



- (51) **International Patent Classification:**
G05B 13/04 (2006.01) **H04L 29/06** (2006.01)
G06F 21/55 (2013.01)
- (21) **International Application Number:**
PCT/EP2013/002162
- (22) **International Filing Date:**
22 July 2013 (22.07.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
12005375.6 24 July 2012 (24.07.2012) EP
- (71) **Applicant:** **ETH ZURICH** [CH/CH]; Raemistrasse 101/ETH transfer, CH-8092 Zurich (CH).
- (72) **Inventors:** **ANDERSSON, Göran**; Buenstrasse 14, CH-8600 Dübendorf / ZH (CH). **LYGEROS, John**; Pilgerweg 4, CH-8044 Zürich / ZH (CH). **VRAKOPOULOU, Maria**; Winterthurerstrasse 16, CH-8006 Zürich / ZH (CH).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM,

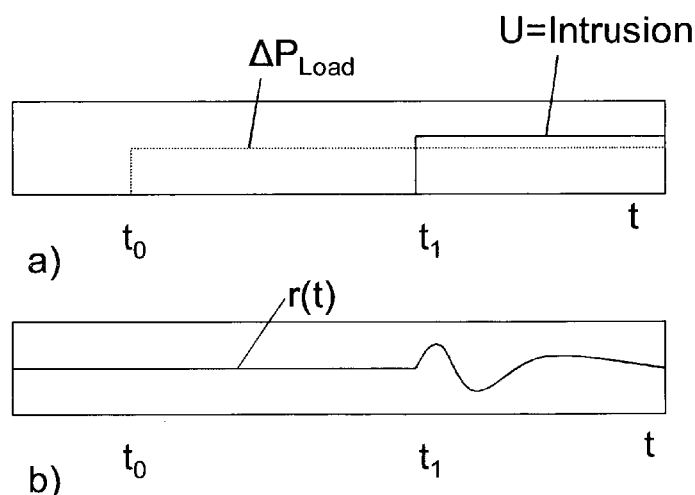
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

- (54) **Title:** APPARATUS AND METHOD FOR DETECTING AN INTRUSION IN ELECTRIC POWER NETWORKS

**FIG. 3**

(57) **Abstract:** In a method for detecting an intrusion in an electric power network, status signals are measured from the electric power network. A vector ($Y(t)$) of the measured status signals is supplied to a filter (1), a transfer function of which filter (1) is given by $N(p)*L(p)$ with p representing a differential operator, wherein $L(p)$ is a polynomial matrix in the differential operator p to be applied to the status signal vector ($Y(t)$), and $N(p)$ is a polynomial vector in the differential operator p and represents a solution to equation $N(p)*H(p)=0$ wherein $H(p)$ is a polynomial matrix in the differential operator p to be applied to internal status signals ($x(t)$) and/or to a load deviation pattern ($d(t)$) applied to a model of the electric power network. The filter (1) supplies an intrusion detection signal ($r(t)$) in response to applying the received status signal vector ($Y(t)$) to the filter (1). In a preferred approach, the filter is designed as insensitive as possible to load deviations.

**APPARATUS AND METHOD FOR DETECTING AN INTRUSION IN ELECTRIC
POWER NETWORKS****NETWORKS**Technical Field

5

The present idea pertains to the field of intrusion detection in electric power networks.

Background Art

10

Electric power networks, also denoted as power grids, are key for today's way of living in view of an ever increasing amount of electrical load to be served by those electric power networks.

15

With the advent of computational infrastructure for controlling electrical power networks including its generators etc., the generation and distribution of electricity in turn becomes more and more prone to defects in such IT infrastructure and/or to manipulation of such IT infrastructure. In the context of computing, an external manipulation of IT infrastructure is also denoted as intrusion. The art of detecting intrusions in computational resources and/or informational networks is denoted as intrusion detection.

20

25

Hence, it is desired to detect intrusions in electrical power networks including intrusions as a result of intrusion in the IT infrastructure of an electrical power network.

30

Disclosure of the Invention

This problem is solved by an apparatus for detecting an intrusion in an electric power network, and by a method for detecting an intrusion in an electric power network.

35

According to a first aspect of the present invention, an apparatus comprises a receiver for receiving a vector of status signals measured from the electric power network and a filter for providing an intrusion detection signal in response to applying the received status signal vector to the filter. A transfer function of which filter is given by $N(p)*L(p)$ with p representing a differential operator, wherein $L(p)$ is a polynomial matrix in the differential operator p to be applied to the status signal vector $(Y(t))$, and $N(p)$ is a polynomial vector in the differential operator p representing a solution to equation $N(p)*H(p)=0$ wherein $H(p)$ is a polynomial matrix in the differential operator p to be applied to internal status signals $(x(t))$ of a model of the electrical power network and/or to a load deviation pattern $(d(t))$ applied to a model of the electrical power network.

According to a second aspect of the present invention, a method is provided wherein status signals in the electric power network are measured and a vector of the measured status signals is applied to a filter. The filter supplies an intrusion detection signal in response to applying the received status signal vector to the filter. A transfer function of the filter is given by $N(p)*L(p)$ with p representing a differential operator, wherein $L(p)$ is a polynomial matrix in the differential operator p to be applied to the status signal vector $(Y(t))$, and $N(p)$ is a polynomial vector in the differential operator p and represents a solution to equation $N(p)*H(p)=0$ wherein $H(p)$ is a polynomial matrix in the differential operator p to be applied to internal status signals $(x(t))$ of a model of the electric power network and/or to a load deviation pattern $(d(t))$ applied to a model of the electrical power network.

In a preferred embodiment, the electric power network contains computational infrastructure for controlling actuators of the electric power network such as

generators, switches, etc. In a specific embodiment a computational infrastructure is common for the electrical power network such that a central control may adjust the power output at different generators within a given area of the electrical power network. Such system is also known as Automatic Generation Control (AGC) since the power generation and distribution is automatically controlled without the intervention of a human being. Specifically in such system, the central control may be vulnerable to attacks / intrusion into the IT infrastructure.

In a preferred embodiment, the filter is online connected to sensors for measuring signals representative of the operation of the electrical power network, such as the measuring of a frequency of a turbine of a generator. Preferably, the vector of measured status signals represents signals or status information at a common point in time, or within a short period of time, such as within five minutes. In an embodiment, the filter may be located at the location of a central control unit representing the AGC, and may be embodied by a common computational infrastructure.

In a preferred embodiment, the intrusion detection signal is displayed on a display and/or triggers an optical or acoustic warning. The intrusion detection signal may also be used for triggering emergency routines such as powering down a generator, injecting a counter-signal balancing an intrusion signal, and/or shutting down the central control unit for preventing from further damages.

Other advantageous embodiments are listed in the dependent claims as well as in the description below.

Brief Description of the Drawings

The invention will be better understood and objects other than those set forth above will become apparent from the following detailed description thereof. Such description makes reference to the annexed drawings, wherein:

Figure 1, a sample topology of an electrical power network.

Figure 2, a block diagram of generators connected to a central control unit,

Figure 3, a sample intrusion detection signal as result of a method and/or an apparatus according to an embodiment of the present invention, and

Figure 4, a block diagram according to an embodiment of the present invention.

