is shown in FIG. 19. In particular, FIG. 19 depicts a plot of the process offsets obtained on the process runs in relation to tank 4 in stage 4, including a mixture of normal process runs and a few attacks. From FIG. 19, it can be observed that the process offsets obtained associated with normal process runs are close together and follow the normal profile of the process runs. On the other hand, the process offsets obtained associated with attacks (attack start and attack stop are denoted in FIG. 19) show clear deviations. Accordingly, from FIG. 19, it is evident that using process offsets according to various example embodiments of the present invention enable easy detection of attacks since the attack scenarios clearly deviate from the normal process offsets. In some cases, when the attack was stopped, the slope of the process offsets (corresponding to process skew fingerprint) tends to return to normal as expected but the whole data offsets have deviated for the overall process.

[00102] FIGs. 20A and 20B show the CUSUM detector for the same process. In particular, FIGs. 20A and 20B depict plots in relation to an attack detection example for LIT-401, outflow process. From FIGs. 20A and 20B, it can be observed that the process skew fingerprint according to various example embodiments of the present invention enables the detection of an attack easily and effectively. A detailed analysis was carried out for all the three stages and corresponding state processes in the SWaT testbed and the results are presented in Table 5 shown in FIG. 21. In particular, FIG. 21 shows the evaluation results of the process skew based detection method 500 according to various example embodiments of the present invention on

the attack data from the SWaT testbed. The TPR presents the attacks which were detected accurately as percentage (attacks-detection/total-attacks-executed). From FIG. 21, it can be seen that all the attacks are detected in all the scenarios with 100% TPR. Furthermore, FPR is close to the desired 5% false alarm rate except for two instances. Accordingly, the process skew based detection method 500 has shown perfect performance on attack detection.

[00103] A stealthy attack is an attack designed to be hidden for a system model based attack detector. For a stealthy attack, the objective of the attacker is to modify the physical process measurements to achieve its objective and remain hidden. FIGs. 22A and 22B show the execution of such an attack in stage 1 of the SWaT testbed. In FIG. 22A, a plot of level sensor (LIT-101) actual measurements and sensor estimates obtained using the system model is shown. In FIG. 22B, respective residual (measured - estimated) values for the level sensor are shown. Upper and lower limits for a statistical detector are also shown. In FIG. 22A, the dotted line shows the ground truth for the state process, while the attacker is spoofing the sensor values and managed to derive the system away from the normal operation over time during the attack period. The spoofed values are chosen such that the residual values never grow bigger than a model-based detector threshold and hence, could not get detected. But from the ground truth, the process dynamics are not what the attacker is making the PLC believe. Accordingly, using the process offsets according to various example embodiments of the present invention, it is possible to detect the presence of such an attacker. In particular, if an attacker wants to deviate the process from its desired operation, it must defy the process dynamics and expose itself in the process offsets. Accordingly, it has been demonstrated that the process skew based detection method 500 is able to detect attacks that are stealthy for the system model based detectors.

[00104] Although the process skew based detection method 500 according to various example embodiments of the present invention has been described with respect to a water treatment plant, it will be appreciated by a person skilled in the art that the present invention is not limited to a water treatment plant. For example, physical processes have been discussed herein with respect to water/fluid dynamics but it will be appreciated that other similar processes are also applicable, such as but not limited to, gas or other chemical fluids where the process skew based detection method 500 can also be applied in the same or similar manner. Moreover, a range of different processes and process states have been considered herein which demonstrate the scalability of the process skew based detection method 500 according to various example embodiments of the present invention. Accordingly, demonstration on a real system highlights its applicability in real-world applications.

[00105] Accordingly, various example embodiments demonstrate that indeed a process skew (process offset) exists for each process (e.g., process run) due to the deviations in the process itself from designed. As described hereinbefore, the process skew based detection method 500 may be used to fingerprint different state processes of a physical process, for example, filling, emptying or a combination of these process dynamics in a water treatment system. Therefore, it is possible to detect attacks on the state processes, as well as identify the particular state process/processes (or the particular process state(s)) of the physical process being attacked when the attack occurred. In this regard, the extensive evaluation of the process skew based detection method 500 on a real-world water treatment system validated its applicability and practicality, as well as effectiveness.

[00106] While embodiments of the invention have been particularly shown and described with reference to specific embodiments, it should be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the scope of the invention as defined by the appended claims. The scope of the invention is thus indicated by the appended claims and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced.