Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids

Béla Genge, *Member, IEEE,* Piroska Haller, *Member, IEEE,* Cristian-Dragoş Dumitru, and Călin Enăchescu

***Abstract*—We formulate two Intrusion Detection System (IDS) design problems for Smart Grids. The first one optimally places IDS devices on communication paths, while the second one addresses the resilient communications requirement and enhances the first problem with the provisioning of K distinct back-up paths and additional IDS devices. The developed problems harmonize real-time communication requirements with the infrastructure's resource limitations (e.g., bandwidth), detection requirements, and the available budget. A heuristic approach is developed based on the column-generation model to reduce the computation time. Experimental results comprising the Romanian 440kV and 220kV power transmission networks, the Romanian Educational communication Network (RoEduNet), alongside synthetic topologies demonstrate the effectiveness and applicability of the heuristic methodology on large problem instances.**

***Index Terms*—Smart Grid, Intrusion Detection Systems, Network Design, Resilience, Column-Generation, Heuristic.**

I. Introduction

THE proactive adoption of state-of-the-art information and communication technologies (ICT) in the cyber and the physical dimensions of the electricity grid facilitated the development of a new infrastructural paradigm known as the Smart Grid (SG). The SG constitutes the next generation electricity grid; it improves the operational benefits of control, reliability and safety, and delivers the services for new applications including renewable energy systems, vehicle-to-grid systems, voltage control and load reduction programs [1], [2].

This pervasive integration of ICT into electricity grids, however, exposes critical assets to new risks and damaging cyber attacks. Unlike traditional ICT systems where the effects of disruptive actions are generally limited to cyber operations, in the context of SG, such attacks can result in the loss of vital services. For example, in 2007 at Tempe AZ, the accidental activation of a load-shedding program opened 141 circuit breakers and caused large scale blackouts, affecting 98700 customers [3]. On the other hand, the collapse of India's northern electricity grid in July 2012 affected more than 600 million people and led to the loss of power in transportation, health care, and many other sectors [4]. Although the aforementioned incidents were not the result of cyber attacks, they demonstrated the level of damage that a potential attack may cause. More recently, however, the cyber-attack targeting the Ukrainian electricity grid [5] demonstrated the exceptional impact of cyber-physical attacks, where an ordinary malware infection may leave vast populated regions without electricity.

In light of these sophisticated threats, the protection of critical SG assets has become a matter of national security. The implementation of protection schemes in SG, however, is not a trivial task. This is mainly owed to the difficulties in quantifying cyber security risks, to the variety of possible threats, and to the limited security budgets. Several risk assessment and security schemes have been developed as support for utilities in the implementation of security programs [6], [7], [8], [9]. These methodologies are suggesting that protection schemes need to be encapsulated in the design of SG, where various requirements characteristic to industry-grade communications need to be harmonized with security requirements, and the features of legacy and state of the art technologies.

This paper develops optimal network design problems to address the existing gap between security/resilience requirements and the provisioning of cost-effective SG communications. The security requirement is formulated in terms of the monitoring of communications by SG Intrusion Detection Systems (IDS), while the resilience requirement addresses the ability of the infrastructure to function in the presence of disturbances, e.g., failure or cyber attacks. In particular, we formulate two optimal IDS network design problems aimed to address the gap between previous studies focusing on the development of detection engines [10], [11], [12], [13], [14], the placement of IDS engines based on various criteria [15], [16], [17], [18], and the design of the underlying communication network [19], [20]. Compared to these works, this paper targets the more challenging problem of designing a resilient SG communication infrastructure, where IDS engines are spread across the infrastructure to ensure the resilient monitoring of flows at a minimum cost.

The first design problem minimizes costs, while optimally selecting communication paths and the location of IDS devices. The second design problem extends the first one with the provisioning of K distinct back-up paths for each communication flow in order to facilitate the design of resilient SG communications. In order to reduce the computation time, we formulate a simple heuristic that uses the column generation model [21] and separately solves the path selection, and the IDS monitoring sub-problems.

Extensive numerical results demonstrate the applicability of the methodologies in two scenarios: a qualitative analysis is performed on an installation encompassing the Romanian 400kV and 220kV transmission networks and the Romanian Educational communication Network (RoEduNet); a quanti-

B. Genge, P. Haller, and C. Enăchescu are with the Department of Computer Science, C.D. Dumitru is with the Department of Electrical Engineering and Computer Science, Petru Maior University of Tîrgu Mureş, Mureş, Romania, 540088 e-mail: bela.genge@ing.upm.ro, phaller@upm.ro, cristian.dumitru@ing.upm.ro, ecalin@upm.ro.

Manuscript received August 30, 2016.

tative analysis is conducted by leveraging synthetic data to demonstrate the scalability and efficiency of the developed heuristic.

We believe that this work brings several major contributions, including:

1) It formulates an IDS network design problem that harmonizes real-time communication requirements pertaining to the selection of shortest routing path, with the communication infrastructure's resource limitations, detection requirements, and the available budget.
2) It formulates a K-resilient IDS design problem that allocates K distinct back-up paths to each flow.
3) It develops a simple heuristic to effectively reduce the computation time of the two IDS design problems.

The remainder of this paper is structured as follows. Section II presents an overview on related studies. Section III presents the two IDS design problems and the heuristic IDS design methodology. Experimental results are outlined in Section IV and the paper concludes in Section V.

II. Related Work

The study of IDS is a well established field of research. The work of Horkan [22] showed the various opportunities and design decisions that need to be taken into account for distributing detection devices across an industrial communication network. Berthier, *et al.* [23] identified the parameters that need to be monitored in Advanced Metering Infrastructures (AMI) for detecting cyber attacks. In their later work, Berthier and Sanders [24] developed a specification-based intrusion detection sensor for AMI. The work uses state machines, and three constraint categories including network, device and application constraints. These are used to build the specification of the system, i.e., the normal operation, where any deviation from the normal is treated as a possible threat.

Zhang, *et al.* [10] developed an IDS provisioned across different layers of SG. Its modules adopted Support Vector Machine and Artificial Immune Systems for detecting and classifying malicious data. Lo and Ansari [16] reported CONSUMER, a hybrid IDS for distribution networks. Their framework comprises a sensor grid placement algorithm to deploy grid sensors and to guarantee state estimation solvability. While CONSUMER focuses on the observability of smart grid measurements, it does not harmonize the monitoring requirements with other significant aspects including the routing of communications, real-time communications, and budgetary limitations. A behavior rule-based IDS was proposed by Mitchell and Chen [11] for securing head-ends, distribution access points/data aggregation points and subscriber energy meters. In the same direction we mention the work of Pan, *et al.* [12], which adopted data mining techniques to automatically learn patterns by fusing data obtained from synchrophasor measurements, and power system audit logs. The developed IDS prototype was used to classify disturbances, normal control operations, and cyber-attacks. Zhou, *et al.* [13] reported a multimodel-based anomaly IDS in industrial process automation. The methodology includes a classifier based on an intelligent hidden Markov model, aimed to differentiate the hardware/software faults from cyber attacks. Hui Lin, *et al.* [25] developed a specification-based intrusion detection framework based on the Bro network traffic analyzer [26]. The approach includes a parser for the DNP3 protocol, which supports the definition of process-specific semantics related to network events. [14] presented a semantic analysis framework that integrates IDS with the power flow analysis. The approach monitors the network in real-time, it processes control packets and runs a power flow look-ahead evaluation based on simulation in order to determine the possible impact of commands on the physical process. More recently, Bao, *et al.* [27] developed behavior rules to identify devices deviating from normal specifications and to detect sophisticated attackers. While the above-mentioned works may detect device misbehavior, their focus is not related to the design problems addressed by the paper at hand.

In the direction of optimal network design we start by mentioning the early work of Frisanco [19]. Here, the author proposed several mathematical problems, which can be used for optimal redundant path planning in ATM networks. While the work of Frisanco is similar to ours in terms of using bandwidth reservation for redundant path planning, the methodology presented in this paper goes further by addressing the security requirements of communications in smart grids. To this end, the present work focuses on the optimal provisioning of IDS, while taking into account the redundant planning of paths, the infrastructure costs, and the characteristics of communication flows in terms of monitoring requirements. Recently, in [28], Hui Lin, *et al.* explored the advantages of Software-Defined Networks to achieve an attack-resilient infrastructure. The approach changes the configuration of network switches, it automatically disconnects compromised PMUs, and reconnects legitimate, i.e., non-compromised, PMUs. On the other hand, Thakore, *et al.* [17] developed a methodology for the optimal deployment of monitoring devices. The authors formulate a 0-1 integer program with inequality constraints, which aims to minimize costs, while ensuring that the detection requirements are satisfied. Even though the approach is evaluated in a different field of research (traditional Web service software), it provides valuable insights on the possible refinement of the monitoring requirements and cost parameters included in the present work.