Modes for Carrying Out the Invention

An electrical power network according to an embodiment of the present invention may be understood as a network confined by a given geographical area. An electrical power network may include multiple generators for generating electrical energy. The generators are typically allocated in power plants spread across the area. Power lines also denoted as buses are provided between generators and between generators and consumers for transferring the generated electrical energy to a destination. In addition, there may be power lines between areas with different electrical power networks which lines are also denoted as tie lines. Those tie lines may be used for compensating a shortage of energy in one of the connected electrical power networks, or for any other balancing of power levels in the different networks.

In an embodiment, the generators for generating electrical energy are equipped with a frequency control. This means that a frequency of an electrical output

of the generator is controllable. At the same time, the frequency of the electrical power signal supplied by the generator into the electrical power network represents a frequency of a turbine of the generator since it is a rotational motion of such turbine which generates the electrical power signal. A local control of the frequency may be applied, which is also denoted as primary frequency control, and which preferably may reside at the location of the generator or at the associate power plant. The primary frequency control may include monitoring a frequency output of each generator or a rotation frequency of the corresponding turbine. The frequency preferably can be adjusted in order to match a reference value, or in order to compensate for more or less power required in the network as a result of increased or decreased electrical load in the network. Hence, the local control unit may be adapted to preferably adapt a set-point in form of such reference value for the generator and is capable of controlling the frequency of the generator, preferably in a closed-loop-control, and as a result, is capable of controlling the frequency of the electrical power signal supplied into the power lines.

Preferably, multiple generators of an electrical network, e.g. confined to a common area, are under a common control in addition to the local control. The common control includes a central control unit that is adapted to act on multiple individual generators spread across the electrical power network and mostly being arranged remote from the central control unit. Hence, in the present embodiment a central control unit may act on various generators in the network and control their frequency. Such central control unit may adjust the power output of the various generators at even different power plants in response to a generation-load mismatch in the electrical power network. Such concept is also denoted as Automatic Generation Control (AGC). In such embodiment, preferably a system frequency of the electrical power

network is measured and is regulated in a closed-loop control to match a reference frequency or to compensate for generation-load mismatches in the network. The various generators of the electrical power network participating in the AGC represent actors of such closed-loop control. Subject to a deviation of the system frequency from the reference frequency, which deviation may be caused by an increase or decrease in load on the network, individual, multiple or all generators participating in the common closed-loop frequency control may be addressed for increasing or decreasing their individual power output. Such common closed-loop frequency control which is also denoted as secondary frequency control may be executed in parallel to the primary frequency control. A selection of which generators are addressed by the common frequency control may be made subject to a policy, for example, to provide equal wear amongst the generators such that always the generators with the least runtime may be preferred when an increased supply of more power is desired. Other criteria may, of course, be applied.

In addition to a control of the system frequency which may include a control of the frequency of the various individual generators participating in the common frequency control approach, a power exchange on tie lines between electrical power networks may be controlled, too, by such central control adjusting an exchange of energy between different electrical power networks. Preferably, the generators of an electrical power network and/or the power exchanged via tie lines is controlled in the common closed-loop control system to predefined fix or variable reference values which may represent the above mentioned set-points.

For determining a filter to be introduced later on, it is preferred to first model the behaviour of an electrical power network as follows:

It is assumed that the electrical power network comprises a number g of generators and a number n of

non-generator nodes such as consumers. Each generator may be modelled as a constant voltage source behind a transient reactance x'_d . Therefore, for each generator a virtual node E_G - also denoted as internal generator node - is added to represent the internal voltage source, resulting in a system representing the electrical power network of an area A with $n+g$ buses.

Assuming that dynamics of a turbine associated with a generator i for generating electrical energy is represented by a first order transfer function, an oscillation of the subject generator i may be described in the time domain by:

$$\dot{\delta}_i = 2\pi(f_i - f_0) \quad \text{equation (1)}$$

$$\dot{f}_i = \frac{f_0}{2H_i S_{B_i}} (P_{m_i} - P_{e_i} - \frac{1}{D_i}(f_i - f_0) - \Delta P_{Load_i}) \quad \text{equation (2)}$$

$$\dot{P}_{m_i} = \frac{1}{T_{ch,i}} (P_{m_i}^0 + \Delta P_{p_i} + \Delta P_{agc} - P_{m_i}) \quad \text{equation (3)}$$

wherein

- δ_i represents a rotor angle of a turbine of the generator in rad,
- f_i represents a rotor electrical frequency in Hz,
- P_{m_i} represents a generated electrical power of the turbine as its output in MW,
- P_{e_i} represents an electrical power consumed by the load on the generator and the other loads of the electrical power network connected through to the generator, in MW,
- ΔP_{Load} represents a deviation of the load from its initial value at the generator node in MW (),
- f_0 represents the initial rotor electrical frequency in a steady state in Hz, e.g. 50 Hz in Europe,
- H_i represents the inertia time constant in sec, defined as a ratio between a rotational energy stored in the generator and a nominal power of the generator,

- S_{Bi} represents the generators rated power in MW,,
i.e. its nominal power,
- D_i represents a frequency dependency of the load,
- $T_{ch,i}$ represents a time constant of the turbine in
5 sec,
- P_{mi}^0 represents an initial set-point of the genera-
tor in MW,
- ΔP_{pi} represents a deviation in power caused by the
primary frequency control at the subject generator
10 in MW,
- P_{mi} is the generated power output of the turbine of
the subject generator in MW,
- ΔP_{agc} represents a deviation in power caused by the
secondary frequency control at the subject generator
15 in MW.

Equation (3) basically claims that a load de-
viation ΔP_{Load} impacts the frequency f_i according to equa-
tion (2) and as a result the power P_{mi} generated by the
turbine preferably compensates ΔP_{pi} representing an
20 in/decrease of power by means of a primary frequency con-
trol at the subject generator i , and ΔP_{agc} representing an
increase/decrease of power by means of a secondary prima-
ry frequency control by a central control unit including
a frequency regulation at the subject generator and in-
25 cluding a share of power imported /exported from/to other
electrical networks via its tie lines. Hence, ΔP_{agc} repre-
sents a power increase/decrease caused at the generator
node by what is called the automatic generation control
AGC or the secondary frequency control, which power in-
30 crease/decrease is broken down to the individual
nodes/generators.

However, P_{ei} and P_{agc} are related to dynamic
states of the generator i via algebraic equations. Power
flows in the electrical power network instead may prefer-
ably be expressed by means of voltages at given locations
35 and by means of a bus admittance matrix of a network rep-
resenting the electrical power network. Hence, within the

above model description of the electrical power network it is desired to express the power flows as a function of the internal voltage E_{Gi} of the subject internal node i , i.e. generator i . A vector E_G comprising the generator
 5 internal node voltages of the electrical power network is built, wherein E_{Gi} denotes the voltage at the i -th generator out of the set of g generators. Here, it is assumed that $E_{Gi} = |E_{Gi}^0|$ at δ for all $i=1, \dots, g$ wherein δ is a phase
 10 angle of the generator voltage which is assumed to coincide with the rotor angle δ , and wherein $|E_{Gi}^0|$ is constant given that voltage control is not used. Hence, a power flow with respect to a generator node i may only depend on its phase angle δ .

