REPORT

COST STSM Reference Number: COST-STSM-IC1404-35588

Period: 2016-11-07 to 2016-12-06

COST Action: IC1404

STSM Applicant: Dr Krzysztof Michalak, Wroclaw University of Economics, Wrocław (PL), krzysztof.michalak@ue.wroc.pl

STSM Topic: Modelling domain-specific knowledge for optimizing threat prevention in multiplex networks

Host: Yamir Moreno, Institute for Biocomputation and Physics of Complex Systems (BIFI), Universidad de Zaragoza, Zaragoza (ES), yamir.moreno@gmail.com

1. Initial purpose of the visit

The STSM was intended for **starting a cooperation based on fields of research represented by the Host, the Applicant and the IC1404 participants** that can be brought together in order to improve threat-prevention approaches in complex networks.

The research objectives of the mission were:

- **RO1:** To **define modelling standards** for representing complex network structure including different types of relationships, multiple network layers and different types of entities and their characteristics **important from the point of view of threat prevention**.

- **RO2:** To elaborate **mathematical models of the spreading of threats in multiplex networks** described using modelling standards resulting from RO1. The realization of this objective involved design and implementation of simulation methods as well as theoretical study of the dynamics of the studied phenomena.

- **RO3:** To adapt one **metaheuristic optimization method** to using representations elaborated when realizing RO1 and understanding of the problem achieved when realizing RO2.

2. Description of the work carried out during the STSM

During the STSM a cooperation has been established between the Host (the BIFI team), the Applicant and the IC1404 participants. The work focused on **problems that concern protection against a threat spreading in a multilayer network**. In the context of CPSs a multilayer network can, for example, be **a network of several different utilities in a smart city** (power grid, telecommunications network, etc.) or **a network of interconnected services or production facilities**. The threat can be a computer virus, a technical or economical failure, delivery delay, etc. The spreading of the threat can be limited by protecting nodes of the network or links that connect them and **an optimization algorithm is assigned a task of finding cost-effective ways of preventing the threat from spreading**.

From the research on complex systems (multilayer networks among others) it is known that **certain parameters of the network**, such as failure thresholds, probability of the spreading of the threat or the strength of the coupling between layers **significantly influence the behaviour of the system**. For example, it is not uncommon that with a small change of, let's say, the probability of the spreading of the threat the system switches from easy to protect to very unstable and prone to failures. Such phenomena are known as **phase transitions**. Another studied phenomenon are occurrences of **catastrophic failures**, that is situations in which an initially small number of failed nodes grow rapidly and leads to the malfunctioning of all (or most of) the elements of the network.

The work performed jointly by the Host and the Applicant focused on **identifying phenomena occurring in multilayer networks (such as phase transitions and catastrophic failures) and their influence on optimization problems**. The BIFI team started investigating methods for theoretical understanding of the spreading of a threat influenced by threat-preventing solutions found by an optimization algorithm. The work performed by the Applicant focused on experimental studies of various scenarios of threat prevention optimization in multilayer networks.

In parallel, **the cooperation between the Applicant and the participants of the IC1404 action has been established**. The focus of this area of work was to determine applications in the area of Cyber Physical Systems which have a multilayer network structure (such as multilayer smart city infrastructure or complex service-oriented architectures). Resulting from these studies, **a model was proposed which represents a multilayer CPS** taking into account classes of objects, their attributes and behaviour that are important from the point of view of **understanding the behaviour of the system as a complex network and for the optimization of threat-prevention actions**.

3. Description of the main results obtained

This section **summarizes the results obtained during the STSM**. A more detailed description of the results is presented in Annex 1 later in this document.

Based on the experience of the Applicant and the BIFI team, as well as a literature study, **five optimization scenarios were defined which are applicable to multilayer networked CPSs** and in which phenomena related to complex network structures can be observed. The optimization scenarios (described in more detail in Annex 1, section 2) were:

- S1: The classical Firefighter Problem (FFP) in which a limited number of nodes N_f can be protected in each time step and the goal is to find the best sequence in which to protect nodes (maximizing the number of nodes saved).
- S2: A multiobjective optimization scenario in which a trade-off is sought between number of protected and saved nodes.
- S3: Optimization focused on decreasing the probabilities of the spreading of the threat between network nodes.
- S4: Optimization focused on increasing resilience to the threat (failure thresholds) of nodes in the network.
- S5: Increasing the delay before failure and decreasing recovery time in networks in which nodes can recover from failures.

For selected optimization scenarios metaheuristic **optimization methods were elaborated and implemented** (thus **realizing the research objective RO3**). In the experiments **the following phenomena related to complex network structures were observed** (see Annex 1, section 3 for details):

1. In the optimization scenario S2 based on a two-layer network an abrupt increase in optimization problem difficulty was observed when probability of the spreading of the threat between layers P_{couple} changed from 0 to a non-zero (positive) value.
2. In the optimization scenario S1 a similar change in the quality of solutions has been observed around $P_{\text{couple}} = 0.0001$ when the dependency between the number of nodes protected in each time step N_f and the best number of saved nodes found by the optimization algorithm changed from a linear to a nonlinear one.
3. An abrupt change in the severity of cascading failures was observed in the model proposed by Burkholz et al. [BLGS15] between the values of the coupling strength parameter $\delta_{10} = 0.4$ and $\delta_{10} = 0.5$ (at which catastrophic failure is likely to occur).

In addition to the experimental work summarized above, a literature study was performed which, among others, suggests that in time-delayed networks the combination of multilayer structure and time-delayed propagation of the states can lead to a very complex dynamics [GKZJ16, SGJK15].

In parallel, **we sought real-life examples of CPSs which have a multilayer network architecture and thus can be expected to experience the phenomena related to complex network structures** described above. With the help of the IC1404 action participants the following scenarios were identified:

1. Service based-systems oriented on service outsourcing [ENKP15] in which it is important to limit the effects of failures of individual services as well as prevent catastrophic failures.
2. Process networks in which, for example, inventory planning can be optimized [GAWG16] thus lessening the effects of delivery delays.

3. Virtual enterprises [NNMMM16] in which contract realization can be endangered by failures of peers in a collaboration networks to deliver required products or services.
4. Infrastructure networks that are dependent on each other such as power grid and telecommunications [SW08], power grid and water supply network [DHW15]. Such infrastructure systems can get very complex. For example in the paper [RBJF15] a hierarchy of 31 networks is mentioned (6 air route networks, 2 energy networks, 13 rail networks, 5 road networks, 4 river networks and 1 communication network).

