C. Alcaraz, J. Lopez, and K-K. Raymond Choo, "Resilient Interconnection in Cyber-Physical Control Systems", *Computers & Security*, vol. 71, pp. 2-14, 2017.
http://doi.org/https://doi.org/10.1016/j.cose.2017.03.004
NICS Lab. Publications: https://www.nics.uma.es/publications

Resilient Interconnection in Cyber-Physical Control Systems

Cristina Alcaraz[1], Javier Lopez[1], and Kim-Kwang Raymond Choo[2]

[1]Computer Science Department, University of Malaga,

Campus de Teatinos s/n, 29071, Malaga, Spain

[2]School of Information Technology & Mathematical Sciences,

University of South Australia,Adelaide, South Australia

{alcaraz,jlm}@lcc.uma.es

raymond.choo@fulbrightmail.org

May 26, 2019

Abstract

Secure interconnection between multiple cyber-physical systems has become a fundamental requirement in many critical infrastructures, where security may be centralized in a few nodes of the system. These nodes could, for example, have the mission of addressing the authorization services required for access in highly-restricted remote substations. For this reason, the main aim of this paper is to unify all these features, together with the resilience measures so as to provide control at all times under a limited access in the field and avoid congestion. Concretely, we present here an optimal reachability-based restoration approach, capable of restoring the structural control in linear times taking into account: structural controllability, the supernode theory, the good practices of the IEC-62351 standard and the contextual conditions. For context management, a new attribute is specified to provide a more complete authorization service based on a practical policy, role and attribute-based access control (PBAC + RBAC + ABAC). To validate the approach, two case studies are also discussed under two strategic adversarial models.

Keywords: Structural controllability, Cyber-Physical Systems, Interconnection, Access Control, Resilience, Redundancy

1 INTRODUCTION

Taking into account our earlier work [1, 2, 3], this paper presents a secure decentralized interconection system composed of a cost-effective, self-healing approach based on redundant pathways [3], and autorization services for specific cyber-physical systems (CPS) (see Figure 1). These networks follow constructions given by *structural controllabilty* introduced by Lin in [4] and the *supernode theory* [5], in which the access control is centralized in a few proxies via the Internet [2]. The mission of these proxies is to provide access according to a set of factors: the roles of the subject, the type of action in the field, the security policies assigned for the access in an object and the contextual conditions. Precisely, it is the context management that differentiates this paper with respect to the previous ones [1, 2], as it not only focuses on the secure access control in the field but also on the network decongestion tasks during the self-healing processes, required to address threatening situations [1].

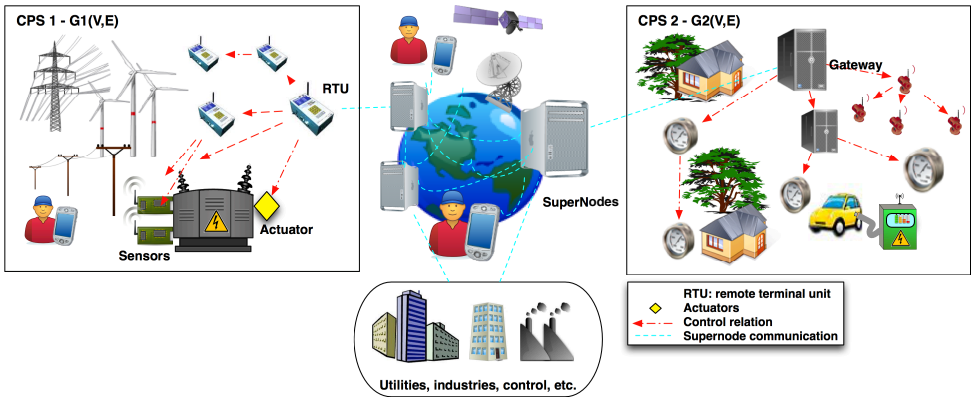

Figure 1: Interconnection of two cyber-physical systems through supernodes

As stated in [3], the redudancy of links is one of the most optimal and effective resilience measurements for critical contexts. For this reason, we adapt the mechanism proposed in [3] to remodel the control in CPS with a direct interface to the gateways and with indirect connection to the supernodes through them. These gateways (e.g. servers, remote terminal units (RTU)) are in charge of supervising any incoming and outgoing communication, as well as anomalies at the respec-

tive CPS. The result, is a complex interconnection system (see Figure 2) based on policy enforcement points (PEP) whose petitions (based on authentication tokens obtained from each infrastructure working in the interconnection) must be processed by the closest policy decision points (PDP); i.e. the supernodes. These PDP manage the access through their automated authorization mechanisms, regulated in part, by a dynamic policy, role and attribute based access control (PBAC + RBAC + ABAC) [6] under the least privilege scheme established by the IEC-62351-8 standard in [7].