A work that is closely related to the methodology developed in this paper is that of Ghasempour and Gunther [18]. The authors developed an approach to optimize the number of aggregators in smart grid communications, while taking into account delays, costs and energy consumption. They constructed a delay model based on assumptions concerning the receive, processing and transmission delays of aggregators. Nevertheless, the approach does not account for the connectivity matrix between nodes, it does not embrace security requirements, and it does not address resilience to cyber attacks. Next, we mention the work of Cardenas, *et al.* [15], which is perhaps the closest to the methodology proposed in this paper. They developed a cost model-based framework to aid utilities in the provisioning of IDS. The framework leverages the output of risk assessment methodologies, which represent the input to a decision assistance model. The model can be used to

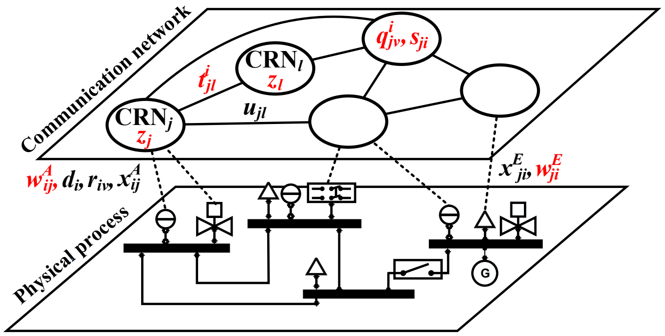


Fig. 1: Relationship between the key symbols and the cyber-physical architecture of a power grid. Parameters are denoted by black, and variables by red coloring.

analyze the trade-off between cost and benefits of installing intrusion detection systems in different locations. Compared to [15], the present work integrates the communication network (connectivity matrix) into the decision process and identifies the optimal positioning of detection devices, while delivering a resilient detection infrastructure. Lastly, we mention our previous work [20], where the resilient IDS design problem was formulated as a heuristic algorithm. Conversely, this paper presents an optimal resilient IDS problem together with a heuristic to reduce the computation time.

Based on the previous analysis, we note that while several IDS methodologies have been developed for SG, the more challenging problem of encapsulating large-scale communications, intrusion detection and real-time requirements into a comprehensive methodology was not properly addressed yet. We believe that the uniqueness of the developed methodology and its applicability to smart grid infrastructures is given by the encapsulation of the non-bifurcated path selection, the use of static routing, and by the selection of the shortest routing path. The three components are necessary to design the communication infrastructure such as to conform to industrial specifications in terms of communication delays and availability of redundant paths [29]. We observe, however, that in case routing decisions and flow characteristics are similar to industry-grade requirements, the methodology can be applied to other scenarios as well.

III. IDS Design Problems

A. Scenario Description

The methodology presented in this paper embraces the large-scale characteristic of Smart Grid communication networks. It presumes that each communication flow, hereinafter called simply flow, provides the means for monitoring and control, as well as the necessary means to transfer data between two end-points, e.g., log files, Voice Over IP (VoIP). The monitoring is performed through observed variables, while the control is performed through a set of control variables. Control nodes may take various forms, yet the best known implementation is the dedicated control hardware. Nevertheless, this work assumes that human operators are an integral part of Smart Grids and may close significant control loops at a local, regional or national level by means of various ICT hardware and software. Hence, control loop end-points may include control nodes, but also the measurement and the actuation nodes. Lastly, we assume that each flow comprises two end-points: access and egress. Data between these end-points is routed by a set of candidate routing nodes (CRNs), which are interconnected according to a connectivity matrix. A summary of the main abbreviations, symbols and notations used throughout this paper are given in Table I and Table II, while the relationship between the key symbols and the cyber-physical architecture of a power grid is illustrated in Fig. 1.

TABLE I: Main Abbreviations

Abbreviation	Definition
AMI	Advanced metering infrastructure
CRN	Candidate routing node
H-INDP	Heuristic to solve the INDP
H-RINDP	Heuristic to solve the RINDP
H-RINDP$_\mathrm{L}$	Heuristic to solve the link resilient INDP
H-RINDP$_\mathrm{N}$	Heuristic to solve the node resilient INDP
ICT	Information and communication technologies
IDS	Intrusion detection systems
INDP	IDS network design problem
ISP	Internet service provider
MU	Monetary units
RCG	Resilient communication group
RINDP	Resilient IDS network design problem
RINDP$_\mathrm{L}$	Link resilient INDP
RINDP$_\mathrm{N}$	Node resilient INDP
RoEduNet	Romanian educational communication network
SG	Smart grid
VoIP	Voice over IP

B. IDS Network Design Problem

In the IDS network design problem (INDP) we define $I = \{1, 2, ..., i, ...\}$ as the set of flows, $J = \{1, 2, ..., j, ...\}$ as the set of CRNs, and $V = \{1, 2, ..., v, ...\}$ as the set of IDS device classes, where each device class is assumed to detect a set of cyber-attacks. The reasoning behind the definition of set V is that smart grids may embrace a wide variety of network traffic, which may require a differentiated type of analysis for the detection of cyber attacks. For example, traditional ICT traffic is usually monitored by classic IDS based on traditional cyber-attack signatures, e.g., ARP poisoning and Denial of Service (DoS). Conversely, the monitoring and the detection of abnormal behavior particularly in the physical dimension of smart girds, e.g., the abnormal consumption of energy as reported by smart meters, requires deep-packet inspection, including process-specific dynamics. Such sophisticated detection engines are usually embedded in smart grid-specific IDS [30] and are included as a different class of IDS in the definition of V.

Next, the problem's parameters are defined. Let c^L_{jl} be the cost of buying one unit of bandwidth between CRNs j and l, c^A_{ij} the cost of buying one unit of bandwidth between the access end-point of flow i and CRN j, c^E_{ji} the cost of buying one unit of bandwidth between the egress end-point of flow i

TABLE II: Key Notations and Descriptions

Notation	Description
Sets/Indices:	
I, J, V, P	Flows (I), CRNs (J), IDS device classes (V), paths (P)
i, k, j, v, p	Flow (i and k), CRN (j), IDS device class (v), path (p)
Parameters:	
c^A_{ij}, c^E_{ji}	The cost of access (c^A_{ij}) and egress (c^E_{ji}) bandwidth
c^L_{jl}	The cost of bandwidth on link (j, l)
c^V_{jv}	The cost of detection for device of class v at CRN j
c^P_i	Penalty cost for not monitoring flow i
c^I	The total budget for provisioning the IDS
c^F_{ip}	The composite cost of c^A_{ij} and c^E_{ji} for path p
d_i	The demand of flow i
h_{ik}	The membership of i and k to the same RCG
r_{iv}	Monitoring of flow i by an IDS device of class v
u_{jl}	The capacity of link (j, l)
x^A_{ij}, x^E_{ji}	Access (x^A_{ij}) and egress (x^E_{ji}) flow connectivity
$\hat{y}^p_i$	The selection of path p for flow i (optimal solution)
δ^p_{jl}	The presence of link (j, l) on path p
γ^p_i	The allowed paths to route flow i
ζ^p_j	The selection of CRN j on path p (optimal solution)
Variables:	
o_{iv}	Exclusion of i from monitoring by devices of class v
q^i_{jv}	Monitoring of flow i in CRN j by a device of class v
s_{ji}	Routing of flow i by CRN j
t^i_{jl}	Routing of flow i on link (j, l)
w^A_{ij}, w^E_{ji}	Selection of access (w^A_{ij}) and egress (w^E_{ji}) CRN j
y^p_i	Routing of flow i on path p
z_j	Selection of CRN j

and CRN j, and c^V_{jv} the cost of buying one unit of bandwidth for an IDS device of class v installed at CRN j. Then, let x^A_{ij} be a binary parameter with value 1 if the access end-point of flow $i \in I$ can be connected to CRN $j \in J$, and x^E_{ji} a binary parameter with value 1 if the egress end-point of flow i can be connected to CRN j. Let d_i denote the demand of flow i and u_{jl} the capacity of link (j, l). We assume that if CRNs j and l are not connected, then $u_{jl} = 0$. To provide the utilities the opportunity to express the various monitoring requirements of each flow, we define the binary variable r_{iv} to indicate that flow i needs to be monitored by an IDS of class $v \in V$.

Considering the limitations on security budgets, it is reasonable to assume that not all flows may be monitored by the IDS for cyber attacks. Therefore, we define c^P_i to be the penalty cost of not monitoring flow i, which is also used to prioritize flows in order to ensure the monitoring of critical communications. Subsequently, we define c^I as the total available security budget, i.e., maximum cost for provisioning the IDS.

Next, the problem's variables are defined. Let z_j be a binary variable with value 1 if CRN j is selected, s_{ji} a binary variable with value 1 if CRN j routes flow i, t^i_{jl} a binary variable with value 1 if flow i is routed on link (j, l), and q^i_{jv} a binary variable with value 1 if flow i is monitored by an IDS device of class v at CRN j. Let w^A_{ij} be a binary variable with value 1 if the access end-point of flow i is routed by CRN j, and the binary variable w^E_{ji} with value 1 if the egress end-point of flow i is routed by CRN j. We define the binary variable o_{iv} with value 1 if flow i is not monitored by detection devices of class v due to the unavailability of resources, e.g., limited budget.