For any rest of nodes of the electrical power network excluding the generator internal nodes, voltages
 15 V_{Ni} are included in a corresponding vector V . For removing the algebraic constraints for P_{ei} and P_{agc} the internal nodes of the generators are retained and any rest of the nodes is eliminated by assuming a constant impedance load
 20 for allowing the rest of nodes to be included in a network admittance matrix Y . In such approach, the nodes are partitioned by

$$I = \begin{bmatrix} I_G \\ I_N \end{bmatrix} = Y \begin{bmatrix} E_G \\ V_N \end{bmatrix} = \begin{bmatrix} Y_{GG} & Y_{GN} \\ Y_{NG} & Y_{NN} \end{bmatrix} \begin{bmatrix} E_G \\ V_N \end{bmatrix} \quad \text{equation (4)}$$

25 wherein the bus admittance matrix Y includes transient reactances of the generators and admittances representing loads. Hence, the bus admittance matrix Y represents a topology of the electrical power network including reac-
 30 tances/admittances of both of nodes, generators and non-generators. E_G and V_N represent the above voltage vectors, and I_G and I_N represent the associate injection current vectors. For resolving equation (4) it can be assumed that at the non power generating nodes V no current is
 35 injected, i.e. $I_N=0$. In this case, equation (4) can be resolved into

$$I_G = Y_G E_G \quad \text{equation (4.1)}$$

$$V_N = K_V E_G + Y_{NN}^{-1} \quad \text{equation (4.2)}$$

with

$$Y_G = Y_{GG} - Y_{GN} Y_{NN}^{-1} Y_{NG} \text{ and } K_V = -Y_{NN}^{-1} Y_{NG}$$

Equation (4) helps in determining the value P_{ei} of power consumed in generator i since such power may be denoted as voltage E_{Gi} of the subject node multiplied by the conjugate of the current on the buses / power lines to other generator nodes j to which the present generator node i is connected to. The current on the buses/power lines to the other generators j can be expressed by the voltage E_{Gj} of these other nodes divided by the reactances of these other nodes j .

Hence, the power consumption per generator node i is determined by:

$$P_{ei} = \sum_{j=1}^g |E_{Gi}^0| |E_{Gj}^0| (B_{ij} \sin(\delta_i - \delta_j) + G_{ij} \cos(\delta_i - \delta_j)) \quad \text{equation (5)}$$

wherein B_{ij} and G_{ij} are real and imaginary admittance values of the admittance matrix Y_G .

Hence, by equations (1), (2), (3) and (5), a generator node i is described by means of nonlinear differential equations.

An entire electrical power network confined to a given area may as such be described by a model comprising a set of nonlinear differential equations containing the differential equations for all generator nodes comprised in the electrical power network.

Whenever an intrusion is assumed, such intrusion may apply to the term ΔP_{agc} in the model for the reason that this term represents the power adjustment caused by the central control unit regulating, such that any intrusion into the central control unit by e.g. a virus or anything similar affecting the IT infrastructure of the

central control unit may lead to convert equation (3) into

$$\dot{P}_{m_i} = \frac{1}{T_{ch,i}} (P_{m_i}^0 + \Delta P_{p_i} + (\Delta P_{agc} + U) - P_{m_i}) \quad \text{equation (3.1)}$$

5

wherein U denotes an intrusion signal.

The above model of the electrical power network now including the intrusion signal U may be rewritten in a more compact form in the following ordinary
10 state space description:

$$\begin{aligned} \dot{X}(t) &= h(X(t)) + B_u u(t) + B_d d(t) + B_f f(t) \\ Y(t) &= CX(t) + D_u u(t) + D_d d(t) + D_f f(t) \end{aligned} \quad \text{collectively equation (6)}$$

15 wherein

- vector $X(t) := [\{\delta_i\}, \{f_i\}, \{P_{m_i}\}, \Delta P_{agc}]$ represents internal states of the electrical power network containing turbine rotation angles δ_i , electrical frequencies f_i of the various generators i , generated power outputs of the turbine of the subject generator P_{mi} , and deviations in power caused by the secondary frequency control at the subject generator ΔP_{agc} ,
- $d(t) := \{\Delta P_{Load_i}(t)\}$ represents an unknown load disturbance ΔP_{Load_i} ,
- 25 - $u(t)$ represents an input signal to the electrical power network, such as an excitation,
- $f(t) := U$ represents a possible intrusion signal to be detected, and
- vector $Y(t) := [\{f_i\}, \{P_{m_i}\}]'$ represents measured states of
30 the system, and specifically electrical frequencies f_i of the various generators i , and generated power outputs of the turbine of the subject generator P_{mi} which states are measurable in the electrical power network at each generator,
- 35 - $h(\cdot)$ is a non-linear function representing the nonlinearities of the electrical power network.

The nonlinear function $h(\cdot)$ and the constant matrices B_u , B_d , B_f , C , D_u , D_d and D_f can be obtained by a mapping between coefficients of equations (1), (2), (3) and (5) for each node i on the one hand, to equation (6) on the other hand.

The equation (6) may be rewritten by applying a differential operator p which preferably is $p=d/dt$ into a linear algebraic model of the electrical power network described by

$$H(p)x + L(p)z + F(p)f = 0 \quad \text{equation (7)}$$

while for a non-linear model of the electrical power network a non-linear term $E(x)$ as a function of an unknown signal x may be added to equation (7) such that a nonlinear model of the electrical power network may in general be described by

$$E(x) + H(p)x + L(p)z + F(p)f = 0 \quad \text{equation (8)}$$

The signals x , z , f in the differential operator notation correspond to the signals of the ordinary state space description according to equation (6) as follows:

$$\begin{aligned} x &:= \begin{bmatrix} X - X_e \\ d \end{bmatrix} \\ z &:= \begin{bmatrix} Y \\ u \end{bmatrix} \\ f &:= f \end{aligned}$$

with X_e denoting an equilibrium state of equation (3), e.g. an operating point or set-point. Therefore, in the differential operator notation, x represents typically unknown states, which collectively include not measurable states X of the electrical power network and load disturbances d , also denoted as load deviations or load deviation patterns as unknown external disturbances, while

z collectively represents measurable states Y and known input states u of the electrical power network.

A simple mapping between the ordinary state space description of equation (6) and the description in the differential operator notation according to equation (8) leads to the following correspondences of matrices:

$$E(x) := \begin{bmatrix} h(x) - A(X - X_e) \\ 0 \end{bmatrix} \quad \text{wherein } A := \frac{dh}{dX} \Big|_{X=X_e} \text{ mapping (1.1)}$$

$$H(p) := \begin{bmatrix} -p + A & B_d \\ C & D_d \end{bmatrix} \quad \text{mapping (1.2)}$$

$$L(p) := \begin{bmatrix} 0 & B_u \\ -I & D_u \end{bmatrix} \quad \text{mapping (1.3)}$$

$$F(p) := \begin{bmatrix} B_f \\ D_f \end{bmatrix} \quad \text{mapping (1.4)}$$

Whenever there is no known excitation of the system $u(t)=0$ such that $u:=0$ in the transform domain, B_u and D_u can be set to zero.

In a system without excitation, and assuming a linear system for the time being according to equation (7), the design for a filter for isolating intrusion attacks can be derived as follows:

The filter to be designed shall preferably isolate attacks from other non-attack scenarios, such as, e.g. power generation peaks caused by sudden changes in electrical load. Such filter may be described in the transform domain by a transfer function $N(p)*L(p)$ since the filter will be supplied with signals/states z measured in the electrical power network.