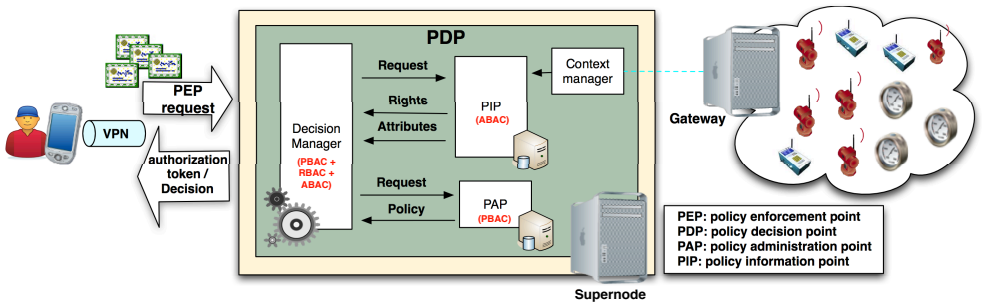

Figure 2: General architecture based on the work [2]

The IEC-62351-8 corresponds to the IEC-62351 series [8] which specifies peer-to-peer security in control systems and the protection of the communication channels. This standard suggests the RBAC model as a potentially efficient mechanism for large control distributions, which together with the security polices of the IEC-62351-3 [9] and the contextual attributes related to the criticality of the context, allows authorized access to restricted objects in the field (e.g. sensors, actuators, meters and IEC-61850 objects). Moreover, through PBAC + RBAC it is possible to reallocate system controls and their security as defined by the organization policy, where the aim is: (i) to launch authorization solutions in power systems under the condition of roles-rights to subjects or entities (either users, software processes or IEC-61850 objects [10]); (ii) propel policy and role-based access control in critical systems; and (iii) enable diversity and interoperability between components of a CPS [11].

With RBAC it is also possible to permit dynamic separation of duties (DSD) to facilitate the activation of secondary roles and the rapid assistance in critical situations [12]; e.g. assume as secondary roles those labeled as Operator and/or SECADM, and both with control rights. In these circumstances, the system must temporarily deny access to other general-purpose entities to avoid saturating the communication channels, and leave functioning the corresponding control entities

in the field (Operators and SECADM). However, although these functionalities are essential for the dynamic access in critical situations, the access control does not completely ensure resilience. They must be complemented with automatic self-healing mechanisms to ensure defense and protection of their own control.

Until very recently there have been no optimal restoration solutions that reach linear times and in all cases. The vast majority of the solutions have been mainly based on tree-like structures for general-purpose networks without considering the specific requirements of the context and its criticality level. Examples of this are, for instance, the nice tree decomposition structures to facilitate the redundancy of driver nodes [13]; or tie-set structures to manage anomalies [14]. A variant of the latter is the rapid spanning tree protocol (RSTP) as an evolution of the traditional spanning tree protocol (STP), which can be applied to handle traffic loops and broadcast congestion in mesh topologies [15]. However, recent work in the field of structural controllability is taking a drastic turn towards this type of research to incorporate more dynamic approaches, where redundant pathways are increasingly demonstrating their ability to respond to extreme situations in optimal times [3]. Given this, we improve upon the work in [1] by incorporating redundant pathways reaching linear and quadratic orders similar to [3], but this time remodeling the system to guarantee multiple CPS interconnections at all times, and through gateways.

To conceptually represent several interconnected CPS, the architecture depicted in Figure 1 can be formally characterized through graph theory to embed structural controllability together with its driver nodes, which are obtained from the POWER DOMINATING SET (PDS) problem introduced by Haynes *et al.* in [16]. This new concept, also considered by Kneis in [17], is supported by the specific structures of the power grids and their monitoring systems; this being the main reason why we apply the PDS problem to our studies instead of traditional maximum matching, described in [18]. As a result, a graphical representation is given to interconnect several CPS through the different gateways whose nodes are also part of the set of driver nodes, responsable for permitting the access according to the 'real state' of the context. To compute this state, this paper proposes a new indicator of criticality related to the dynamic variations of the control, the value of which is complementary to the observation level outlined in [2]. In this way, it is possible to detect the case in which structural controllability of a network deteriorates completely with respect to its original release, and regardless of whether its observation level in state t has been restored once, or even, several times in the past. In these extreme cases, a re-computation of the entire control network can be required to restore the original control relationships where control loads and

their dynamics need to be transferred by predetermined routes.