The objective of the network design is to minimize costs by minimizing the costs of bandwidth, and of detection by IDS:

$$F^* = \min \sum_{j,l \in J, i \in I} c^L_{jl} d_i t^i_{jl} + \sum_{j \in J, i \in I} \left(c^A_{ij} w^A_{ij} + c^E_{ji} w^E_{ji} \right) d_i + \sum_{i \in I, j \in J, v \in V} c^V_{jv} d_i q^i_{jv} + \sum_{i \in I, v \in V} c^P_i o_{iv}, \tag{1}$$

and is subject to the following constraints:

$$\sum_{j \in J} w^A_{ij} = 1, \sum_{j \in J} w^E_{ji} = 1, \quad \forall i \in I \tag{2}$$

$$w^A_{ij} \leq x^A_{ij} z_j, w^E_{ji} \leq x^E_{ji} z_j, \quad \forall i \in I, j \in J \tag{3}$$

$$w^A_{ij} - w^E_{ji} - \sum_{l \in J} \left(t^i_{jl} - t^i_{lj} \right) = 0, \quad \forall j \in J, i \in I \tag{4}$$

$$\sum_{i \in I} d_i t^i_{jl} \leq u_{jl} z_j, \sum_{i \in I} d_i t^i_{jl} \leq u_{jl} z_l \quad \forall j, l \in J \tag{5}$$

$$\alpha s_{ji} \geq w^A_{ij} + w^E_{ji} + \sum_{l \in J} t^i_{jl}, \quad \forall i \in I, j \in J \tag{6}$$

$$s_{ji} \leq w^A_{ij} + w^E_{ji} + \sum_{l \in J} t^i_{jl}, \quad \forall i \in I, j \in J \tag{7}$$

$$q^i_{jv} \leq r_{iv} s_{ji}, \quad \forall j \in J, v \in V, i \in I \tag{8}$$

$$r_{iv} \sum_{j,l \in J} (t^i_{jl} - \alpha q^i_{jv}) \leq \alpha o_{iv}, \quad \forall i \in I, v \in V \tag{9}$$

$$\sum_{i \in I, j \in J, v \in V} c^V_{jv} d_i q^i_{jv} \leq c^I \tag{10}$$

Constraints (2) and (3) limit the number of connections between access/egress flow end-points and CRNs to one. Constraint (4) is a classical multicommodity flow conservation constraint [21], which imposes the selection of a continuous path between access and egress connection endpoints. Constraint (5) imposes that the bandwidth required to route flows on link (j, l) does not exceed the link capacity. Constraints (6) and (7) impose that $s_{ji} = 1$ if flow i is routed by j, where α is a large integer. The value of α needs to be larger than the value of $w^A_{ij} + w^E_{ji} + \sum t^i_{jl}$ in all possible scenarios (the worst case scenario is that $w^A_{ij} = 1, w^E_{ji} = 1$, and $t^i_{jl} = 1, \forall i \in I, j, l \in J$). s_{ji} is then used in constraint (8) to impose the selection of detection devices of class v at CRN j for flow i, only if CRN j is also selected. Constraint (9) imposes the activation of variable o_{iv} in case that the budget is insufficient to monitor all flows, and constraint (10) enforces that the total cost of the monitored flows does not exceed c^I.

We observe that the cost parameters included in (1) allow to prioritize between the selection of the shortest path and the minimization of the cost of the IDS. In particular, the cost parameters c^L_{jl} and c^V_{jv} permit the tuning of the optimization problem to express the trade-off between the cost of links c^L_{jl} and the cost of detection devices c^V_{jv}. Utilities can thus emphasize, for instance, the significance of the shortest path over the infrastructure cost by increasing the value of c^L_{jl}. Furthermore, to distinguish between high priority flows (with real-time requirements), and flows without real-time constraints c^L_{jl} can be replaced by c^L_{jli}. This way, the value of c^L_{jli} can be adjusted on a per-flow basis, thus enforcing the selection of the shortest path for communications with real-time constraints.

On the other hand, the access and egress cost parameters (c^A_{ij} and c^E_{ji}) embrace the costs of connecting communication end-points to the CRNs. These are significant features, which, in practice need to be taken into account since the infrastructure for connecting the end-points may require additional investments.

Besides these aspects, recall that the INDP also includes a second prioritization mechanisms through the c^P_i cost parameter. To this end, c^P_i ensures the prioritization of flows in terms of monitoring by enforcing the exclusion of lower-priority flows in case of insufficient funds. This two-dimensional prioritization is a salient feature of INDP providing various opportunities to adjust the optimal solution according to the infrastructure's requirements.

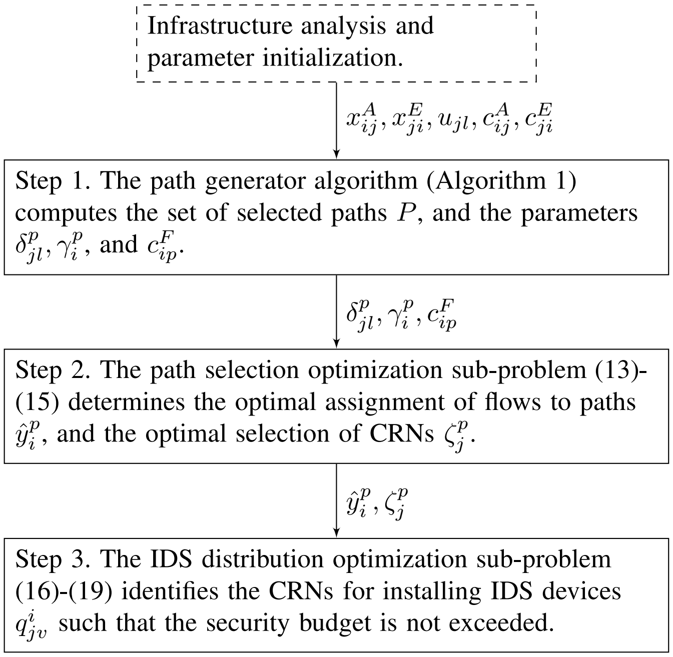
Lastly, it should be noted that the INDP presumes that the real-time communication requirement of industrial communication flows is the minimization of the path length. Hence, the minimization of the communication latency. The choice for using this approach, rather than adopting a minimum-latency threshold, was that the INDP builds on bandwidth reservation, which is subject to the capacity limitation constraints. As a result, the problem ensures that communications are congestion-free, and therefore, the use of minimum-path-length can minimize the communication latency. However, in case that measurements pertaining to link latency are available, and there is a strict packet delivery time for high-speed messages, e.g., alerts, the INDP can be extended with additional constraints to ensure that maximum latency limits are not exceeded. Additional information related to the definition of latency constraints is available in [31].

C. Resilient IDS Network Design Problem

The resilient IDS network design problem (RINDP) imposes the provisioning of K distinct back-up communication paths for each flow, and the provisioning of IDS devices along each communication path. For this purpose the RINDP extends I with an additional set of K back-up flows associated to each main flow i. It further defines the resilient communication group (RCG) encompassing the main flow together with all of its associated back-up flows, and the binary parameter h_{ik}, $i,k \in I$, such that $h_{ik} = 1$ if i and k are part of the same RCG. We assume that $h_{ii} = 1$. The INDP problem is extended with the following constraints, which impose the selection of distinct links for flows in the same RCG.

$$\sum_{k \in I} (t^k_{jl} + t^k_{lj}) h_{ik} \leq 1, \qquad \forall i \in I, j, l \in J \tag{11}$$

The problem comprising (1)-(11) is defined as the link resilience problem and is denoted by $\mathrm{RINDP_L}$. We further


Infrastructure analysis and parameter initialization.

$x^A_{ij}, x^E_{ji}, u_{jl}, c^A_{ij}, c^E_{ji}$

Step 1. The path generator algorithm (Algorithm 1) computes the set of selected paths P, and the parameters $\delta^p_{jl}, \gamma^p_i$, and c^F_{ip}.

$\delta^p_{jl}, \gamma^p_i, c^F_{ip}$

Step 2. The path selection optimization sub-problem (13)-(15) determines the optimal assignment of flows to paths $\hat{y}^p_i$, and the optimal selection of CRNs ζ^p_j.

Step 3. The IDS distribution optimization sub-problem (16)-(19) identifies the CRNs for installing IDS devices q^i_{jv} such that the security budget is not exceeded.

Fig. 2: The main steps of the developed heuristics.

assume a second and more restrictive scenario, which imposes the selection of distinct CRNs for flows in the same RCG:

$$\sum_{k \in I, l \in J} (t^k_{jl} + t^k_{lj}) h_{ik} \leq 1, \qquad \forall i \in I, j \in J \tag{12}$$

The problem comprising (1)-(10), and (12) is defined as the node resilience problem and is denoted by $\mathrm{RINDP_N}$.

D. Heuristic to Solve the IDS Network Design Problems

Unfortunately, the computing time for obtaining an optimal solution for INDP and RINDP might be very large even for small problem instances. Therefore, we develop a simple heuristic, named H-INDP and H-RINDP, to reduce the computation time of INDP and of RINDP, respectively. The heuristic is composed of three main steps, as described below. The first step adopts the column-generation model (CGM) [21] and generates the set P denoting the selected paths between all flow's possible access and egress end-points. Even though apparently the number of paths can be very large, as explained in [21] this is only the case of symmetric networks, that is, of networks where most of the nodes have the same degree of connectivity. However, real communication networks exhibit a hierarchical structure of connections between CRNs [32], where a key objective is to minimize the path length in order to minimize communication delays. Therefore, the selection of shorter paths is desirable in industrial communications, and this requirement can be used to significantly reduce the size of P. As later shown by results, these assumptions effectively reduce the number of possible paths, and enable feasible computations for large problem instances as well. The second step separately solves the path selection sub-problem, while the third step solves the IDS distribution sub-problem and identifies the CRNs where IDS devices need to be installed.