Based on the previously mentioned results **a model was proposed which represents a multilayer CPS** taking into account classes of objects, their attributes and behaviour that are important from the point of view of understanding the behaviour of the system as a complex network and for the optimization of threat-prevention actions (thus **realizing the research objective RO1**). This model is described in Annex 1, section 4. To facilitate collaboration on applying optimization methods in the context of multilayer CPSs some **examples were prepared** (see Annex 1, section 5) showing how to use the proposed model to represent a multilayer system in various scenarios.

In order to **realize the research objective RO2**, a work was started with the BIFI team on mathematical modelling of multilayer networks discussed above currently focusing on discovering at what values of parameters (probabilities of spreading, couple strength, etc.) abrupt changes of the behaviour of the system can be expected.

4. Future collaboration with the host institution (if applicable)

At this point **two areas of collaboration were identified**. One is the development of mathematical models to help understand the behaviour of complex network systems with the intent to improve optimization methods. The other area is the collaboration with IC1404 participants on applications of the elaborated methods to networked CPSs, most likely in scenarios described in the previous section. This area of work includes solving real-life cases as well as further development of the proposed model and adaptation of optimization methods to the updated model.

5. Foreseen publications/articles and other contributions

The current work done in collaboration with the BIFI team and the IC1404 participants is expected to result in publications on improved optimization methods, models representing real-life CPSs cases as complex network systems and applications of optimization methods to threat-prevention in these CPSs.

Annex 1 – Results

1. Overview

The research carried out during the STSM focused on a scenario in which a CPS can be represented as a multilayer network [LMG15]. As shown in Fig. 1. such a system consists of two or more networks (in which connected nodes interact) with a coupling between the layers. A network structured in such a manner is easier to describe theoretically than a network with multiple connections of mixed types which allows, for example, drawing conclusions about the dynamics on the entire network by studying (a much simpler) network representing connections between layers each taken as a whole [SCM14].

There are also numerous real-life examples of such networks, such as power grid and telecommunications [SW08], power grid and water supply network [DHW15]. In the paper [RBJF15] a hierarchy of 31 networks is mentioned (6 air route networks, 2 energy networks, 13 rail networks, 5 road networks, 4 river networks and 1 communication network).

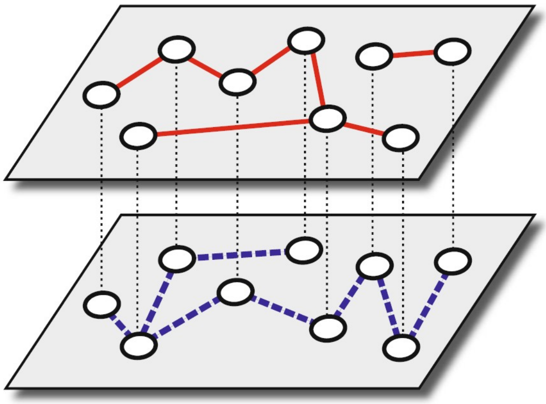

Fig. 1. An ex ample of a multilayer network [LMG15]. Nodes in each layer are linked, and thus may interact (red and blue edges). There is also coupling between layers (thin black dashed lines).

In the case of threat containment in such systems we assume that a threat is spreading in one or more layers which may also affect other layers due to the coupling between them. This threat can be a malfunction, a disease, a financial problem (e.g. a bankruptcy), etc.

In the research described below it was assumed that we are interested in preventing the threat from spreading in the network. In the literature various actions are mentioned that can be taken to improve the resilience of the system. For example the paper [BD15] mentions increasing the capacity of selected links within layers, reducing the interdependencies between layers and increasing the capacity of the entire network. In the Firefighter Problem FFP [H95] it is assumed that the threat spreads in discrete time steps and in each time step it is possible to protect a limited number of nodes N_f. Depending on the problem formulation the goal is to protect the maximum number of nodes (in the original version of the problem) or to maximize multiple objectives calculated using several different values with which the worth of the nodes in determined [M14].

2. Optimization Scenarios

The following scenarios were identified as interesting from the point of view of optimization research:

S1: Classical Firefighter Problem (FFP)

Assuming that a given number of nodes N_f can be protected in each time step, we are interested in determining which nodes to protect (and at what time step) to save as many nodes as possible. This optimization problem can be studied in a deterministic and non-deterministic variants depending on if the probability of spreading of the threat to adjacent nodes is $P_{\text{spread}} = 1$ (deterministic) or $P_{\text{spread}} < 1$ (non-deterministic).

S2: Trade-off between number of protected and saved nodes

In this scenario we assume that we can protect as many nodes as we want, but each protected node incurs a given cost (for example a unit cost, that is, each protected node costs 1). We are interested in minimizing the cost of protection and maximizing the number of saved nodes. Similarly as in the previous scenario the problem can be deterministic ($P_{\text{spread}} = 1$) or non-deteministic ($P_{\text{spread}} < 1$).

S3: Probabilities

In every model which involves non-deterministic spreading of the threat, we can assume that the probability of the spreading of the threat can be decreased at a certain cost. The optimization problem is then to minimize the losses while also minimizing the costs of making the spreading of the threat less probable.

S4: Thresholds

The model described by Burkholz et al. [BLGS15] describes spreading of failures in a two-layer network in which a node can withstand the damaging influence of the failed neighbours up to a certain threshold. An easily seen target for optimization in this model is the height of the thresholds. In the economic setting described in the aforementioned paper, the interpretation is that companies can use various precautions to protect themselves, but, obviously, this incurs costs. This scenario may concern traditional companies as well as virtual enterprises [NNMMM16].

S5: Increasing the delay before failure, decreasing recovery time

In a network in which nodes can resist the damaging influence from other nodes for a certain time we can assume that this capability can be increased by investing some resources (e.g. money) in selected nodes. An example of this approach can be the optimization of inventory in process networks [GAWG16]. Increasing inventory levels incurs costs, but protects, to a certain extent, from suppliers failing to provide needed materials or components. Thus, the overall systemic risk can be reduced at a certain cost. Similar issues arise in modular production environment [JBW08] where delays or failures in one component influence the others. Another area of applications could be virtual enterprises [NNMMM16]. In scenarios where nodes recover from failures the recovery time can be shortened, also at a cost.

3. Phenomena in Multilayer Networks

During the STSM several phenomena were studied that appear in multilayer networks and influence the quality of solutions obtained when optimizing resource allocation in the threat containment scenarios. One of the tasks that were undertaken in the STSM was **to define common elements of the multilayer network description that can be used in modelling of a networked CPS and used for optimizing the system in order to increase its resilience to threats spreading in the multilayer network**. The following points summarize the phenomena that were identified.