It can further be derived that, when there is no attack i.e. $f=0$, equation (7) reads as

$$H(p)x + L(p)z = 0 \quad \text{equation (7.1)}$$

Multiplying equation (7.1) by $N(p)$ results in

$$H(p)N(p)x = -L(p)N(p)z \quad \text{equation (7.2)}$$

Given that the right hand side of equation (7.2), i.e. $L(p)N(p)z$, represents an output r of the filter $L(p)N(p)$ supplied with the measured signals z , such
 5 filter is desired to return at its output r for any z the value zero since it is assumed that no attack $f=0$ is applied to the electrical power network, such that the output r remains silent, i.e. zero in this case. Hence, the
 10 term on the left hand side of equation (7.2) shall be zero, too, in case of no attack, i.e. $f=0$:

$$N(p)H(p)x = 0 \quad \text{condition (1)}$$

15 In case of an attack, however, $f \neq 0$ in equation (7). A multiplication of equation (7) by the polynomial vector $N(p)$ reads as

$$N(p)H(p)x + N(p)L(p)z + N(p)F(p)f = 0 \quad \text{equation (7.3)}$$

20

wherein, again, the term $N(p)L(p)z$ represents the filter output r , which output r in case of an attack $f \neq 0$ shall not be zero, such that

$$25 \quad r = N(p)L(p)z = N(p)H(p)x + N(p)F(p)f \neq 0 \quad \text{equation (7.4)}$$

This leads to condition

$$N(p)F(p) \neq 0 \quad \text{condition (2)}$$

30

Given that except for the polynomial vector $N(p)$ all the other polynomial matrices $H(p)$, $L(p)$ and $F(p)$ are known, see mappings (1.1) - (1.4), one or more vectors N can be determined by means of solving the algebraic equations for condition (1). A vector $N(p)$ that in
 35 addition fulfils condition (2) contributes to a set of x polynomial vectors

$$N_y(p) := [N_0(p), \dots, N_y(p), \dots, N_{x-1}(p)]$$

that fulfils conditions (1) and (2) wherein
 5 each of these polynomial vectors $N_y(p)$ may be applied for building the filter with the transfer function $N(p) * L(p)$.

Hence, the filter only raises an alarm in its output r when an attack signal $f \neq 0$ is present and isolates other scenarios, i.e. non-attack scenarios, by not
 10 raising an alarm in its output r .

The filter also may be denoted as residual generator. For determining the transfer function of the residual generator the residual generator first is defined as a polynomial matrix, see conditions (1) and (2).
 15 The polynomial matrix may then preferably be translated into a linear programming framework, and as such is converted into a Linear Programming LP optimization problem. Linear programming is known to the skilled person as a technique for the optimization of linear functions dependent on given constraints. For the reason that the
 20 polynomial matrix now is converted into algebraic equations for which coefficients are searched for, the above differential operator p may now be replaced by variable s . After such conversion the vectors and matrices now
 25 read as:

$$\begin{aligned} \bar{N} &:= [N_0 N_1 \dots N_{d_N}] \\ \bar{H} &:= \begin{bmatrix} H_0 \dots & H_{d_H} \dots & 0 & 0 \\ 0 \dots & H_0 \dots & 0 & 0 \\ 0 \dots & \dots & H_{d_H} & \\ 0 \dots & \dots & H_{d_H-1} & H_{d_H} \end{bmatrix} \\ \bar{F} &:= \begin{bmatrix} F_0 \dots & F_{d_F} \dots & 0 & 0 \\ 0 \dots & F_0 \dots & 0 & 0 \\ 0 \dots & \dots & F_{d_F} & \\ 0 \dots & \dots & F_{d_F-1} & F_{d_F} \end{bmatrix} \end{aligned}$$

such that the conditions (1) and (2) may now equivalently be written as

$$\bar{N}\bar{H}=0 \quad \text{condition (1.1)}$$

5

$$\left\| \bar{N}\bar{F} \right\|_{\infty} \geq 1 \quad \text{condition (2.1)}$$

Condition (2.1) refers to the infinite vector norm which means that in vector $\bar{N}\bar{F}$ the absolute value of at least one of the vector elements shall be equal to 1 or shall exceed 1.

10

Conditions (1.1) and (2.1) can be resolved by computational tools.

In the following, the above approach is extended in a preferred embodiment to nonlinear models as is described by equation (8). As can be derived from equation (8), the nonlinearity is represented by term $E(x)$ additive to the linear description of the model according to equation (7). Hence, the linear part of the system can be decoupled from its nonlinear part and can be treated separate according to the above description.

20

Multiplying equation (8) by $N(p)$ and respecting that $N(p)L(p)z$ represents the intrusion detection output r of the filter with filter transfer function $R(p)=N(p)L(p)$ such that:

25

$$\begin{aligned} r &:= R(p)z = N(p)L(p)z = -(N(p)H(p)x + N(p)F(p)f + N(p)E(x)) \\ &= -d^{-1}(p)N(p)(F(p)f + E(x)) \end{aligned} \quad \text{equation (8.1)}$$

wherein $d(p)$ denotes a stable dynamic of sufficient order.

30

Therefore, in one embodiment, a main objective may be to reduce a contribution of the term $E(x)$ in equation (8.1) thereby increasing the residual/filter output sensitivity with respect to an attack/intrusion f .

35

Without loss of generality, a linear part of $E(x)$ may be extracted and it may be assumed that

$$\lim_{x \rightarrow x_e} \frac{\|E(x)\|}{\|x - x_e\|} = 0$$

5

wherein x_e is an equilibrium state of the system, and $\|\cdot\|$ stands for the Euclidean norm of a vector. Therefore, it may be assumed that a contribution of the nonlinear term $E(x)$ may be neglected provided that the system as modelled normally works around an equilibrium state x_e . From a practical perspective this may be a reasonable assumption since in many applications a system dynamic is considerably deviated from a nominal operating point in the presence of an attack signal.

15

Hence, according to this embodiment, the condition (2.1) can slightly be modified into

$$\max_{\bar{N}} \|\bar{N} \bar{F}\|_{\infty} \quad \text{condition (2.2)}$$

20

while condition (1.1) may be transformed into

$$\text{subject to } \begin{cases} \bar{N} \bar{H} = 0 \\ \|\bar{N}\|_{\infty} \leq 1 \end{cases} \text{ collectively condition}$$

(1.2)

25

and includes condition (1.1) and adds another optimization constraint which preferably is for avoiding unbounded solutions. Obviously this other constraint does not loose generality as the filter $R(p)$ in equation (8.1) can be computed up to a scalar. It is also a result that the other constraint in condition (1.2) is indeed an LP constraint in an augmented state space

30

Condition (2.2) means that in case there are multiple solutions $\bar{N}$ found for solving the linear programming framework according to condition (1.1), it is preferred to select that vector $\bar{N}$ as solution that shows

the maximum absolute vector element value amongst all solution vectors N . The maximum absolute vector element denotes the element of a vector that shows the highest absolute value amongst all vector elements of said vector.

5 By doing so, a sensitivity of the filter with respect to attack events is increased, and in particular is maximized, since $\bar{N}\bar{F}$ in condition (2.2) targets at a contribution of the attack signal f to the output r of the filter. Recall that $\bar{N}\bar{F}$ represents the vector contain-
10 ing all nominator coefficients of a transfer function from the attack signal f to output signal r of the filter.

In a different embodiment, it is a sensitivity of the filter towards uncertainties, i.e. for example
15 sudden load deviations in the electrical power network that is addressed rather than the sensitivity of the filter for attack signals being increased. The sensitivity with respect to uncertainties is preferred to be reduced or minimized. Uncertainties may encompass load deviations
20 represented by $d(t)$ in the state space description of equation (6) or included in the differential operator notation x according to equation (8). Load deviation patterns, also denoted as disturbances patterns, may also occur suddenly and may have tremendous impact on the sta-
25 bility of the system.