Algorithm 1 Path Generator Algorithm

```
$P = \emptyset$;
**for** each $i \in I, j, j' \in J$ **do**
    **if** $x^A_{ij} <> 0$ and $x^E_{j'i} <> 0$ **then**
        $P' = $ @GeneratePaths$(j, j')$;
        $\gamma^p_i = 1, \forall p \in P'$;
        $c^F_{ip} = c^A_{ij} + c^E_{j'i}, \forall p \in P'$;
        $P = P \cup P'$;
    **end if**
**end for**
$\delta^p_{jl} = 1$ if $(j, l) \vdash p = \texttt{True}, \forall j, l \in J, p \in P$.
```

The main steps of the developed heuristics are depicted in Fig. 2.

We start by defining the binary variable y^p_i with value 1 if flow i is routed on path $p \in P$, the binary parameter δ^p_{jl} with value 1 if path p contains the link (j, l), the binary parameter γ^p_i with value 1 if flow i can be routed on path p, and the cost of connecting access and egress end-points to path p, denoted by parameter c^F_{ip}. In step 1, Algorithm 1 is used to precompute the values of δ^p_{jl}, γ^p_i, and c^F_{ip}, where $\vdash$ is defined as the boolean operator $(\_,\_) \vdash \_ : (J \times J) \times P \rightarrow \{\texttt{True}, \texttt{False}\}$. $\vdash$ returns `True` if link (j, l) is on path p, and `False`, otherwise. The algorithm starts by generating the set of paths P' between each pair of CRNs j, j' that may route flow i by using the @GeneratePaths(j, j') function. The impact of this function on the generated solutions is analyzed in the following sections. Based on the generated paths, the algorithm then continues with the initialization of parameters γ^p_i, c^F_{ip}, and δ^p_{jl}.

In step 2, the path selection optimization sub-problem aims to select the paths with the minimum costs and is defined as:

$$H^*_P = \min \sum_{j,l \in J, i \in I, p \in P} c^L_{jl} d_i \delta^p_{jl} y^p_i + \sum_{i \in I, p \in P} c^F_{ip} d_i \gamma^p_i y^p_i, \qquad (13)$$

$$\text{s.t.} \quad \sum_{i \in I, p \in P} d_i \delta^p_{jl} y^p_i \leq u_{jl}, \quad \forall j, l \in J \qquad (14)$$

$$\sum_{p \in P} y^p_i = 1, \forall i \in I, \; y^p_i \leq \gamma^p_i, \forall i \in I, p \in P \qquad (15)$$

Next, the IDS device distribution optimization sub-problem is defined as part of step 3. By solving the first sub-problem we determine the optimal assignment of flows to paths $\hat{y}^p_i$, the sub-set of selected CRNs $J^S \subset J$, the sub-set of selected paths $P^S \subset P$, and the optimal selection of CRNs ζ^p_j such that $j \in J^S$, $p \in P^S$. The IDS distribution sub-problem then identifies the CRNs for installing IDS devices such that the security budget is not exceeded:

$$H^*_D = \min \sum_{i \in I, j \in J^S, v \in V} c^V_{jv} d_i q^i_{jv} + \sum_{i \in I, v \in V} c^P_i o_{iv}, \qquad (16)$$

$$\text{s.t.} \quad q^i_{jv} \leq r_{iv} \sum_{p \in P^S} \hat{y}^p_i \zeta^p_j, \quad \forall i \in I, j \in J^S, v \in V \qquad (17)$$

$$r_{iv}(\hat{y}^p_i - \sum_{j \in J^S} \zeta^p_j q^i_{jv}) \leq \hat{y}^p_i o_{iv}, \forall p \in P^S, i \in I, v \in V (18)$$

$$\sum_{i \in I, j \in J^S, v \in V} c^V_{jv} d_i q^i_{jv} \leq c^I \qquad (19)$$

For RINDP$_{\mathrm{L}}$ we define H-RINDP$_{\mathrm{L}}$ by extending the path selection sub-problem with the following constraints imposing the selection of link-independent back-up paths:

$$\sum_{k \in I, p \in P} (\delta^p_{jl} + \delta^p_{lj}) h_{ik} y^p_k \leq 1, \qquad \forall i \in I, j, l \in J \qquad (20)$$

Similarly, we define the CRN-independent problem H-RINDP$_{\mathrm{N}}$ for RINDP$_{\mathrm{N}}$ by extending the path selection sub-problem with the following constraints:

$$\sum_{k \in I, l \in J, p \in P} (\delta^p_{jl} + \delta^p_{lj}) h_{ik} y^p_k \leq 1, \qquad \forall i \in I, j \in J \qquad (21)$$

We emphasize that while the reduction of the problem's complexity is addressed by means of the developed heuristics, the methodology yields an optimal solution in several cases. These have been summarized as part of Theorem (1) and Corollary (1.1).

Theorem 1. *The optimal cost of INDP is equal to the optimal cost of H-INDP, provided that the set of paths P_F resulting from the optimal selection of links (t^i_{jl}) in INDP is a subset of P and that the cost of detection devices is independent from the location of CRNs.*

Proof. We need to prove that $F^* = H^*_P + H^*_D$, provided that $c^V_{jv} = c^V_v, \forall j \in J$ and that $P_F \subset P$, where c^V_v is the unique cost of detection devices. We observe that (1) comprises two cost components: the cost of the multicommodity flow problem in node-arc formulation, denoted by $F^*_1 = F^*_{1L} + F^*_{1E}$, where $F^*_{1L} = \sum c^L_{jl} d_i t^i_{jl}, F^*_{1E} = \sum \left(c^A_{ij} w^A_{ij} + c^E_{ji} w^E_{ji}\right) d_i$; and the cost of the selected IDS, denoted by $F^*_2 = \sum c^V_{jv} d_i q^i_{jv}$. Hence, we can write that $F^* = F^*_1 + F^*_2$. On the other hand, (13) also comprises two components: the cost of links, denoted by $H^*_{P1} = \sum c^L_{jl} d_i \delta^p_{jl} y^p_i$; and the cost of edges, denoted by $H^*_{P2} = \sum c^F_{ip} d_i \gamma^p_i y^p_i$. Consequently, $H^*_P = H^*_{P1} + H^*_{P2}$.

Based on the notations above, we observe that for $p \in P^*_F$, if link (j, l) is part of path p, that is $(j, l) \vdash p = \texttt{True}$, then $\exists p' \in P$ such that $(j, l) \vdash p' = \texttt{True}$. Since the cost of link (j, l) is the same in the INDP and H-INDP, then the selection of link (j, l) as part of the solution of the INDP will also yield the selection of the same link as part of the solution of the H-INDP. Hence, $F^*_{1L} = H^*_{P1}$.

Earlier, we have established that $c^F_{ip} = c^A_{ij} + c^E_{ji}$. As a result, H^*_{P2} can be rewritten as $H^*_{P2} = \sum (c^A_{ij} + c^E_{ji}) d_i \gamma^p_i y^p_i$, which is equivalent to F^*_{1E} within the boundaries of our initial assumptions. It follows that $F^*_1 = H^*_{P1} + H^*_{P2} = H^*_P$.

Lastly, we need to prove that $F^*_2 = H^*_D$. Based on the assumption that $c^V_{jv} = c^V_v$, then H^*_D can be rewritten as $H^*_D = \sum c^V_v d_i q^i_{jv}$. Once again, this is equivalent to F^*_2. □

Corollary 1.1. *It follows from the proof of Theorem 1, that the optimal cost of INDP is equal to the optimal cost of H-INDP, provided that all cost parameters ($c^A_{ij}, c^E_{ji}, c^L_{jl}, c^V_{jv}$) are independent from the location of CRNs.*

Lastly, we note that while the heuristic significantly reduces the execution time, its application to very large infrastructures spanning across different administrative domains needs to be carefully and realistically planned. In such scenarios it is reasonable to assume that precise information on flows, costs and infrastructure is usually not available outside a given administrative domain. To address such restrictive scenarios, we can perform a domain-based decomposition [33], where each domain is reduced to a node connected to its neighboring nodes, i.e., other administrative domains, with one or more links. Then, the H-INDP and H-RINDP are applied to the reduced problem, which yields the optimal inter-domain routing and monitoring of flows. Subsequently, for each domain, the optimal allocation of detection devices is determined by applying the same heuristic methodology. By doing so, the approach preserves the information privacy of each administrative domain and ensures the scalability and the realistic applicability of H-INDP and H-RINDP to sensitive and very large-scale scenarios as well, e.g., continental power grids.