3.1. Influence of Coupling Strength

Keeping the characteristic of each layer constant (the type of graph, parameters like density, threat spreading probability, etc.) it is interesting to see how the solutions of optimization problems change with the change of the strength of the coupling between layers. This strength can be defined in various ways, for example we can set the probability of the spreading of the threat between layers $P_{\text{couple}} \in [0, 1]$. With this scenario in mind two series of experiments were performed.

Quality of the solutions in multiobjective optimization

In this experiment the optimization was performed using the NSGA-II algorithm [DPAM02] in the optimization scenario S2: minimizing the number of nodes requiring protection and maximizing the number of nodes saved at the end of the simulation. Experiments were performed for different values of the probability of the spreading of the threat between layers P_{couple} and the probability of the spreading of the threat within each layer $P_{\text{spread}} = 0.5$.

Quality of the solutions in multiobjective optimization was measured by calculating the hypervolume measure [ZTLF02] also known as the size of the objective space covered [ZT98] for a Pareto front of solutions generated by the optimization algorithm. For a given set of solutions P the hypervolume is the Lebesgue measure (area in R^2, volume in R^3, and the generalization of these concepts in R^m for $m > 3$) of the portion of objective space that is dominated by solutions in P collectively:

$$HV(P) = L\left(\bigcup_{x \in P} [f_1(x), r_1] \times \cdots \times [f_m(x), r_m]\right),$$

where:

m - the dimensionality of the objective space,
$f_i(\cdot)$, $i = 1, \ldots m$ - the objective functions,
$r = (r_1, \ldots, r_m)$ - a reference point,
$L(\cdot)$ - the Lebesgue measure on R^m.

The NSGA-II algorithm works iteratively, improving the solutions in consecutive generations. In Fig. 2 the quality of the solutions found by the optimization algorithm is shown. Each line represents the results obtained for a different value of the P_{couple} parameter (the probability of spreading of the threat from one network layer to another).

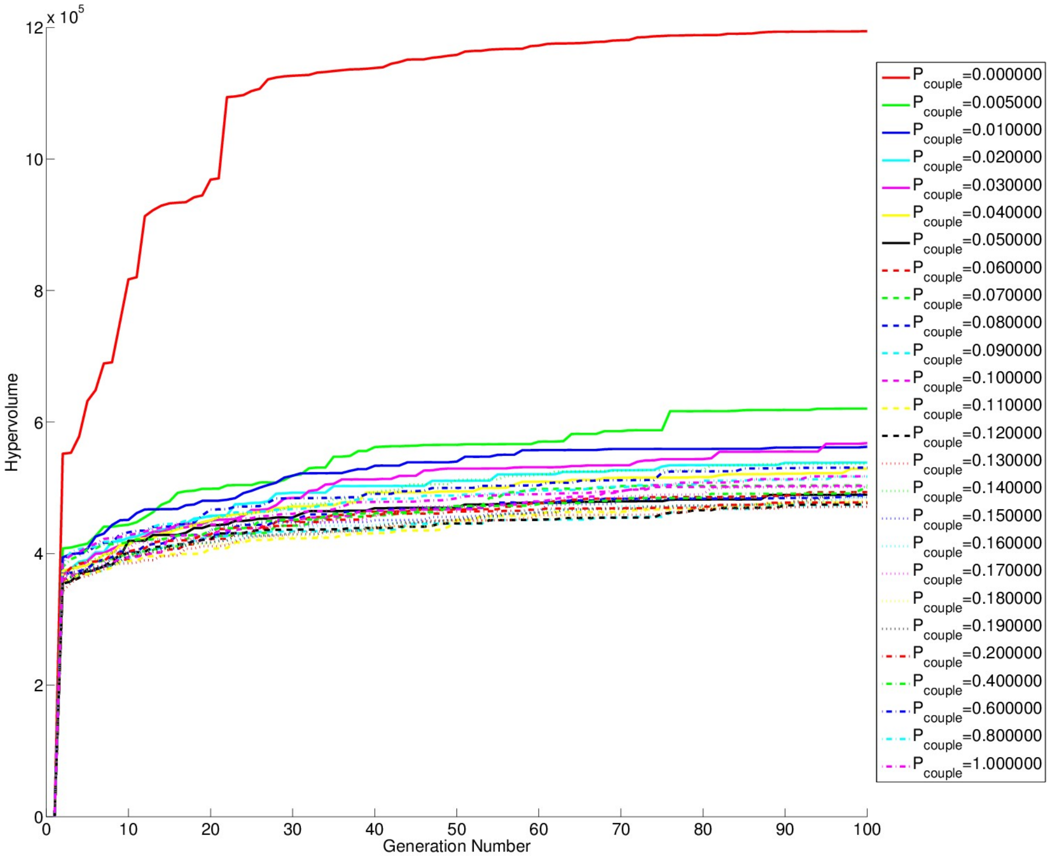

Fig. 2. The quality of the solutions found by the optimization algorithm depending on the value of the P_{couple} parameter.

Clearly, there is a difference between all scenarios in which $P_{\text{couple}} > 0$ and the case in which $P_{\text{couple}} = 0$. Even for the values as small as $P_{\text{couple}} = 0.005$ the optimization problem is much harder than when $P_{\text{couple}} = 0$ as evidenced by much lower hypervolume values. Experiments for $P_{\text{couple}} \in (0, 0.005)$ are currently ongoing with the aim of discovering what is the difficulty of the optimization problem between these values. Because of long running time of the simulations for small values of P_{couple} the experiments, have not yet been finished as of the time of the writing of this document.

Quality of the solutions in single-objective constrained optimization

In another round of experiments the optimization was performed according to scenario S1, that is, with a preset value N_f of nodes that can be protected in each time step and the goal of maximizing the number of the nodes saved from the threat at the end of the simulation. These experiments were performed with $N_f = 1, ..., 15$ and the probability of the spreading of the threat within each layer $P_{spread} = 0.5$.

In Fig. 3 the number of nodes that were saved in the best solution found versus the number of nodes requiring protection is plotted. Each line represents the results obtained for a different value of the P_{couple} parameter (the probability of spreading of the threat from one network layer to another). Obviously, with the increasing value of the P_{couple} parameter the problem becomes more difficult. However, also the characteristics of the relationship between the number of the protected nodes and the nodes that are saved from the threat changes. For larger values of the P_{couple} parameter the relationship is approximately linear, while for smaller values of this parameter it is easy to save many nodes initially, but increasing the number of saved nodes requires a large increase of the parameter N_f.