In an embodiment, a model of the electrical power network which, for example, may be modelled according to the equation (8) may be exposed to load deviation patterns in the absence of attack signals f and in the
30 absence of input signals u . Determined/measured signals/status denoted as z in equation (8) may represent a reaction of the simulated electrical power network to such stimuli in load deviation. These measured signals/statuses z which represent an excitation of the electrical power network model in response to the load deviation
35 stimuli may then be supplied to the filter and the

corresponding intrusion detection output r at the filter may be monitored.

An energy measure dependent on the output $r(t)$ may be taken as an indicator as to which polynomial vector $N(p)$ out of multiple polynomial vectors $N(p)$ as solution to condition (1), (1.1) or (1.2) shall be selected for designing the filter $N(p)*L(p)$.

Translating this approach into conditions for resolving the linear programming frame work according to condition (1.2), the conditions may in this embodiment be set to

$$\begin{aligned}
 & \min_{\tilde{N}} \|\tilde{N} Q \tilde{N}\| && \text{condition (2.3)} \\
 & \text{with} \\
 & Q := \tilde{D} G \tilde{D}^* \\
 & \text{subject to. } \begin{cases} \tilde{N} \tilde{H} = 0 \\ \|\tilde{N} \tilde{F}\|_{\infty} \leq 1 \end{cases} && \text{collectively condition} \\
 & (1.3)
 \end{aligned}$$

This means that in case there are multiple different solutions $N(p)$ found for solving the linear programming framework according to conditions (1.1) it is preferred to select the solution $N(p)$ that shows the minimum scalar value as a result of a matrix multiplication of $\tilde{N} Q \tilde{N}^*$.

In the present embodiment, in contrast to applying constraints to the nonlinear structure of system dynamics constraints are imposed on disturbance signals. It may be assumed that some rough information about disturbance patterns is available i.e. the disturbances may in one example be upfront restricted to a certain family of disturbances. In the present example, it is aimed at controlling a contribution of the nonlinear term $E(x)$ according to equation (8) to the filter output r in the presence of these disturbances. In essence, the filter

may be trained by these disturbances in order to identify the normal behaviour of the system while such disturbances appear.

For this purpose, a certain disturbance pattern t - which also was denoted so far as $d(t)$ or P_{Load} - is assumed to result in signal x . A mapping of the disturbance pattern t into the nonlinearity $E(x)$ shall be given by $t \mapsto E(x(.))$ over a given time interval $[0, T]$. A corresponding approximation may be given by

10

$$e(t) := E(x(t)) \approx \sum_{i=0}^n \beta_i b_i(t) = \beta B(t) \quad \text{with } t \in [0, T] \quad \text{equation (9)}$$

wherein $\beta := [\beta_0 \dots \beta_n]$ is a constant matrix, and $B := [b_0 \dots b_n]$ is a vector of smooth functions, collectively also denoted as basis. For example, $[b_0 \dots b_n]$ may be polynomials of different degree.

Further, it may be assumed that a subspace for the smooth functions is closed under differential operator p . This requirement, for instance, is satisfied for a polynomial or a Fourier basis. The aforementioned assumption may give rise to translate the linear operator p as a matrix operator i.e.

25

$$pB(t) := \frac{d}{dt} B(t) = DB(t) \quad \text{equation (10)}$$

In case $r_e(t) := N(p)e(t)$ defines an error output of the filter $r_e(t)$ owed to the nonlinearities of the system, which represents a contribution of the nonlinear term, in accordance to the approximation in equation (9) and the operator in equation (10), and in view of the projection into the subspace, the error output $r_e(t)$ of the filter can also be approximated by:

30

$$r_e(t) \approx \tilde{N} \tilde{D} B(t) \quad \text{equation (11)}$$

$$\text{with } \tilde{D} := \begin{bmatrix} \beta \\ \beta D \\ \dots \\ \beta D^{d_N} \end{bmatrix}$$

wherein d_N is a degree of the filter. Hence, it is a second order norm L_2 of the error output signal r_e may be formulated as a quadratic function of the filter coefficients $\bar{N}$ as follows:

$$\|r_e\|_{L_2}^2 \approx \bar{N} \tilde{D} G \tilde{D}^T \bar{N} \quad \text{equation (12)}$$

$$\text{with } G_{ij} := \int_0^T b_{i-1} b_{j-1} dt$$

10

wherein where the matrix $\tilde{D}$ is defined as in equation (10). Once a basis B is determined for approximating the disturbance pattern, $\tilde{D}$ is known and preferably is a differentiation matrix owed to the requirement for the basis as formulated in equation (10),

$$\text{and preferably } D = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & n & 0 \end{bmatrix}$$

G is dependent on the basis, too, preferably compensates for scaling of different members $[b_0 \dots b_n]$ of the basis and is a symmetric matrix with dimension $(d_N + 1)$. Note that G may indeed be the Gram matrix

$$G_{ij} = \frac{T^{i+j-1}}{i+j-1} \text{ of the subspace } N \text{ contained in a Hilbert space}$$

endowed with the inner product $\langle f, g \rangle := \int_0^T f g dt$. Hence, condition (2.3) can be resolved for one or more $\bar{N}$.

25

In Figure 1, an electrical power network is introduced according to an embodiment of the present invention. The sample network topology is illustrated wherein a first area A_1 is covered by a first electrical

power network and an adjacent second area A2 is covered by a different electrical power network. Each electrical power network includes multiple generators for generating electrical energy and consumers of the electrical energy.

5 Generators and consumers are represented by dots in each area A1, A2. Power lines represented by lines in Figure 1 are provided between generators and between generators and consumers. Power lines between the two areas A1 and A2 are denoted as tie lines T.

10 In a sample embodiment, each area A1, A2 may be equipped with both primary and secondary frequency control. Let $G = \{i\}_1^g$ denote a set of generator indices, and $A1 = \{i \in G \mid i \text{ in area 1}\}$ and $A2 = \{i \in G \mid i \text{ in area 2}\}$ denote a set of generators that belongs to area A1 and area A2 respectively. Let also $L_{tie} = \{(k, m) \mid k, m\}$ be edges of a tie line and $\{k \in A1, m \in A2\}$ wherein a tie line is a line connecting the two independently controlled areas. Then, a model of the two area power system may be described by the above general equations (1) and (2) for each generator in each area, and by:

$$\dot{P}_{m_{a1}} = \frac{1}{T_{ch,a1}} (P_{m1}^0 + v_{a1} \Delta P_{p_{a1}}^{sat} + \omega_{a1} \Delta P_{agc1}^{sat} - P_{m_{a1}}) \quad \text{equation (3.2)}$$

$$\dot{P}_{m_{a2}} = \frac{1}{T_{ch,a2}} (P_{m1}^0 + v_{a2} \Delta P_{p_{a2}}^{sat} + \omega_{a2} \Delta P_{agc2}^{sat} - P_{m_{a2}}) \quad \text{equation (3.3)}$$

25 Inside each area A1, A2 only some of the generators may be equipped with a primary frequency control. In Figure 2 a part of a network topology is illustrated including five generators A, B, C, D, and E, wherein except for generator E all generators are equipped with a local control, i.e. a primary frequency control AP, BP, CP, DP. Generator E may only be controllable centrally, i.e. by a secondary frequency control ES. On the other hand, only some of the generators may not be controllable by the central control unit, i.e. generators A and C, while the remaining generators B and D are controllable

by the central control unit CC, which is referred to as BS, DS. In reality, operators of these generators, respectively the associate power plants may have contracts that the generation utilities have established with the transmission system operator (TSO) of the area which transmission system operator controls the central control unit. To respect a topology in which not all generators may be equipped with a local control a binary vector v is introduced in equations (3.2) and (3.3). To respect a topology in which not all generators may be centrally controllable a binary vector ω is introduced in equations (3.2) and (3.3).