IV. Experimental Results

We evaluate the sensitivity of the IDS design problems to different parameters like the installation costs, the number of flows, the number of CRNs, and the detection requirements associated to each flow. Numerical results are given for two different scenarios: *Scenario A* involves the Romanian high voltage power transmission system and the Romanian Educational communication Network (RoEduNet); and *Scenario B* involves synthetic data aimed to test the scalability of the proposed IDS design problems, and the gap between the solutions of the full optimization problems and the heuristic methodology.

The IDS design problems have been implemented in AIMMS [34], where the CPLEX engine was selected as the solver. The path generator algorithm was implemented in the `Python` language. The experiments have been performed on a host with Intel i3-4005U CPU (1.7GHz), 8MB of RAM, and the Windows 10 OS.

A. Scenario A: The Romanian Power Transmission Network

In this scenario the analysis focuses on Romania's 400kV and 220kV transmission network (see Fig. 3). In order to ensure a realistic estimation of parameters, meetings with representatives of a local electricity grid operator and Internet Service Provider (ISP) were arranged. The Romanian communication network of electricity grid operators encompasses a mixture of network technologies and it builds on the operator's own communication lines (primary) based on fiber optics installed on top of power lines and on communication channels leased from national ISPs (secondary). Despite the high bandwidth provided by the operator's fiber optics network, temperature variations between different seasons have an exceptional impact on the reliability of communications. The temperature changes increase the cost of maintenance in certain regions, which has led to the adoption of leased lines from different ISPs as primary communications. In terms of network traffic, operators from each substation send real-time data (e.g., voltages, power flows) to five regional operators at a rate of 13Kbps (first flow). A separate communication channel is used to transfer Voice Over IP (VoIP) and system diagnosis data at a rate of 360Kbps (second flow).

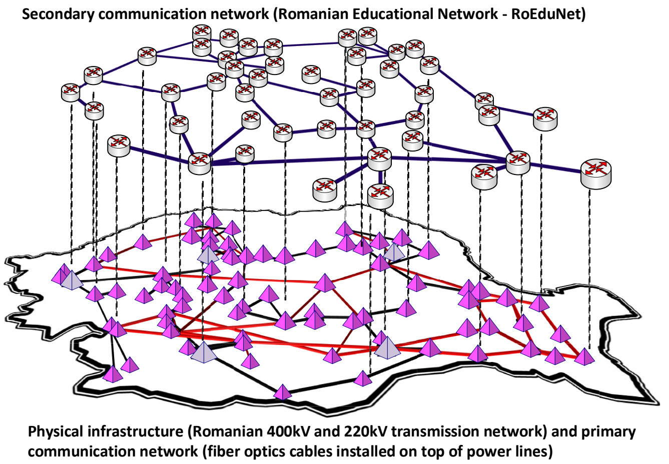

Secondary communication network (Romanian Educational Network - RoEduNet)
Physical infrastructure (Romanian 400kV and 220kV transmission network) and primary communication network (fiber optics cables installed on top of power lines)

Fig. 3: Romanian 400kV (denoted by red lines) and 220kV (denoted by black lines) power transmission network, primary and secondary communication infrastructures.

TABLE III: Initial Parameter Values for *Scenario A*

Parameter	Value
c_{jl}^L, c_{ij}^A [MU/Kbps]	1
c_{ji}^E [MU/Kbps]	1 (j is a regional CRN), $MAXINT$ (otherwise)
c_{jv}^V [MU/Kbps]	100 ($v = v_1$), 10 ($v = v_2$)
c_i^P [MU/Kbps]	*MaxCost* ($i \in I^D$), $MaxCost \cdot \lvert I^D \rvert$ ($i \in I^R$)
c^I [MU/Kbps]	$\sum c_{jv}^V d_i$
d_i [Kbps]	13 (real-time traffic), 360 (VoIP/diagnosis)
u_{jl} [Mbps]	1000 (primary), 10 (secondary), 1 (inter-network)
x_{ij}^A	1 ($\lvert\lvert accpos(i), crnpos(j)\rvert\rvert < \beta^F$), 0 (otherwise)
x_{ji}^E	1 (j is a regional CRN), 0 (otherwise)

1) Parameterization: Given the set of all CRNs J let $J^P \subset J$ be the set of CRNs from the primary network (88 nodes), and $J^S \subset J$ the set of CRNs from the secondary network (46 nodes) such that $J^P \cup J^S = J$ and $J^P \cap J^S = \emptyset$. According to the discussions with the electricity operator we presume the routing of two flows from each substation to each regional operator. The first flow is the real-time data traffic (with a demand of $d_i = 13$Kbps), while the second flow includes VoIP and system diagnosis data (with a demand of $d_i = 360$Kbps). Given that Romania's high voltage transmission network consists of 88 substations, set I will comprise 176 flows. We assume that I^R is the set of real-time flows, and I^D is the set of VoIP and system diagnosis flows, such that $I^R \cup I^D = I$ and $I^R \cap I^D = \emptyset$. Lastly, the set V consists of two classes of IDS devices: (i) industrial IDS ($v_1 \in V$) capable to detect process-specific anomalies (abnormal voltage, short-circuits, ground faults); and (ii) traditional IDS ($v_2 \in V$) capable to detect classical cyber attack signatures, e.g., ARP poisoning, Denial of Service (DoS) attacks. The device classes in V can be instantiated in each node $j \in J$. The industrial real-time traffic is usually monitored by both types of devices ($r_{iv} = 1, \forall i \in I^R, v \in V$), while the VoIP/system diagnosis flows need only the presence of traditional IDS ($r_{iv} = 1, \forall i \in I^D, v = v_2$).

At first, for the sake of simplicity, we assume that $c_{jl}^L = 1$

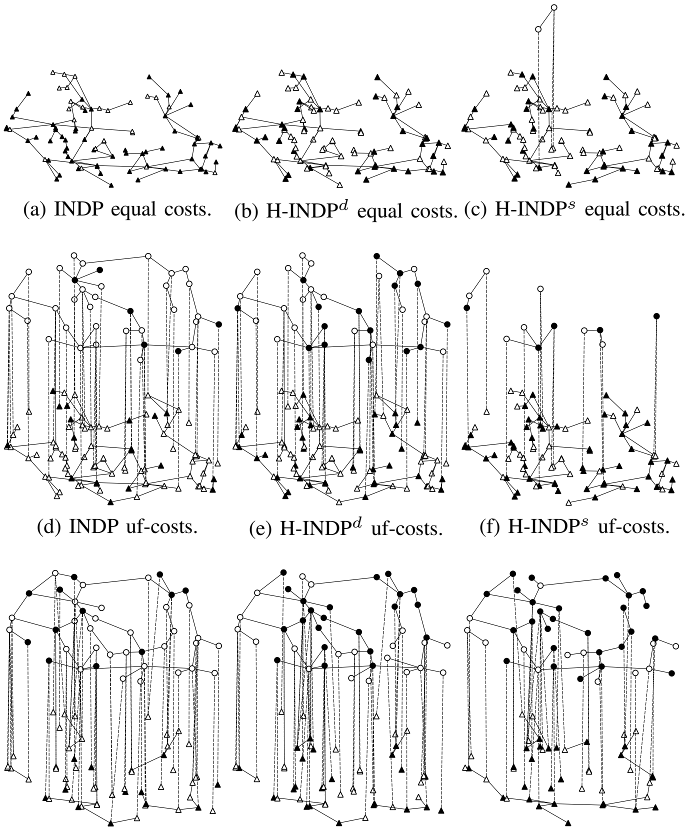
Monetary Units (MU) per Kbps $\forall j, l \in J$, $c_{ij}^{A} = 1$MU/Kbps, and $c_{ji}^{E} = 1$MU/Kbps if j belongs to the flow's set of regional CRNs and $c_{ji}^{E} = MAXINT$ MU/Kbps, otherwise ($MAXINT$ is a large integer). The cost of detection devices is assumed to be the same in the primary and in the secondary networks. Nevertheless, we assume that $c_{jv}^{V} = 100$MU/Kbps for v_1 and $c_{jv}^{V} = 10$MU/Kbps for v_2, which is a realistic and clear distinction between the cost of traditional and industrial IDS.

The connectivity of each flow's access end-point to the neighboring CRNs is determined according to the Euclidean distance (written as $||a, b||$, where a and b are two geographical points given by latitude and longitude) between the geographical location of the two nodes. Considering the possible limitations of directly connecting two distant nodes, we define β^{F} to denote the Euclidean distance above which connections between flows and CRNs are unfeasible, and β^{R} to denote the Euclidean distance above which connections between two CRNs are unfeasible. Let $x_{ij}^{A} = 1$ if $||accpos(i), crnpos(j)|| < \beta^{F}$, and $x_{ji}^{E} = 1$ if j is the flow's regional CRN ($crnpos(j)$ is a function that returns the position of CRN j, and $accpos(i)$ is a function that returns the position of the access end-point of flow i).