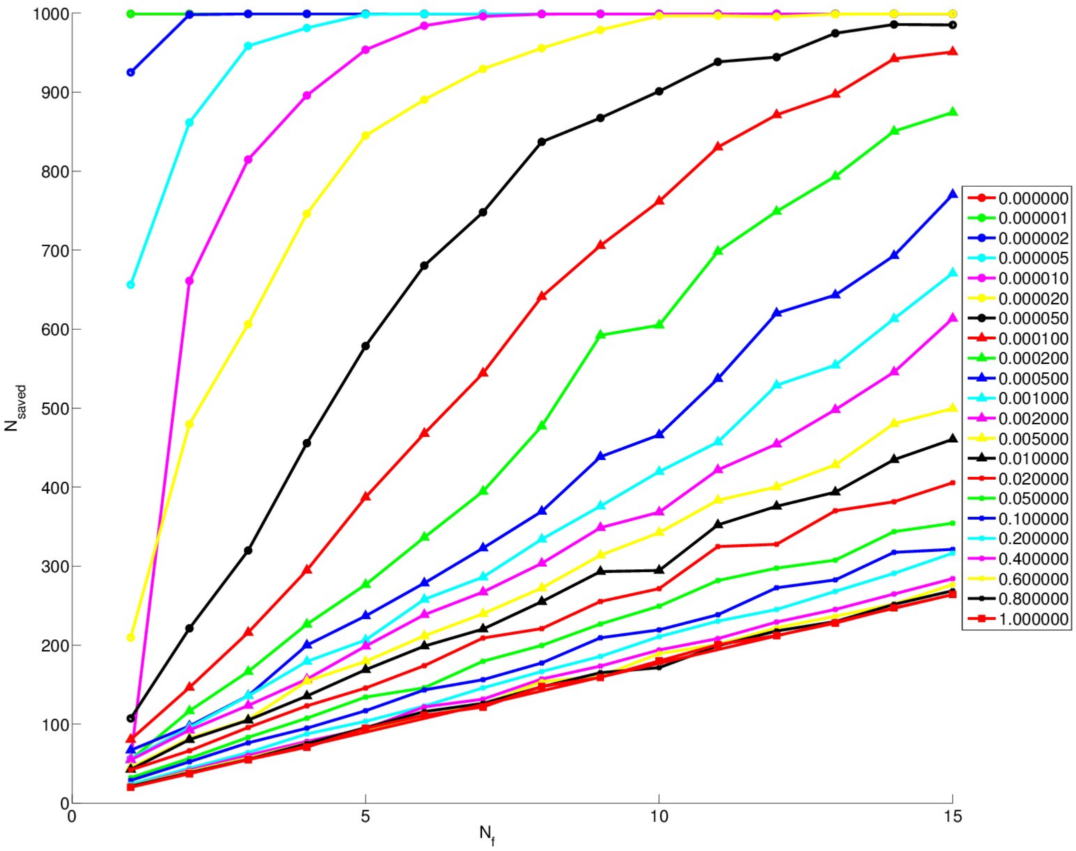

Fig. 3. The number of nodes that were saved in the best solution found versus the number of nodes requiring protection depending on the value of the P_{couple} parameter.

Conclusions

From this set of experiments it can be seen that the strength of the coupling between network layers (here represented as the probability of the spreading of the threat P_{couple}) has a significant effect on the quality of solutions of optimization problems related to containment of threats in a multilayer network.

3.2. Cascading failures

Cascading failures are a phenomenon that is well known in the case of power grids [SSGH14] as well as hierarchical infrastructure networks [DHW15]. A cascading failure occurs when interactions between nodes in the network cause many more nodes to fail than the ones initially malfunctioning. The severity of the phenomenon depends on the strength of the interactions in the network. For example in the economic model proposed by Burkholz et al. [BLGS15] the nodes form two layers, each node has a threshold value assigned which determines how resistant it is to failure, and there is an asymmetric coupling between the layers. That is, there is a coupling with strength $\delta_{01} = 1.0$ from one layer to the other and a coupling with a value of δ_{10} in the other direction (these parameters describe by how much the failure in one layer overloads the corresponding node in the other layer).

The coupling parameter δ_{10} has an important effect, because the characteristics of the spreading of failures in the network changes fundamentally depending on the value of the parameter δ_{10}. For example in experiments performed on a graph with $N = 1000$ nodes and threshold values drawn uniformly from [0, 1] it could be observed that there is a change in the behaviour of the network between the values of $\delta_{10} = 0.4$ and $\delta_{10} = 0.5$. This is visible in Fig. 4 and Fig. 5. which show how the number of nodes that fail after the cascading failure stops spreading changes with the number of nodes that are in the failed state at the beginning of the simulation (for $\delta_{10} = 0.4$ and $\delta_{10} = 0.5$).