Such primary frequency control may be activated independently and locally for each generator i with an objective to regulate the frequency by adjusting the generating power as described in the following equation (13):

$$\Delta P_i = -\frac{1}{S_i}(f_i - f_0) \quad \text{equation (13)}$$

In equations (3.2) and (3.2) the secondary frequency (AGC) related control signals represented by ΔP_{agc} may, for the two areas A1, A2, be expressed by:

$$\begin{aligned} \Delta \dot{P}_{agc1} &= \sum_{j \in A1} c_{1j}(f_j - f_0) + \sum_{j \in A1} b_{1j}(P_{mj} - P_{ej}(\delta) - \Delta P_{Loadj}) - \frac{1}{T_{n1}}g_{11}(\delta, f) - C_{p1}g_{12}(\delta, f) \\ &\quad - \frac{K_1}{T_{N1}}(\Delta P_{agc1} - \Delta P_{agc1}^{sat}) \\ \Delta \dot{P}_{agc2} &= \sum_{j \in A2} c_{2j}(f_j - f_0) + \sum_{j \in A2} b_{2j}(P_{mj} - P_{ej}(\delta) - \Delta P_{Loadj}) - \frac{1}{T_{n2}}g_{21}(\delta, f) - C_{p2}g_{22}(\delta, f) \\ &\quad - \frac{K_2}{T_{N2}}(\Delta P_{agc2} - \Delta P_{agc2}^{sat}) \end{aligned}$$

collectively equation (14)

Constants c and b are based on the weighted frequency measurement that the central control unit gets as an input. T_n , C_p and K are design constants for its control loop. In addition, saturation limits are applied as follows:

$$\Delta P_{p_i}^{sat} = \begin{cases} \Delta P_{p_i}^{\min} & \text{if } \Delta P_{p_i} \leq \Delta P_{p_i}^{\min} \\ \Delta P_{p_i} & \text{if } \Delta P_{p_i}^{\min} < \Delta P_{p_i} \leq \Delta P_{p_i}^{\max} \\ \Delta P_{p_i}^{\max} & \text{if } \Delta P_{p_i} \geq \Delta P_{p_i}^{\max} \end{cases}$$

$$\Delta P_{agc_i}^{sat} = \begin{cases} \Delta P_{agc_i}^{\min} & \text{if } \Delta P_{agc_i} \leq \Delta P_{agc_i}^{\min} \\ \Delta P_{agc_i} & \text{if } \Delta P_{agc_i}^{\min} < \Delta P_{agc_i} \leq \Delta P_{agc_i}^{\max} \\ \Delta P_{agc_i}^{\max} & \text{if } \Delta P_{agc_i} \geq \Delta P_{agc_i}^{\max} \end{cases}$$

5 Again, the network topology is reflected by:

$$P_{ei} = \sum_{j=1}^g |E_{Gi}| |E_{Gj}| (B_{ij} \sin(\delta_i - \delta_j) + G_{ij} \cos(\delta_i - \delta_j))$$

$$g_{11}(\delta) = \Delta P_{T_{12}} = \sum_{(i,j) \in L_{tie}} P_{ij} - P_{t_{12}}^0 \quad g_{22}(\delta) = \Delta P_{T_{21}} = \sum_{(i,j) \in L_{tie}} P_{ji} - P_{t_{21}}^0$$

10 with

$$P_{ij} = |V_i| |V_j| (G_{ij} \cos(\delta_i - \delta_j) + B_{ij} \sin(\delta_i - \delta_j))$$

$$g_{12}(\delta) = \Delta P_{T_{12}} \cdot$$

$$g_{21}(\delta, f) = \Delta P_{T_{12}}$$

15 The central control CC unit may utilize frequency measurements from its control area and power flow measurements on the tie lines so as to bring their values back to their operating set-points, i.e. f_0 for the frequency, and ΔP_{Tij}^0 for the total active power exchange. This
 20 may be the closed-loop control implemented in the central control unit. The control signal/s to the actuators may be a centralized control signal that is distributed to some generators of the set of generators inside its control area.

25 Based on the above set of differential equations the electrical power network model can be enhanced to adding an undesired intrusion signal. Preferably, such intrusion signal is targeted at the central control unit including its infrastructure and associated informational
 30 network. In this sense, such intrusion signal U may be additive to the central control signal for centrally controlling the frequency of the generators participating.

As a result, in case the attack occurs in area A1 which may result in a modification of equation (3.2):

$$\dot{P}_{m_{a1}} = \frac{1}{T_{ch,a1}} (P_{m1}^0 + v_{a1} \Delta P_{p_{a1}}^{sat} + \omega_{a1} (\Delta P_{agc1}^{sat} + U) - P_{m_{a1}}) \quad \text{equation (3.3)}$$

5

The above model including the intrusion signal U may be rewritten in a more compact form in the following ordinary state space description:

$$\begin{aligned} \dot{X}(t) &= h(X(t)) + B_d d(t) + B_f f(t) \\ Y(t) &= CX(t) \end{aligned} \quad \text{collectively equation (6.1)}$$

10

see equation (6), however, with no excitation $u(t)=0$

Again $X := [\{\delta_i\}_1^g, \{f_i\}_1^g, \{P_{m,a1}\}_{a1 \in A1}, \{P_{m,a2}\}_{a1 \in A2}, \Delta P_{agc1}, \Delta P_{agc2}]$ represents internal states of the electrical power network including turbine rotation angles δ_i and electrical frequencies f_i of the various generators i ,

15

$d := \{\Delta P_{Load}(t)\}_1^g$ represents the unknown load disturbance,

20

$f(t) := U$, represents the intrusion signal to be detected, and

$Y := [\{f_i\}_1^g, \{P_{m,a1}\}_{a1 \in A1}, \{P_{m,a2}\}_{a1 \in A1}]$ represents measured states of the system.

25

Such ordinary state space description again can be rewritten by using a differential operator p as is explained with respect to the general embodiment.

In a sample embodiment of a simulated network including two areas as introduced above, the electrical network of the first area was exposed to a cyber attack on the AGC / central control unit, in the presence of load deviations ΔP_{Load} in all nodes.

30

The filter designed according to the above teaching, has proven to be insensitive to a normal operation of the network including load deviations ΔP_{Load} . On the other hand, the filter proves to be highly sensitive to any undesirable intrusion U in the AGC command. That is, as long as available measurements are consistent with

35

the normal settings of the power network and small deviations are normally caused due to load deviations, the filter does not show anything on the monitor between t_0 and t_1 , i.e. the intrusion detection signal $r(t)$ as shown in FIG. 3a) remains silent, i.e. ~ 0 . However, once an intrusion signal U is injected to the AGC, the filter alarms within a very short time, see at t_1 in FIG. 3b).

In Figure 4, a block diagram of a filter 1 according to an embodiment of the present invention is shown which filter 1 is exposed to a signal status vector $Y(t)$, and provides at its output the intrusion detection signal $r(t)$:

Hence, a tractable approach to design a filter for nonlinear systems is introduced.

For details on the AGC modelling it is referred to P. M. Esfahani et al, "Cyber attack in a two-area power system: Impact identification using reachability", in American Control Conference, 2010, pp. 962 - 967 which is incorporated by reference.