Next, since the primary communication network builds on fiber optic cables, we assume that $u_{jl} = 10$Gbps, $\forall j, l \in J^{P}$ if there is a physical link between j and l, and $u_{jl} = 0$, otherwise. Despite the presence of fiber optic cables in the secondary network as well, this network is shared among different operators, e.g., other ISPs. Hence, for the secondary network we assume $u_{jl} = 10$Mbps $\forall j, l \in J^{S}$ in the case there is a physical link between j and l, and a value of 0, otherwise. Conversely, connections between the two networks are usually implemented via a mixture of solutions including GPRS, and 10/100/1000Mbps cables. We presume that the capacity of links between the two networks is of 1Mbps if $||crnpos(j), crnpos(l)|| < \beta^{R}$ and is 0, otherwise.

The cost penalty parameter c_{i}^{P} needs to be initialized with a value that is larger than the sum of all possible infrastructure costs. This is to ensure that the variable o_{iv} from (1) is activated only in case that any other alternative would yield an unfeasible solution. Therefore, we define $MaxCost = \sum c_{jl}^{L} d_i + \sum \left(c_{ij}^{A} + c_{ji}^{E}\right) d_i + \sum c_{jv}^{V} d_i$ as the maximum cost of the worst case scenario in which all flows are monitored in all nodes by all IDS classes. Then, we define $c_{i}^{P} = MaxCost, \forall i \in I^{D}$ and $c_{i}^{P} = MaxCost \cdot |I^{D}|, \forall i \in I^{R}$, where $|\_|$ is the set cardinality operator. $MaxCost$ thus acts as the penalty cost and ensures that the solver first activates o_{iv} for all flows in I^{D}, before it proceeds to the activation of o_{iv} for flows in I^{R}. In other words, a differentiated cost will ensure that in the case of insufficient funds the solver will first exclude from monitoring the lower priority flows, i.e., flows from I^{D}, while maintaining the monitoring of higher priority flows in accordance with the available budget. The total available security budget is initially set as the maximum possible infrastructure cost, i.e., $c^{I} = \sum c_{jv}^{V} d_i$.

Lastly, we recall that the choice of implementation for function @GeneratePaths(j, j') in Algorithm 1 may have a significant influence on the performance of H-INDP. Therefore, in the following, we test the influence of two different algorithms available in `Python`'s `NetworkX` module: 1) a depth-first search algorithm [35] (denoted by H-INDP^{d} and H-RINDP^{d}); and 2) Dijkstra's all shortest paths algorithm (denoted by H-INDP^{s} and H-RINDP^{s}).



(a) INDP equal costs. (b) H-INDP^{d} equal costs. (c) H-INDP^{s} equal costs.

(d) INDP uf-costs. (e) H-INDP^{d} uf-costs. (f) H-INDP^{s} uf-costs.

(g) RINDP$_{\text{L}}$ uf-costs. (h) H-RINDP$_{\text{L}}^{d}$ uf-costs. (i) H-RINDP$_{\text{L}}^{s}$ uf-costs.

Fig. 4: Graph visualization of the INDP, H-INDP, RINDP and H-RINDP solutions in *Scenario A* ("uf-costs" denotes the uniform distribution of costs). Triangles denote CRNs in the primary network, and circles denote CRNs in the secondary network. Filled geometric shapes denote the presence of IDS.

Obviously, the above assumptions are general and do not affect the proposed design problems, which are applicable to any topology and configuration. The initial parameter values are summarized in Table III.

2) INDP and H-INDP: As shown by results in Table IV ($\beta^{F} = 1$km, $\beta^{R} = 20$km), the computation time for INDP is 919.3s, while in the case of H-INDP^{d} the computation time is 1.3s for a path depth of maximum 6 nodes, and is 7.1s for depth=8. The high performance of the developed heuristic methodology is also underpinned by the computation time of H-INDP^{s}, in which case an optimal solution is found in 0.52s. The difference between the cost of INDP and H-INDP (hereinafter denoted by 'Gap') is 0%, which is explained by the initial assignment of costs (the same for all assets). The graph visualization of a selection of results is depicted in Fig. 4a (INDP), Fig. 4b (H-INDP^{d}, depth=8), and Fig. 4c (H-INDP^{s}). In the first two cases the solution includes CRNs

TABLE IV: INDP and H-INDP: Initial Setting

INDP		**H-INDP^d**					**H-INDP^s**			
Time [s]	Cost [MU]	Depth	$\|P\|$	Time [s]	Cost [MU]	Gap [%]	$\|P\|$	Time [s]	Cost [MU]	Gap[%]
919.3	567595	6	1795	1.3	567595	0	125	0.52	567595	0
		7	3972	2.7	567595	0				
		8	8623	6.02	567595	0				

TABLE V: INDP and H-INDP: Uniform Cost Distribution

INDP		**H-INDP^d**					**H-INDP^s**			
Time [s]	Cost [MU]	Depth	$\|P\|$	Time [s]	Cost [MU]	Gap [%]	$\|P\|$	Time [s]	Cost [MU]	Gap[%]
337.9	3441304	6	1795	1.3	3923891	14.02	125	0.6	4420017	28.4
		7	3972	2.9	3895087	13.1				
		8	8623	7.1	3890722	13.05				

TABLE VI: RINDP and H-RINDP: Uniform Cost Distribution ('†' denotes that an optimal solution was not found after 24h)

RINDP$_\mathbf{L}$		**H-RINDP$^d_\mathbf{L}$**					**H-RINDP$^s_\mathbf{L}$**			
Time [s]	Cost [MU]	Depth	$\|P\|$	Time [s]	Cost [MU]	Gap [%]	$\|P\|$	Time [s]	Cost [MU]	Gap[%]
2923	3602766	6	21413	214.5	4287698	19.1	503	3.4	4951814	37.4
		7	95642	†						
RINDP$_\mathbf{N}$		**H-RINDP$^d_\mathbf{N}$**					**H-RINDP$^s_\mathbf{N}$**			
†		6	193522	†			6469	145	6528897	

TABLE VII: Path Length (Uniform Cost Distribution)

IDS Design Problem	**Maximum**	**Average**
INDP	12	5.53
RINDL$_\mathrm{L}$	16	7.5
H-INDP^d (depth=6)	6	5.07
H-INDP^d (depth=7)	7	6.08
H-INDP^d (depth=8)	8	7.03
H-INDP^s	6	3.08
H-RINDP$^d_\mathrm{L}$ (depth=6)	6	5.54
H-RINDP$^s_\mathrm{L}$	6	3.51
H-RINDP$^s_\mathrm{N}$	8	3.85

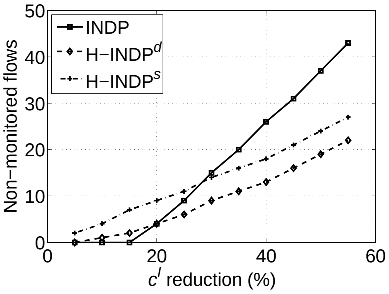


Fig. 5: Effect of c^I variations on the set of monitored flows.

exclusively from the primary network, while the last case includes two CRNs from the secondary network.

Next, we look at the effect of uniform cost distributions on the generated solutions. The cost parameters $c^A_{ij}, c^E_{ji}, c^L_{jl}$, and c^V_{jv} are redefined such that $c^A_{ij} = c^E_{ji} = 1 + URand(1, 10)$ MU/Kbps, $c^L_{jl} = 10 + URand(1, 10)$ MU/Kbps, and $c^V_{jv} = 1 + URand(1, 10)$ MU/Kbps, $\forall i \in I, j, l \in J, v \in V$, where $URand(a, b)$ is a function that returns a random number in the $[a, b]$ interval according to a uniform distribution. The remaining parameters are initialized according to the initial setting (Table III).

The experimental results for this scenario are summarized in Table V. In this case the INDP is solved in 337.9s, which, compared to the previous setting, is almost three times lower and is explained by the fact that the solver performs better in the absence of identical solution choices. We observe that the H-INDP^d outperforms INDP 260 times for depth=6, and 47 times for depth=8. We also observe that the gap is quite small (under 15%), which further motivates the use of the proposed heuristic for large problem instances as well. While the H-INDP^s exhibits a lower computation time compared to H-INDP^d (0.6s), it increases the gap to 28.4%. This is explained by noting that the shortest paths might not lead towards the most cost-effective solution. Conversely, as demonstrated by H-INDP^d, the adoption of longer paths in the path selection sub-problem may reduce this gap. However, we observe that H-INDP^s brings a significant advantage over INDP and H-INDP^d, since it delivers the shortest routing path, thus minimizing communication delays (see Table VII). This is a key advantage of H-INDP^s and a significant trade-off to costs, addressing at the same time a key requirement of industrial real-time communications. To this end, we note that according to recent studies [36] on Internet communications the average path length varies between 6-8, which means that the H-INDP^s may also yield more realistic results. The graph visualization of a selection of results is illustrated in Fig. 4d (INDP), Fig. 4e (H-INDP^d, depth=8), and Fig. 4f (H-INDP^s).

Lastly, for the same scenario we evaluate the effect of c^I variations on the set of monitored flows. Based on the budget required for monitoring all flows in the case of INDP, H-INDP^d (depth=8) and H-INDP^s we gradually reduced the budget by 5%. The results depicted in Fig. 5 showcase the ability of the developed IDS design problems to exclude flows from the monitoring process in the case of insufficient funds. We further observe that the reduction of c^I has a similar impact on all three problems and it constitutes a significant instrument for IDS designers, since it indicates the need for additional funds, while ensuring that a feasible solution is also provided.