Given this, our main contributions are:

- the modeling of a redundancy-based self-healing mechanism, principally centralized in a node to interconnect the entire system via the PDP. To do so, we consider the works in [3, 2] together with the potential features of the IEC-62351-3 and -8 to address PBAC + RBAC;
- the provision of a new context parameter (as part of the actions of ABAC) to manage the severity degree after perturbations, introducing for this the concept of edge betweeness centrality and the maximum load capacity (both described in the next section); and
- the analysis and demonstration of the capacities of DSD through two case studies under two different adversarial models.

The rest of this paper is organized as follows. Section 2 introduces the preliminary concepts, contextualization of the studies and the adversarial models to later be applied in Section 4. In this section, we formalize the self-healing approach taking into account the work in [3], whose practical validation is later presented in Section 5. Finally, Section 6 concludes the paper and outlines future work.

2 CONTEXTUALIZATION AND ADVERSARIAL MODELS

As mentioned, one easy way of addressing the control of large distributions is through graphical representations based on graph theory, where the control is subject to a subset of nodes known as driver nodes. For the construction of these graphs, we depend on the technical capacity of *structural controllability* [4] whose basis is an extension to the control capacities given by Kalman in [19]. Concretely, the concept is based on a directed weighted graph $\mathscr{G}_w(\mathbf{A}, \mathbf{B}) = (V, E)$ such that A depicts the topological map of the network through a non-zero weighted matrix of size $n \times n$; B a matrix ($n \times m$, $m \leq n$) containing the set of driver nodes with the ability to inject control signals into the rest of the network; V the vector of nodes contained in A; and E the set of connected edges. In real contexts, this representation would correspond to a set of cyber-physical elements in V, including those driver nodes in B such as servers and RTU, and the communication links ($\in E$) between the different devices.

As stated in [3], $\mathscr{G}_w(V, E)$ is a weighted graph with cycles, capable of showing the control's dynamics (denoted as control loads) between the different nodes.

This type of variable, based on the edge betweeness centrality (EBC), displays the potential of the nodes to transmit data from one point to another [20], the value of which can be computed as:

$$E_{BC}(e) = \sum_{s,t \in V} \frac{\delta(s,t \mid e)}{\delta(s,t)} \tag{1}$$

where $\delta(s,t)$ includes the number of shortest (s,t)-paths and $\delta(s,t \mid e)$ the number of paths passing through edge e. From Equation 1, E_{BC} comprises a matrix of size $n \times n$ containing the shortest paths that pass through a given edge, such that, edges with the highest centrality participate in a large number of shortest paths. This also means that the nodes with the highest centrality and interaction strength participate with greater frequency and probability in the control and transference of commands, measurements and alarms between peers [20], resulting in a new concept called *control load capacity* (CLC) [3].

To extract the minimum set of driver nodes (henceforth denoted N_D and also included in B), the concept of structural controllability has to adopt the power dominance concept given by Haynes *et al.* in [21], which was later retaken by Kneis *et al.* in [17] to sketch the concept itself in two main observation rules:

OR1 *A vertex in* $\mathbf{N}_D$ *observes itself and all its neighbors*, where **OR1** is related to the DOMINATING SET problem.

OR2 *If an observed vertex v of degree* $d \geq 2$ *is adjacent to* $d-1$ *observed vertices, then the remaining unobserved vertex becomes observed as well*, such that **OR1** $\subseteq$ **OR2**.

As a result, we obtain an interconnected network system composed of a selective set of driver nodes and observed nodes, all of them responsible for monitoring the underlying infrastructures, such as power generators, pylons or motors. As these underlying infrastructures and their monitoring systems follow constructions based on power-law, in which a subset of nodes contains the maximum degree (d^+) of the network (e.g. substations), our conceptual graphs are based on distributions of the type $y \propto x^{\alpha}$. An example of this type of distribution is the Power-Law Out-Degree (PLOD) defined in [22], where the connection probability must be low (e.g. $\alpha = 0.1$) to illustrate more realistic scenarios similar to power grids and their monitoring systems [23]. As for the decentralization of systems and the interconnection of networks (e.g. two or more PLOD-based CPS), we adopt the supernode theory [5]. In this context, each PEP request must be managed by the closest PDP, which act as the main proxies between the observed world and the real world, and provide peer-to-peer communication from any geographical location (see Figure 1). However, the connectivity of PDP to the application context

is not completely direct, it has to pass through the gateways located at each substation (see Figure 2), responsible for transferring all the control and supervising the accessibility and criticality of the observation context.