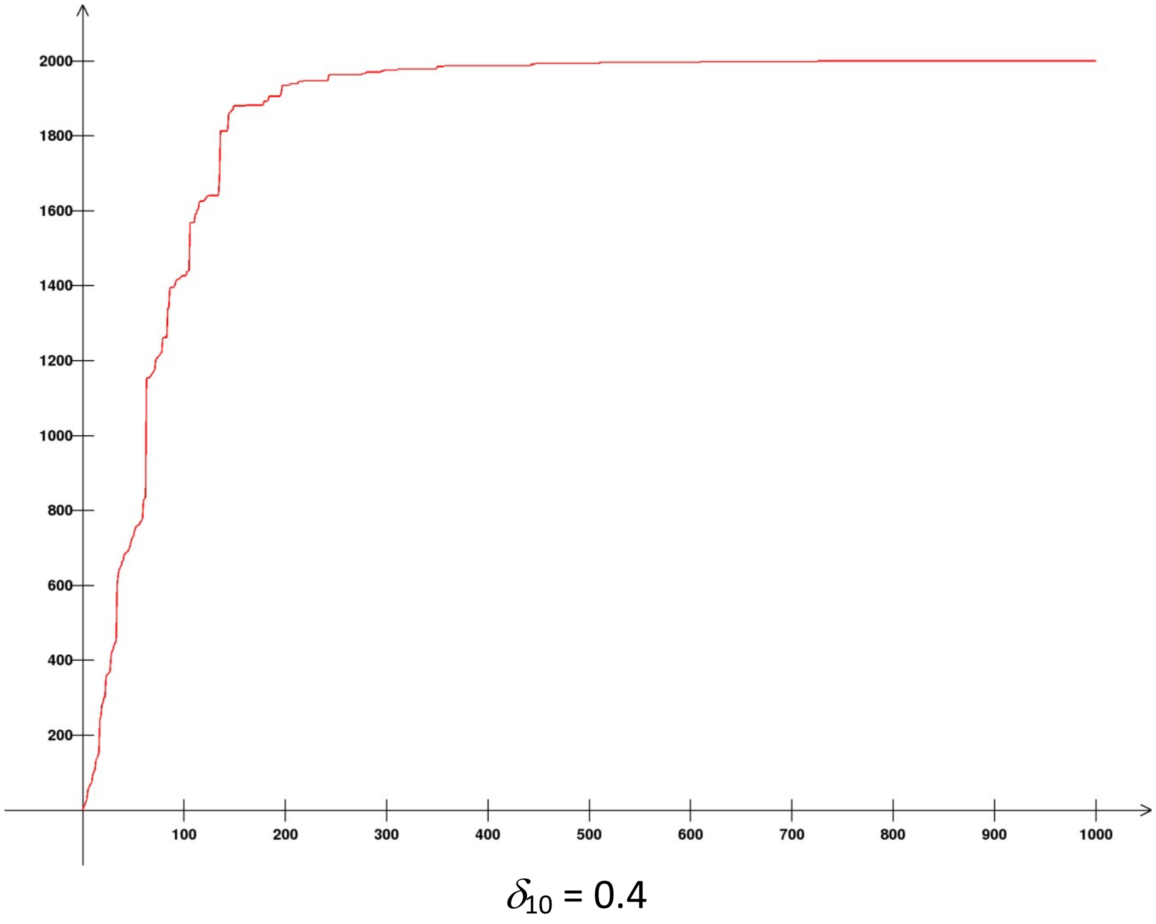

Fig. 4. The number of nodes that fail after the cascading failure stops spreading (vertical axis) versus the number of nodes that initially failed (horizontal axis) for $\delta_{10} = 0.4$.

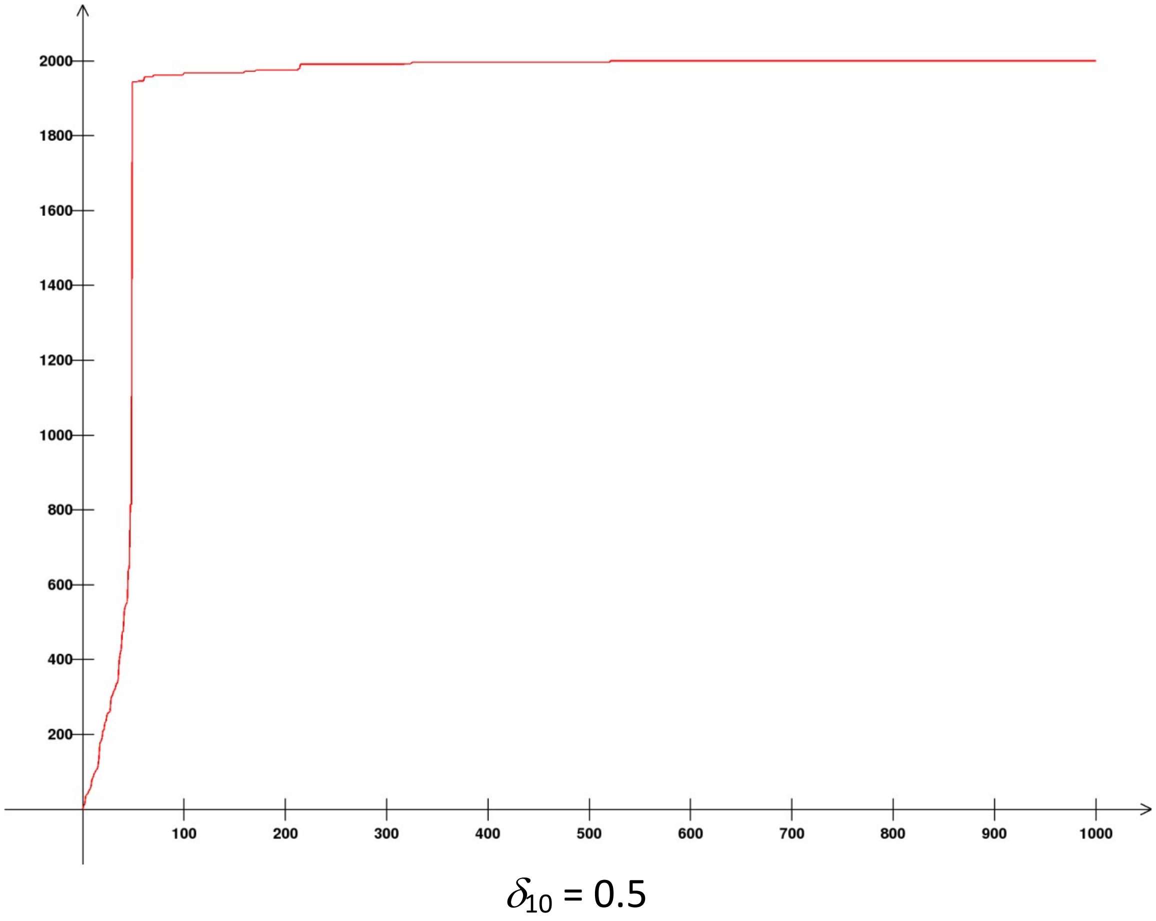

Fig. 5. The number of nodes that fail after the cascading failure stops spreading (vertical axis) versus the number of nodes that initially failed (horizontal axis) for $\delta_{10} = 0.5$.

In Fig. 4. the value on the vertical axis (the number of nodes that fail after the cascading failure stops spreading) grows in smaller increases than in Fig. 5. Also, the line in Fig. 4. can be approximated by a convex curve (with the increases smaller and smaller as the value on the horizontal axis increases). In Fig. 5. on the other hand, the line contains a sudden "jump". This corresponds to the change from 814 to 1944 nodes that fail because of the cascading failure when the number of initially failed nodes increases from 48 to 49.

This is also visible when the maximum increase in the number of failed nodes is considered, that is, the difference of the number of failed nodes at the end of the simulation for any number n and n + 1 nodes initially failed (i.e. the largest jump in the Y value in Fig. 4. and Fig. 5. when the X value is increased by one). In Fig. 6 the average maximum increase obtained for δ_{10} in the range [0, 1] (calculated over 30 repetitions of the test) is shown.

Clearly, there is a change of the behaviour of the network between 0.3 and 0.6 with the largest difference between $\delta_{10} = 0.4$ and $\delta_{10} = 0.5$. In fact, the average value observed for $\delta_{10} = 0.4$ is approximately 665.30, and the value observed for $\delta_{10} = 0.5$ is approximately 1308.57, which is almost twice the first value.