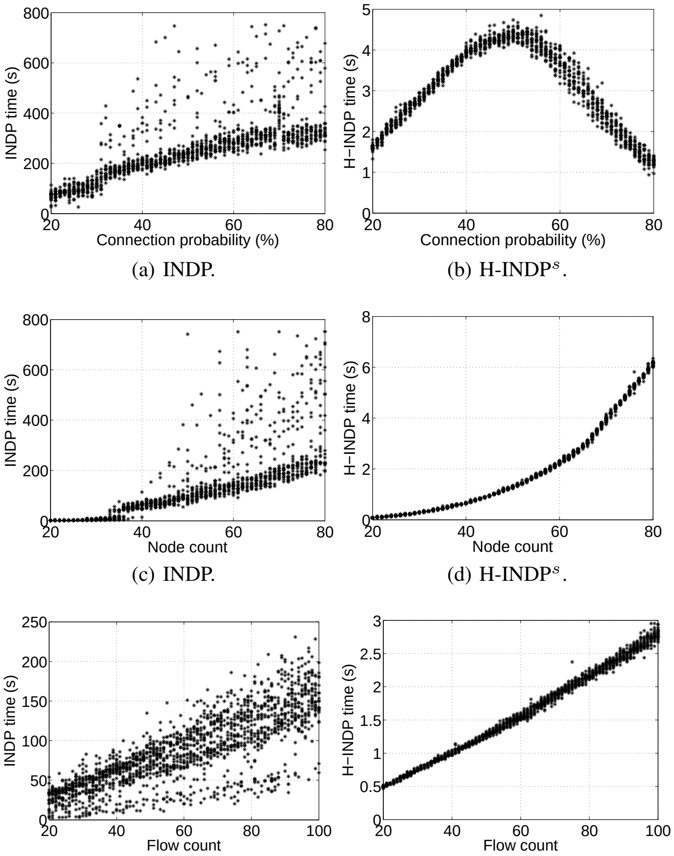
3) RINDP and H-RINDP: To evaluate the solutions of RINDP$_{\mathrm{L}}$ and H-RINDP$_{\mathrm{L}}$ we set $\beta^R = 40$km to ensure the availability of link-independent paths. We further assume that a back-up path is needed for each real-time flow, which effectively increases the number of flows to 264. These variations, however, also increase the problem's complexity and degrade the performance of the IDS design problems. As shown in Table VI, an optimal solution for H-RINDP$^d_{\mathrm{L}}$ is not found even after 24h for depth=7 and depth=8. A trade-off to these large computing times, however, is to permit larger gap values by reducing the size of set P through the H-RINDP$^s_{\mathrm{L}}$. As shown by results, the measured computing time for H-RINDP$^s_{\mathrm{L}}$ is 860 times smaller than the computing time of RINDP$_{\mathrm{L}}$, which is in line with the observations reported above. The graph visualization for a selection of results in this case as well is shown in Fig. 4g (RINDP), Fig. 4h (H-INDP$^d_{\mathrm{L}}$, depth=8), and Fig. 4i (H-RINDP$^s_{\mathrm{L}}$).

Next, we look at the solutions of RINDP$_{\mathrm{N}}$ and H-RINDP$_{\mathrm{N}}$. The CRN-independent problems, however, require additional options in terms of connectivity. Consequently, we set $\beta^F =$ 100km, while maintaining β^R at 40km. As shown in Table VI, by increasing the number of connection options, the solver cannot find an optimal solution for RINDP$_{\mathrm{N}}$ and H-RINDP$^d_{\mathrm{N}}$ even after 24h. However, by reducing the number of paths by means of adopting Dijkstra's shortest path algorithm, the H-RINDP$^s_{\mathrm{N}}$ provides an optimal solution in 145s.

B. Scenario B: Synthetic Data

We aim to test the effect of connection probabilities (denoted by *Scenario B1*), CRN count (denoted by *Scenario B2*) and flow count (denoted by *Scenario B3*) on the computation time and on the gap in the case of INDP and H-INDP^s. The analysis is focused on H-INDP^s considering its superior performance over H-INDP^d (in terms of computation time), as measured in the previous scenarios. In the case of *Scenario B1* we used a fixed number of flows and nodes ($|I| = 100$ and $|J| = 50$), while varying the connection probability between CRNs and flow end-points from 20% to 80% (access and egress end-points were set to be different in all cases, that is $\forall i \in I, j, j' \in J$, if $x^A_{ij} = 1$ and $x^E_{j'i} = 1$, then $j <> j'$). In the case of *Scenario B2* we assumed that $|I| = 50$, 20% connectivity probability for access and egress flow end-points, and 50% connection probability between CRNs. Lastly, in the case of *Scenario B3* we used 50 CRNs, and 50% connection probability. In all scenarios, the remaining parameters were initialized with uniformly distributed random values.

For each configuration we generated 20 sets of synthetic data. In each case the parameter values have been initialized according to the above-mentioned settings. The synthetic data was generated for the INDP with the help of the AIMMS software [34]. After each execution of INDP the values of sets, parameters, and variables were automatically saved to AIMMS-specific output text files. Then, for each set of experimental files, we used `Python` scripts including the `NetworkX` module to compute the values of $\delta^p_{jl}, \gamma^p_i$, and c^F_{ip}, which were finally written to AIMMS-compatible text files. Next, we developed an AIMMS program to automatically execute the path selection and the IDS distribution optimization sub-problems. The output of each run was saved in text files, which have been finally processed by another set of `Python` scripts. Overall, automated experiments have been conducted continuously on 4060 data sets over a six week period.



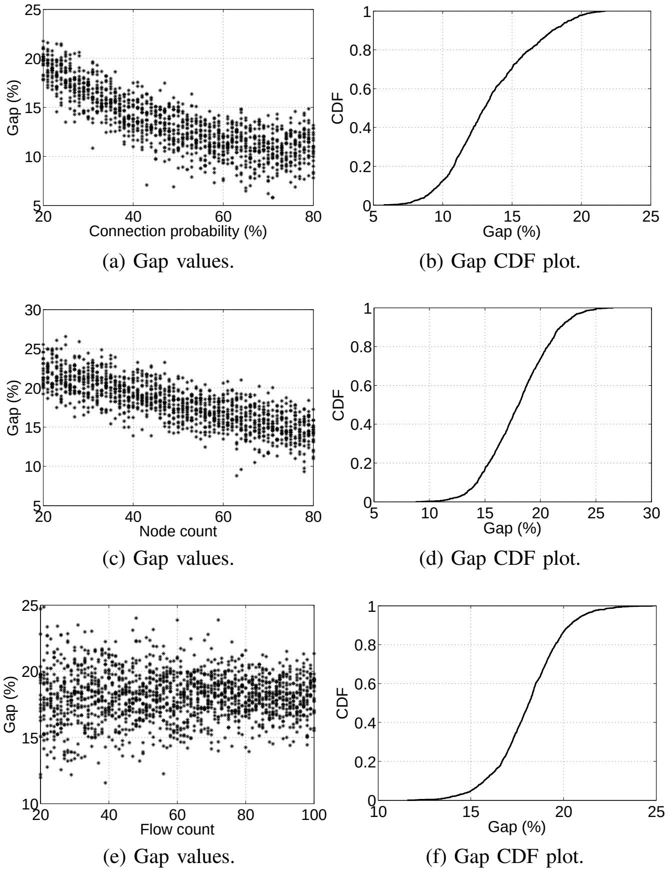
(a) INDP. (b) H-INDP^s.

(c) INDP. (d) H-INDP^s.

(e) INDP. (f) H-INDP^s.

Fig. 6: Computation time with synthetic data.

As shown by the results in Fig. 6, the computation time of INDP is significantly affected by the problem's complexity. Accordingly, in *Scenario B1* in the case of INDP the computation time increases on average from 50s for 20% connection probability to 380s for 80% connection probability. Conversely, the increase of the connection probability has an inverse effect on H-INDP^s. This is explained by the additional and shorter paths that are created with the increase of connection probabilities. The results in *Scenario B2* and *Scenario B3* are also in line with the previous observation. Here, we observe a significant computation time difference between INDP and H-INDP^s. Furthermore, we notice that the H-INDP^s exhibits a linear increase in computation time, which motivates the choice to use the proposed heuristics as a basis



(a) Gap values.

(b) Gap CDF plot.

(c) Gap values.

(d) Gap CDF plot.

(e) Gap values.

(f) Gap CDF plot.

Fig. 7: Gap analysis with synthetic data.

to solve large problem instances.

The result of the gap analysis depicted in Fig. 7 indicates that in most cases (80%) the gap is below 20%. However, as also demonstrated by the previous scenario, the gap can be further reduced by adopting the H-INDP^d, which, as a downside, may affect the computation time. Nonetheless, we note that the H-INDP^s brings key advantages over INDP and H-INDP^d, as demonstrated by previous scenarios. That is, the H-INDP^s enforces the selection of shortest communication paths, which is a fundamental requirement in industrial real-time communications.