Claims

1. Apparatus for detecting an intrusion in an electric power network, comprising

5 a receiver for receiving a vector $(Y(t))$ of status signals measured from the electric power network,

a filter (1) for providing an intrusion detection signal $(r(t))$ in response to applying the received status signal vector $(Y(t))$ to the filter (1),

10 a transfer function of which filter (1) is given by $N(p)*L(p)$ with p representing a differential operator, wherein

- $L(p)$ is a polynomial matrix in the differential operator p to be applied to the status signal vector $(Y(t))$, and

15 - $N(p)$ is a polynomial vector in the differential operator p representing a solution to equation $N(p)*H(p)=0$ wherein $H(p)$ is a polynomial matrix in the differential operator p to be applied to internal status signals $(x(t))$ of and/or to a load deviation pattern $(d(t))$ applied to a model of the electrical power network.

2. Apparatus according to claim 1,

25 which apparatus is designed for detecting an intrusion in a common computational infrastructure for adjusting a power output at different generators within a given area of the electrical power network.

3. Apparatus according to claim 1 or claim 2,

30 wherein in case of multiple polynomial vectors $N(p)$ solving the equation, the polynomial vector $N(p)$ selected for contributing to the filter transfer function is the polynomial vector $N(p)$ that has a minimum scalar value as a result of a matrix multiplication of $\bar{N}Q\bar{N}$,

35 with Q being a matrix representing an accumulated impact of different simulated load deviation patterns (ΔP_{Load}) .

4. Apparatus according to claim 3,

wherein

$$Q := \tilde{D} G \tilde{D}^T$$

$$\tilde{D} := \begin{bmatrix} \beta \\ \beta D \\ \vdots \\ \beta D^{d_N} \end{bmatrix}$$

5 $\beta := [\beta_0 \dots \beta_n]$ is a constant matrix

D is a differentiation matrix,

$$\text{and preferably } D = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & n & 0 \end{bmatrix}$$

G is a symmetric matrix, preferably with elements $G_{ij} := \int_0^T b_{i-1} b_{j-1} dt$, and preferably is a Gram matrix with

10 elements $G_{ij} = \frac{T^{i+j-1}}{i+j-1}$

$B := [b_0 \dots b_n]$ is a vector of smooth functions, such that $\beta B(t)$ represents an approximation of a disturbance pattern applied to the electrical power network over a given time interval $[0, T]$.

15 5. Apparatus according to any one of the preceding claims,

wherein in case of multiple polynomial vectors $N(p)$ solving the equation, the polynomial vector $N(p)$ selected for contributing to the filter transfer function is the polynomial vector $N(p)$ that shows a lowest energy in the corresponding intrusion detection signal $r(t)$ of a filter based on said polynomial vector $N(p)$ when being supplied with the status signal vector $(Y(t))$ determined in the modelled electrical power network when being exposed to a simulated load deviation pattern (ΔP_{Load}) .

20

25

6. Apparatus according to any one of the preceding claims,

wherein the polynomial vector $N(p)$ selected for contributing to the filter transfer function is the

30

polynomial vector $N(p)$ that shows a lowest energy in a combination of corresponding intrusion detection signals $r(t)$ of a filter based on said polynomial vector $N(p)$ when being supplied with the status signal vectors $(Y(t))$ determined in the modelled electrical power network when being exposed to different simulated load deviation patterns (ΔP_{Load}) .

7. Apparatus according to claim 5 or claim 6, wherein the lowest energy is represented by a lowest Euclidian norm $L2$ of $\|r(t)\|_{L2}^2$ energy in the corresponding intrusion detection signal $r(t)$.

8. Electric power network, comprising generators for generating electrical power, power lines for distributing the generated electrical power, sensors for measuring status signals in the electric power network, a common computational infrastructure for adjusting a power output at different generators, and an apparatus according to any one of the preceding claims.

9. Method for detecting an intrusion in an electric power network, comprising measuring status signals in the electric power network,

applying a vector $(Y(t))$ of the status signals measured to a filter (1), a transfer function of which filter (1) is given by $N(p)*L(p)$ with p representing a differential operator, wherein

- $L(p)$ is a polynomial matrix in the differential operator p to be applied to the status signal vector $(Y(t))$, and

- $N(p)$ is a polynomial vector in the differential operator p and represents a solution to equation $N(p)*H(p)=0$ wherein $H(p)$ is a polynomial matrix in the differential operator p to be applied to internal status sig-

nals ($x(t)$) and/or to a load deviation pattern ($d(t)$) applied to a model of the electric power network, and

the filter (1) supplying an intrusion detection signal ($r(t)$) in response to applying the received status signal vector ($Y(t)$) to the filter (1).

10. Method according to claim 9,

wherein the intrusion to be detected is an intrusion in a common computational infrastructure for adjusting a power output at different generators within a given area of the electrical power network.

11. Method according to claim 9 or claim 10,

wherein the model of the electrical power network is exposed to a simulated load deviation pattern (ΔP_{Load}),

wherein a vector of status signals ($Y(t)$) is determined during applying the simulated load deviation pattern (ΔP_{Load}) to the model,

wherein the measured status signal vector $Y(t)$ is supplied to different filters, each of the different filters being designed based on a different one of polynomial vectors $N(p)$ representing a solution to the equation,

wherein the polynomial vector $N(p)$ for contributing to the filter transfer function is selected out of the multiple polynomial vectors $N(p)$ subject to the corresponding intrusion detection signals $r(t)$ of the different filters.

12. Method according to claim 11,

wherein in case of multiple polynomial vectors $N(p)$ solving the equation, the polynomial vector $N(p)$ selected for contributing to the filter transfer function is the polynomial vector $N(p)$ which corresponding filter shows the lowest energy in its intrusion detection signal $r(t)$ upon supply of the determined status signal vector ($Y(t)$), and

in particular wherein the lowest energy in its intrusion detection signal $r(t)$ is determined by a lowest Euclidian norm $L2$ of $\|r\|_{L2}^2$ energy in its intrusion detection signal $r(t)$.

5 13. Method according to any one of the preceding claims 9 to 12,

 wherein the model of the electrical power network is exposed to different simulated load deviation patterns (ΔP_{Load}),

10 wherein a vector of status signals ($Y(t)$) is determined during applying each simulated load deviation patterns (ΔP_{Load}) to the model,

 wherein the measured status signal vectors $Y(t)$ are supplied to different filters, each of the different filters being designed based on a different combination of polynomial vectors $N(p)$ representing a solution to the equation, which combination includes one solution to the equation per simulated load deviation pattern, and

15 wherein the polynomial vector $N(p)$ for contributing to the filter transfer function is determined by the filter with a minimum in energy in the corresponding intrusion detection signal $r(t)$ amongst the different filters.