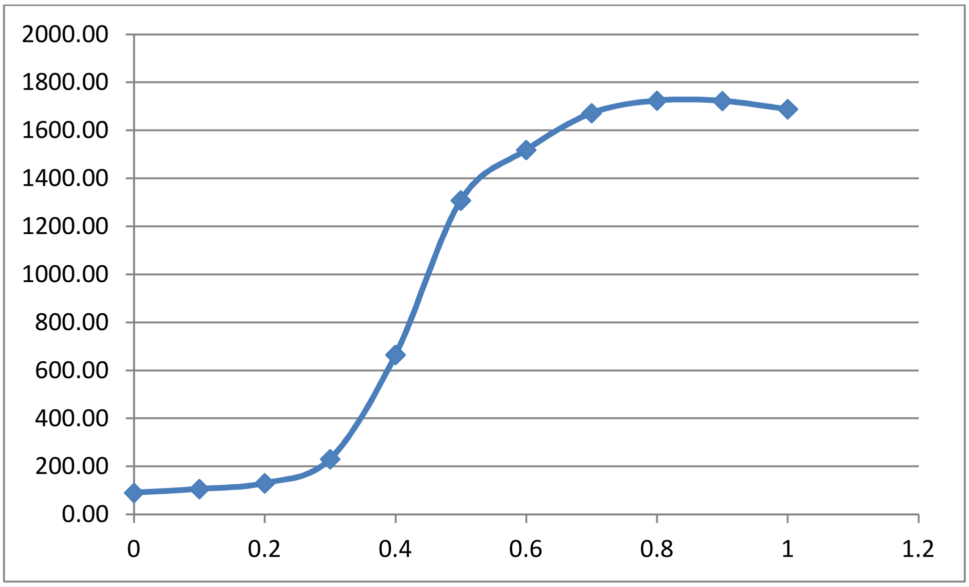

Fig. 6. The average maximum increase in the number of nodes that fail after the cascading failure stops spreading when the number of nodes that initially failed is increased by one.

Conclusions

From this set of experiments it can be seen that the strength of the coupling between network layers (here represented as a parameter describing by how much the failure in one layer overloads the corresponding node in the other layer) has a significant effect on how large portion of the network is consumed by a cascading failure.

3.3. Temporal aspects

Time-delayed networks are also studied in the area of complex systems research. The combination of multilayer structure and time-delayed propagation of the states can lead to a very complex dynamics [GKZJ16, SGJK15]. Thus, it can be expected that these aspects of the network model can also have a profound influence on the quality of results obtained by the optimizer.

Also, especially in the study of epidemics a SIR (Susceptible, Infected, Recovered) model is often used which assumes that the entities in the network can recover back to the healthy state.

These aspects of the network-based optimization have not yet been studied in depth, but it seems reasonable that the models used for representing a networked CPS should be able to represent this kind of information.

4. Modelling Multilayer Networked CPSs

Based on the performed experiments, a literature study and the knowledge of the BIFI team, the following aspects of the networked CPS model seem to be important from the point of view of optimizing threat containment (see Fig. 7 and Fig. 8).

- **A multilayer structure of the network.** This kind of structure is encountered in many real-life applications. For example in the paper [RBJF15] a hierarchy of 31 networks is mentioned (6 air route networks, 2 energy networks, 13 rail networks, 5 road networks, 4 river networks and 1 communication network). In our model this structure is represented using classes (see Fig. 7):

  Network: A container for all other elements

  Layer: Contains nodes

  Node: Belongs to exactly one layer, may be an endpoint of any number of edges (including none, for an isolated node)

  Edge: Connects exactly two nodes. Objects of this class are also used to represent coupling between layers, therefore they are not contained within Layer, but directly in the Network.

- **Representing the state of the nodes.** In this model we assume that the state of a node is represented by an attribute State in the Node class. This attribute is of type NodeState which is an enum with two values: Healthy and Failed. In some optimization problems (e.g. the FFP) it is assumed that the node can also be in a Defended state, but in our model this fact is represented by the value of the CurrentThreshold attribute.

- **Optimizer requirements.** To be able to optimize the network it is necessary to be able to change the parameters of the network and to calculate the costs incurred by these changes. To this end, we assume that in the model initial and current values of the parameters are kept, for example for the threshold determining the failure of the node two attributes are defined: InitialThreshold (the value before the optimization) and CurrentThreshold (the value set by the optimizer. Based on initial and current values of the parameters the cost of protecting the network is calculated using the CalculateNodeProtectionCost and CalculateEdgeProtectionCost methods in the subclasses of the (abstract) CostCalculator class.

- **The strength of the coupling between layers.** This can be represented as the probability of the spreading of the threat between layers or as a parameter representing how badly a node in one layer becomes overloaded by the failure of another node in a different layer. These aspects are modelled as the values of the Strength and P_{spread} attributes of the Edge class (in those instances that connect nodes in different layers).

- **Probabilistic aspects of the spreading of the threat.** In many cases the failure of a node cannot be predicted with certainty because of factors that are not possible to measure exactly (e.g. the wear of elements of a machinery). Therefore, it can be useful to assume, that the threat can spread from one node in the network to another with a certain probability P_{spread} (which, in general, can be anywhere in the range [0, 1]). The probabilistic spreading is modelled by the PSpread attribute of the Edge class.

- **The level of influence from the surrounding nodes.** In simple models, such as the deterministic Firefighter Problem (FFP), the influence from other nodes has a 0-1 characteristics (the node catches on fire when any neighbouring node is burning). However, in real life a node may be susceptible to failure only if the damaging influence from surrounding nodes is big enough. In the model proposed by Burkholz et al. [BLGS15] this is represented by thresholds which prevent nodes from failing if the influence of surrounding nodes is small. The level of influence is modelled by the Strength attribute of the Edge class.

- **Temporal aspects.** Including delays between the overloading of a node and its failure and recovery times. As shown by the available literature these aspects can influence the network dynamics in a very complex way [GKZJ16, SGJK15]. Temporal aspects are modelled by the FailureDelay and RecoveryDelay attributes of the Node class. The ThresholdExceededTime attribute represents the simulation step in which the damaging influence of the surrounding nodes exceeded the CurrentThreshold value (from this time step CurrentFailureDelay timesteps must pass before the node switches to the Failed state). The FailedTime attribute represents the simulation step in which the node failed (from this time step CurrentRecoveryDelay time steps must pass before the node switches to Healthy state). States of the nodes and the conditions for transitions between the states for this model are shown in Fig. 9.