V. Conclusion

We have developed two IDS network design problems for Smart Grids that accommodate traditional design requirements pertaining to shortest path routing and budgetary limitations, alongside modern security requirements including the monitoring of communication flows and the provisioning of resilient infrastructures. In order to reduce the computation time, a heuristic approach that separately solves the path selection and the IDS device distribution sub-problems was presented. The IDS design problems have been extensively analyzed in two scenarios. The results showed the superior performance of the heuristic methodology in terms of computation time and its applicability to large problem instances.

Acknowledgment

This research was supported by a Marie Curie FP7 Integration Grant within the 7th European Union Framework Programme (Grant no. PCIG14-GA-2013-631128).

References

[1] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A stackelberg game approach," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, March 2013.

[2] H. Liu, H. Ning, Y. Zhang, and L. T. Yang, "Aggregated-proofs based privacy-preserving authentication for v2g networks in the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1722–1733, 2012.

[3] J. Weiss, "Protecting industrial control systems from electronic threats," *New York: Momentum Press*, May 2010.

[4] Zeenews Bureau, "North India blackout: Blame it on states," http://zeenews.india.com/news/nation/north-india-blackout-blame-it-on-states_790811.html, 2012, [accessed August 2016].

[5] A. Cherepanov, "BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry," 2016.

[6] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart Grid Information Security (SGIS)," *SG-CG/M490*, 2014.

[7] B. Genge, I. Kiss, and P. Haller, "A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 3 – 17, 2015.

[8] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. T. Yang, and M. Guizani, "Securing vehicle-to-grid communications in the smart grid," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 66–73, 2013.

[9] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. T. Yang, "Role-dependent privacy preservation for secure v2g networks in the smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 208–220, 2014.

[10] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec 2011.

[11] R. Mitchell and I. R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, Sept 2013.

[12] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov 2015.

[13] C. Zhou, S. Huang, N. Xiong, S. H. Yang, H. Li, Y. Qin, and X. Li, "Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 10, pp. 1345–1360, Oct 2015.

[14] H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer, and R. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[15] A. Cardenas, R. Berthier, R. Bobba, J. Huh, J. Jetcheva, D. Grochocki, and W. Sanders, "A framework for evaluating intrusion detection architectures in advanced metering infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 906–915, March 2014.

[16] C. H. Lo and N. Ansari, "Consumer: A novel hybrid intrusion detection system for distribution networks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 33–44, June 2013.

[17] U. Thakore, G. A. Weaver, and W. H. Sanders, "A quantitative methodology for security monitor deployment," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2016, pp. 1–12.

[18] A. Ghasempour and J. H. Gunther, "Finding the optimal number of aggregators in machine-to-machine advanced metering infrastructure architecture of smart grid based on cost, delay, and energy consumption," in *2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan 2016, pp. 960–963.

[19] T. Frisanco, "Optimal spare capacity design for various protection switching methods in atm networks," in *Communications, 1997. ICC '97 Montreal, Towards the Knowledge Millennium. 1997 IEEE International Conference on*, vol. 1, 1997, pp. 293–298 vol.1.

[20] B. Genge, P. Haller, and I. Kiss, “A framework for designing resilient distributed intrusion detection systems for critical infrastructures,” *International Journal of Critical Infrastructure Protection*, vol. 15, pp. 3–11, 2016.

[21] C. Barnhart, C. A. Hane, and P. H. Vance, “Using branch-and-price-and-cut to solve origin-destination integer multicommodity flow problems,” *Oper. Res.*, vol. 48, no. 2, pp. 318–326, Mar. 2000.

[22] M. Horkan, “Challenges for IDS/IPS deployment in industrial control systems,” *SANS Institute reading room*, 2015.

[23] R. Berthier, W. Sanders, and H. Khurana, “Intrusion detection for advanced metering infrastructures: Requirements and architectural directions,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, Oct 2010, pp. 350–355.

[24] R. Berthier and W. H. Sanders, “Specification-based intrusion detection for advanced metering infrastructures,” in *Proceedings of the 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing*, ser. PRDC ’11, 2011, pp. 184–193.

[25] H. Lin, A. Slagell, C. Di Martino, Z. Kalbarczyk, and R. K. Iyer, “Adapting bro into scada: Building a specification-based intrusion detection system for the dnp3 protocol,” in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, ser. CSIIRW ’13, 2013, pp. 5:1–5:4.

[26] V. Paxson, “Bro: A system for detecting network intruders in real-time,” in *Proceedings of the 7th Conference on USENIX Security Symposium - Volume 7*, ser. SSYM’98, 1998, pp. 3–3.

[27] H. Bao, R. Lu, B. Li, and R. Deng, “Blithe: Behavior rule-based insider threat detection for smart grid,” *IEEE Internet of Things Journal*, vol. 3, no. 2, pp. 190–205, April 2016.

[28] H. Lin, C. Chen, J. Wang, J. Qi, D. Jin, Z. Kalbarczyk, and R. K. Iyer, “Self-healing attack-resilient pmu network for power system operation,” *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[29] Institute of Electrical and Electronics Engineers, “Ieee 1646-2004 standard: communication delivery time performance requirements for electric power substation automation,” 2004.

[30] P. Jokar, N. Arianpoo, and V. C. M. Leung, “Electricity theft detection in ami using customers’ consumption patterns,” *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan 2016.

[31] B. Genge, P. Haller, and I. Kiss, “Cyber-security-aware network design of industrial control systems,” *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–12, 2015.

[32] N. Svendsen and S. Wolthusen, “Connectivity models of interdependency in mixed-type critical infrastructure networks,” *Information Security Technical Report*, vol. 12, pp. 44–55, 2007.

[33] B. Genge and P. Haller, “A hierarchical control plane for software-defined networks-based industrial control systems,” in *2016 IFIP Networking Conference and Workshops*, May 2016, pp. 73–81.

[34] AIMMS, “Advanced Interactive Multidimensional Modeling System,” http://www.aimms.com/aimms/, 2016, [accessed August 2016].

[35] R. Sedgewick, “Algorithms in c, part 5: Graph algorithms,” *Addison Wesley Professional, 3rd ed.*, 2001.

[36] M. S. Kang and V. D. Gligor, “Routing bottlenecks in the internet: Causes, exploits, and countermeasures,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’14, 2014, pp. 321–333.

Béla Genge is a Marie Curie Fellow and Associate Professor at the Petru Maior University of Tg. Mures, Romania. He obtained his PhD in 2009 in network security from the Technical University of Cluj-Napoca, Romania, and acquired a 3-year experience as Post-Doctoral researcher at the Institute for the Protection and Security of the Citizen, Ispra, Italy (2010-2013). Since 2016 he is the Head of the Department of Computer Science at the Petru Maior University of Tg. Mures. He is an IEEE Member, and has authored several papers in peer reviewed journals including IEEE Transactions on Emerging Topics in Computing, IEEE Communication Surveys and Tutorials, IEEE Systems, Communications of the ACM, International Journal of Critical Infrastructure Protection, Security and Communication Networks. He serves as a TPC member for numerous international events including IEEE/IFIP Networking, ACM Workshop on Cyber-Physical Systems Security and PrivaCy, and the International Symposium for ICS and SCADA Cyber Security Research. His research interests include security and resilience of Smart Grids, optimal network design techniques, and anomaly detection systems.

Piroska Haller obtained her PhD from the Technical University of Cluj-Napoca, Romania in the field of distributed multimedia systems. She is currently an Associate Professor at the Petru Maior University of Tg. Mures, Romania and an IEEE Member. She has a large number of publications in journals and prestigious conferences including Elsevier’s Control Engineering Practice, IEEE Systems journal, the International Journal of Robotics and Automation, the International Journal of Critical Infrastructure Protection, and the Transactions of the Institute of Measurement and Control. Her research interests include networked control systems, design, optimization and development of large-scale distributed systems, and industrial system security.

Cristian-Dragoş Dumitru is an assistant professor at the Petru Maior University of Tg. Mures, Romania. He received his PhD in Electrical Engineering from the Technical University of Cluj-Napoca in 2011 and his M.Sc. in Advanced Control Automated Systems for Industrial and Energetic Processes from the Petru Maior University of Tg. Mures in 2005. His main teaching expertise includes: Renewable energy sources, Electrical Equipments, Electrotechnics, Electrical networks, Electrical power systems, Reliabilty and diagnosis, Distributed generation and smart grids. He is a member in a research center focused on energy management and electrotechnologies at the Petru Maior University of Tg. Mures. His research interests are focused on renewable energy sources, distributed generation and smart grids. He served as a reviewer for many journals and is actively involved in organizing the International Conference on Interdisciplinarity in Engineering (INTER-ENG) within the Petru Maior University of Tg. Mures. He authored or co-authored over 40 peer-reviewed scientific articles and conference papers, 3 books and contributed to 1 book-chapter. He is the co-inventor of one patent owned by the Petru Maior University of Tg. Mures.

Călin Enăchescu is a Professor within the Department of Computer Science, Petru Maior University of Tirgu Mures, Romania. He has a PhD in Artificial Intelligence, being involved in a large number of scientific projects related to practical applications of neural computing. His research interests include the applications of machine learning techniques in the field of security and resilience of industrial control systems.