20 14. Method according to any one of the preceding claims 9 to 13,

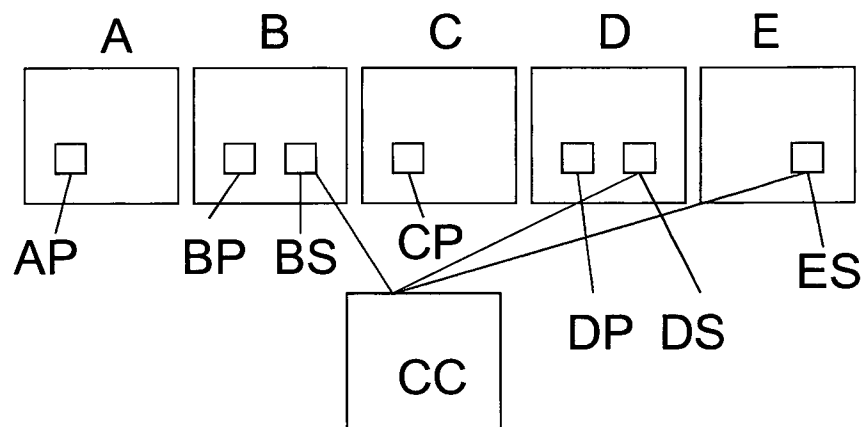
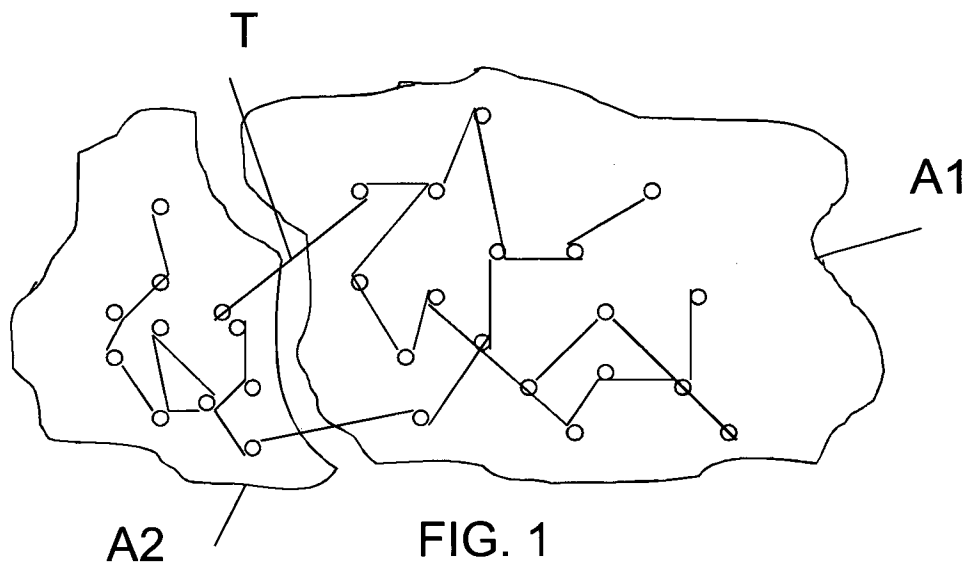
 wherein for determining the polynomial vector $N(p)$ for contributing to the filter transfer function the filter is trained by applying different simulated load deviation patterns to the filter.

25 15. Computer program element comprising computer program code means for representing a filter as used in the apparatus of any one of the claims 1 to 7.

30 16. Computer program element comprising computer program code means for selecting the polynomial vector $N(p)$ according to any one of the previous claims 9 to 13 when being executed on a processing unit.

35

1/2



2/2

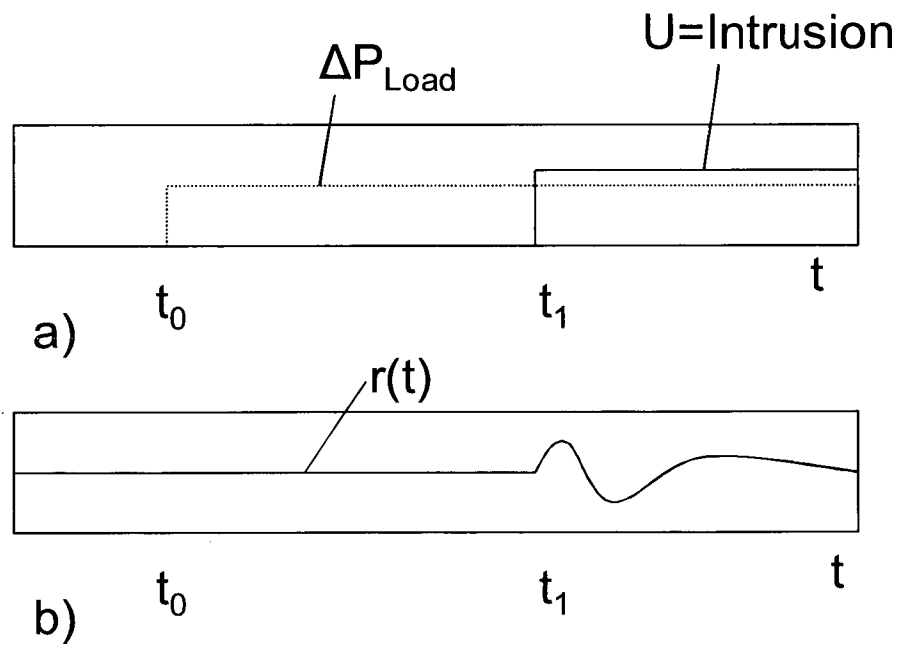


FIG. 3

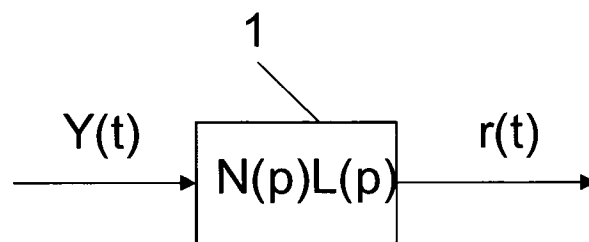


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/002162

A. CLASSIFICATION OF SUBJECT MATTER

INV. G05B13/04 G06F21/55 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G05B G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	HIDEAKI HASHIMOTO ET AL: "Distributed cyber attack detection for power network systems", DECISION AND CONTROL AND EUROPEAN CONTROL CONFERENCE (CDC-ECC), 2011 50TH IEEE CONFERENCE ON, IEEE, 12 December 2011 (2011-12-12), pages 5820-5824, XP032123381, DOI: 10.1109/CDC.2011.6161536 ISBN: 978-1-61284-800-6 Abstract; equations (15), (16); section 5.1; figure 3.1 ----- -/--	1-3, 5-12,15, 16



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

20 August 2013

Date of mailing of the international search report

29/08/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Tchegho Kamdem, A

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2013/002162

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FRANK P M: "FAULT DIAGNOSIS IN DYNAMIC SYSTEMS USING ANALYTICAL AND KNOWLEDGE-BASED REDUNDANCY-A SURVEY AND SOME NEW RESULTS", AUTOMATICA, PERGAMON PRESS LTD., OXFORD, GB, vol. 26, no. 3, 1 May 1990 (1990-05-01), pages 459-474, XP008001193, ISSN: 0005-1088, DOI: 10.1016/0005-1098(90)90018-D	1-3, 5-12,15, 16
A	page 460, equations (1), (2); section 3.1; page 466; sections 5.3, 5.4, 5.5; figures 1-3	4,13,14
Y	----- SIMEU E ET AL: "Automatic design of optimal concurrent fault detector for linear analog systems", FAULT-TOLERANT COMPUTING, 1999. DIGEST OF PAPERS. TWENTY-NINTH ANNUAL INTERNATIONAL SYMPOSIUM ON MADISON, WI, USA 15-18 JUNE 1999, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 15 June 1999 (1999-06-15), pages 184-191, XP010343209, DOI: 10.1109/FTCS.1999.781049 ISBN: 978-0-7695-0213-7	1-3, 5-12,15, 16
A	equations (1), (2); section 3.1; figure 1 -----	4,13,14