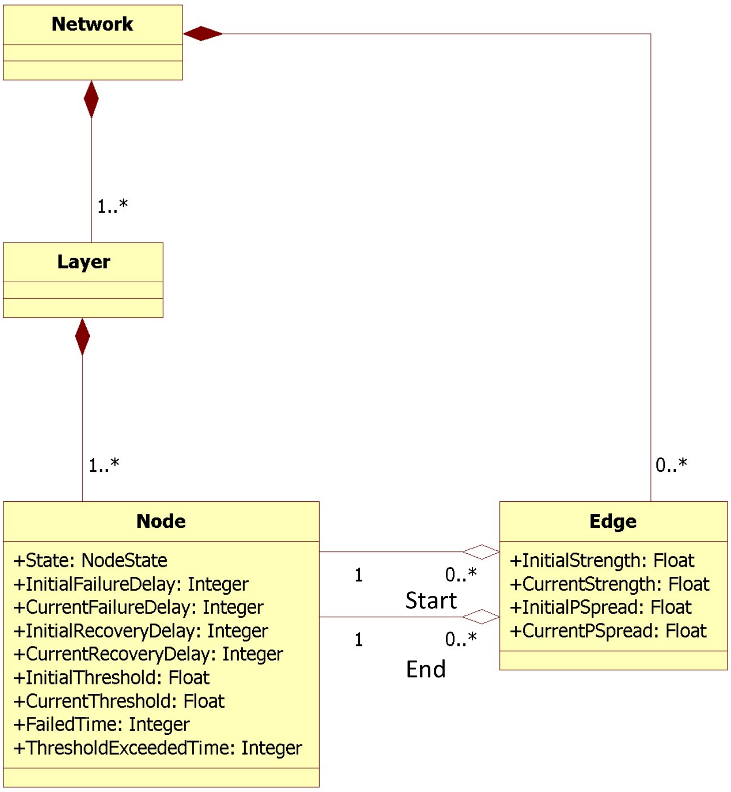

Fig. 7. Classes representing the network structure.

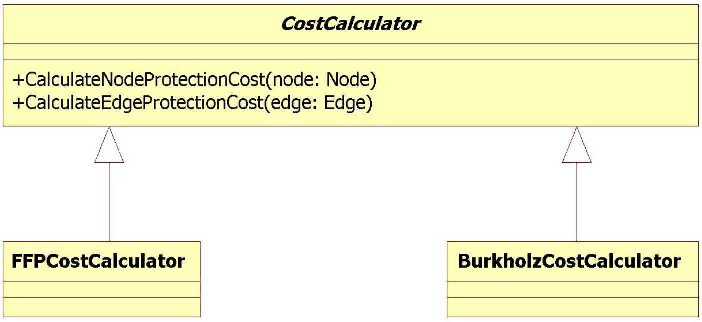
CostCalculator
+CalculateNodeProtectionCost(node: Node)
+CalculateEdgeProtectionCost(edge: Edge)
FFPCostCalculator
BurkholzCostCalculator

Fig. 8. Classes used for calculating the cost of a solution.

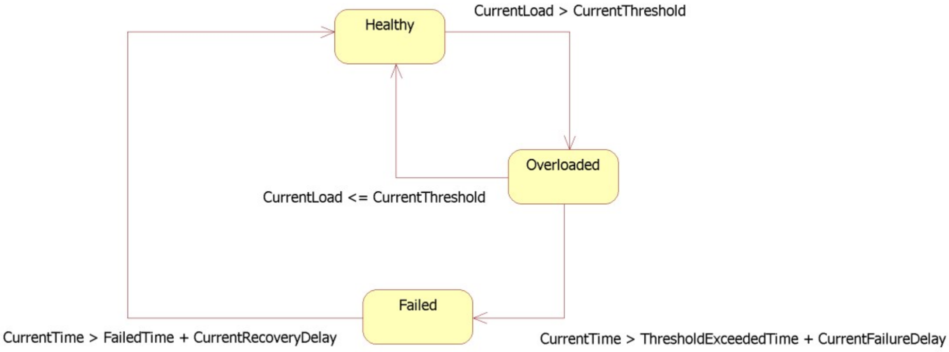
Healthy
CurrentLoad > CurrentThreshold
Overloaded
CurrentLoad <= CurrentThreshold
Failed
CurrentTime > FailedTime + CurrentRecoveryDelay
CurrentTime > ThresholdExceededTime + CurrentFailureDelay

Fig. 9. Transitions between the states of a node. CurrentTime is the number of the current simulation step, CurrentLoad is the total load exerted on the node by its neighbours.

5. Examples

In this section we describe how the proposed model can be used to represent various networked systems.

5.1. Classical Firefighter Problem (FFP)

In the classical FFP the nodes in the graph can be burning, protected or untouched (neither burning nor protected). The fire spreads from the burning nodes to the adjacent, untouched ones. The goal is to save as many nodes as possible from fire, protecting no more than N_f nodes per a time step (see the optimization scenario S1). To model this situation we can use the proposed model with a network of as many layers as necessary. Note, that because the edges in the proposed models are directed and the graph in the classical FFP is undirected we need to add two Edge objects per each edge in the graph used in the FFP instance. The attributes of the objects are set as follows:

Node

State: Some of the nodes have their state set to Failed at the beginning of the simulation, and the remaining ones to Healthy.

InitialFailureDelay, CurrentFailureDelay: set to 0

InitialRecoveryDelay, CurrentRecoveryDelay: set to +∞ (the nodes never recover when burned)

InitialThreshold: set to 0

CurrentThreshold: initially set to 0 for all nodes, set to +∞ when a node gets protected

Edge

InitialPSpread, CurrentPSpread: set to the probability of the fire spreading P_{spread} (1.0 for the deterministic FFP)

InitialStrength, CurrentStrength: set to 1

FFPCostCalculator

CalculateNodeProtectionCost(): returns 0 if CurrentThreshold == 0, returns 1 otherwise

CalculateEdgeProtectionCost(): returns 0 for all edges

5.2. Burkholz model

The model described by Burkholz et al. [BLGS15] describes spreading of failures in a two-layer network in which a node can withstand the damaging influence of the failed neighbours up to a certain threshold (see optimization scenario S4).

To model this scenario we can set the attributes of the objects as follows:

Node

State: Some of the nodes have their state set to Failed at the beginning of the simulation, and the remaining ones to Healthy.

InitialFailureDelay, CurrentFailureDelay: set to 0

InitialRecoveryDelay, CurrentRecoveryDelay: set to +∞ (the nodes never recover when failed)

InitialThreshold: set to any value in the range [0, 1] (depending how resistant to failure a given node initially is)

CurrentThreshold: initially set to InitialThreshold, and set to any value from the range [InitialThreshold, 1] during optimization

Edge

InitialPSpread, CurrentPSpread: set to 1

InitialStrength, CurrentStrength: set to 1 / deg(End), where deg() is the degree of the node End that is the end of the edge.

BurkholzCostCalculator

CalculateNodeProtectionCost(): returns (CurrentThreshold - InitialThreshold)

CalculateEdgeProtectionCost(): returns 0 for all edges

5.3. Time-delayed failures

In this case we assume that the failure of the node can be delayed for a certain number of time steps after the conditions for a failure have occurred. This can be achieved in production systems by optimizing the inventory [GAWG16] or in a two-layer CPS in which the bottom layer is the power grid by providing backup power supplies. The entire system can be described in the same way as in the Burkholz model described in the previous subsections (e.g. thresholds can be used to determine what number of neighbours have to fail, for a given node to fail), but the temporal parameters can be set in a different manner, for example:

Node

InitialFailureDelay: set to any number ≥ 0, depending on how long a given node can initially resist a failure (e.g. for how long stored supplies last)

CurrentFailureDelay: initially set to InitialFailureDelay, and set to any value ≥ InitialFailureDelay during optimization, which represents to what value the failure delay was increased by investing more resources

TimeDelayedCostCalculator

CalculateNodeProtectionCost(): returns (CurrentFailureDelay - InitialFailureDelay)

CalculateEdgeProtectionCost(): returns 0 for all edges

6. Conclusions

In this annex several phenomena are described which occur in multilayer networks and affect the problem of threat containment in networked CPSs. Also, several typical optimization scenarios for threat containment optimization are described. Based on these observations a model was proposed for describing the properties of a networked CPS in enough detail to perform threat containment optimization, taking into consideration multilayer network characteristics. Presented examples show how to apply the proposed model to various networked systems.

References

[BD15] Bollinger, L.A., Dijkema, G.P.J.: Enhancing infrastructure resilience under conditions of incomplete knowledge of interdependencies. In: Dolan, T., Collins, B. (eds.) International Symposium for Next Generation Infrastructure Conference Proceedings: 30 September - 1 October 2014. pp. 11-16. University College London (2015)

[BLGS15] Burkholz, R., Leduc, M.V., Garas, A., Schweitzer, F.: Systemic risk in multiplex networks with asymmetric coupling and threshold feedback. Tech. rep., arXiv.org (2015)

[DHW15] Dunn, S., Holmes, M., Wilkinson, S.: Modelling interdependent cascading failures in real world complex networks using a functional dependency model. In: Dolan, T., Collins, B. (eds.) International Symposium for Next Generation Infrastructure Conference Proceedings: 30 September - 1 October 2014. pp. 23-28. University College London (2015)

[DPAM02] Deb, K., Pratap, A., Agarwal, S., Meyarivan, T.: A fast and elitist multiobjective genetic algorithm: NSGA-II. IEEE Transactions on Evolutionary Computation 6, 182-197 (2002)

[ENKP15] Eshuis, R., Norta, A., Kopp, O., Pitkanen, E., "Service Outsourcing with Process Views", IEEE Transactions on Services Computing, 8(1), 136-154 (2015)

[GAWG16] Garcia-Herreros, P., Agarwal, A., Wassick, J.M., Grossmann, I.E.: Optimizing inventory policies in process networks under uncertainty. Computers & Chemical Engineering 92, 256-272 (2016)

[GKZJ16] Ghosh, S., Kumar, A., Zakharova, A., Jalan, S.: Birth and death of chimera: Interplay of delay and multiplexing. EPL (Europhysics Letters) 115(6), 60005 (2016)

[H95] Hartnell, B.: Firefighter! an application of domination. In: 20th Conference on Numerical Mathematics and Computing (1995)

[JBW08] Jackson, M., Bellgran, M., Wiktorsson, M.: Factory-in-a-box demonstrating the next generation manufacturing provider. In: Mamoru Mitsuishi, K.U., Kimura, F. (eds.) Manufacturing Systems and Technologies for the New Frontier. The 41st CIRP Conference on Manufacturing Systems (2008)

[LMG15] Lee, K.M., Min, B., Goh, K.I.: Towards real-world complexity: an introduction to multiplex networks. The European Physical Journal B 88(2), 48 (2015)

[M14] Michalak, K.: Auto-adaptation of genetic operators for multi-objective optimization in the firefighter problem. In: Corchado, E., Lozano, J.A., Quintin, H., Yin, H. (eds.) Intelligent Data Engineering and Automated Learning IDEAL 2014, LNCS, vol. 8669, pp. 484-491. Springer International Publishing (2014)

[NNMMM16] Narendra, N.C., Norta, A., Mahunnah, M., Ma, L., Maggi, F.M.: Sound conflict management and resolution for virtual-enterprise collaborations. Service Oriented Computing and Applications 10(3), 233-251 (2016)

[RBJF15] Robson, C., Barr, S., James, P., Ford, A.: Resilience of hierarchical critical infrastructure networks. In: Dolan, T., Collins, B. (eds.) International Symposium for Next Generation Infrastructure Conference Proceedings: 30 September - 1 October 2014. pp. 17-22. University College London (2015)

[SCM14] Sanchez-Garcia, R.J., Cozzo, E., Moreno, Y.: Dimensionality reduction and spectral properties of multilayer networks. Physical Review E 89(5) (2014)

[SGJK15] Singh, A., Ghosh, S., Jalan, S., Kurths, J.: Synchronization in delayed multiplex networks. EPL (Europhysics Letters) 111(3), 30010 (2015)

[SSGH14] Song, J., Sanchez, E.C., Ghanavati, G., Hines, P.: Dynamic modeling of cascading failure in power systems. CoRR abs/1411.3990 (2014)

[SW08] Svendsen, N., Wolthusen, S.: Multigraph Dependency Models for Heterogeneous Infrastructures, pp. 337-350. Springer US, Boston, MA (2008)

[ZT98] Zitzler, E., Thiele, L.: Multiobjective optimization using evolutionary algorithms - a comparative case study. In: Eiben, A.E., Back, T., Schoenauer, M., Schwefel, H.P. (eds.) Parallel Problem Solving from Nature - PPSN V, 5th International Conference, Amsterdam, The Netherlands, September 27-30, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1498, pp. 292-304. Springer (1998)

[ZTLF02] Zitzler, E., Thiele, L., Laumanns, M., Fonseca, C.M., da Fonseca, V.G.: Performance assessment of multiobjective optimizers: An analysis and review. IEEE Transactions on Evolutionary Computation 7, 117-132 (2002)