Part of this information is also managed by the context managers included inside the supernodes (i.e. in the PDP − see Figure 2) to influence in the decision processes and authorization in the access to critical devices. In this way, any access request, based on authentication tokens, is not only constrained to access restrictions but also to the type of degradation of the application context, probably caused by non-delivered or intentional influences. In our experiments, we model scenarios with high levels of perturbation where adversaries are able to exploit massive attacks, targeting more than 20% of the network nodes and following a weak adversarial model whose threats can be of targeted or causal nature, as classified in [3]. Specifically, we (i) isolate a set of random nodes removing all their links [**T1**], (ii) eliminate a few (not all) edges of some arbitrary nodes [**T2**], and (iv) randomly add a few edges in some random nodes [**T3**]. From a target point of view, we also isolate those nodes with (v) the highest degree (i.e. the hubs such that $\forall v_i \; max(d^+_{v_i} + d^-_{v_i})$) [**R1**] and with (vi) the highest strength (i.e. the highest CLC such that $\forall v_i \; max(\sum_{i \in E}(E_{EB}(v_i,i) + E_{EB}(i,v_i)))$) [**R2**], in addition to objectively removing a few edges with (vii) the highest peaks of centrality [**R3**].

3 SELF-HEALING: INITIAL CONDITIONS AND RESTORATION

This section presents a reachability-based self-healing mechanism which adapts the redundancy capacities given in [3], with the ability to reconnect with the gateways after perturbation. Concretely, several ways of relinking an affected device were explored in [3], using, for example, a reconnection via a grandfather, father or brother driver node; however, our studies mainly focus on reconnection via a father driver node to simplify the scope of the research. This also means that the new redundant pathways are included within a new graph $\mathscr{G}^r_w(V,E')$ of the same size as $\mathscr{G}_w(V,E)$ such that $\mid E' \mid \geq \mid E \mid$. Taking into account these potential features for the resilience, three initial conditions should also be considered:

[C1] Any restoration process must verify the connectivity to the gateway, respecting the directionality between the gateway and its children.

[C2] Any relink process must consider the power-law nature of the underlying infrastructure and respect the interaction strength established within the network.

[C3] The two observation rules (**OR1** and **OR2**) must always be satisfied according to the two definitions given in Section 2. Part of this verification includes the compliance of **OR2** following the following two conditions:

- **[C3.1]** If there exists an unobserved node u and it is part of N_D, then a driver node $n_d \in N_D$ is required such that: ($\mid O \mid \geq 2$ and $\mid N_D \mid \geq 0$) or ($\mid O \mid = 0$ and $\mid N_D \mid \geq 0$), where O represents the set of observed nodes controlled by an n_d.
- **[C3.2]** If there exists an unobserved node $u \notin N_D$, then a driver node $n_d \in N_D$ is required such that ($\mid O \mid \geq 1$ and $\mid N_D \mid \geq 0$) or ($\mid O \mid = 0$ and $\mid N_D \mid = 0$).

Assuming that the comissioning phase has been successful after the generation of $\mathscr{G}_w^r(V,E)$ [3], Algorithm 3.1 shows the self-healing mechanism proposed in this paper. The mechanism aims first to find a redundant pathway in $\mathscr{G}_w^r(V,E)$ such that the new pathway is part R_e, being R_e the current set of active edges in E'. However, when this optimal solution is not possible or suitable, either because there is no new pathway or the existing redundant pathways are already included in R_e, the system has to find another new driver node with the minimum diameter capable of complying with the condition **C2**. But when neither of these solutions − both of them contemplated in [3], leading to linear and quadratic solutions, respectively − are effective, the system has to resort to a direct connection via the gateway, and without having to consider the type of node and its surroundings (**C3.1** and **C3.2**). Moreover, although **OR1** is always guaranteed at this point and regardless of the different options given by Algorithm 3.1, the compliance of **OR2** is not always ensured. Any suspicion of a child infringing **OR2** forces the system to launch a verification process of **OR2** through the VERIFYOR2, also specified in [13] with a computational cost of $\mathrm{O}(n^2)$ if $n \sim \mid \mathbf{N}_D \mid$ in the worst case scenario.

The correctness proof of Algorithm 3.1 is demonstrated when the following three requirements are met:

- the algorithm guarantees structural controllability and power dominance without infringing the conditions **C1** and **C2** (*restoration*);
- the algorithm is able to finalize in a finite time (*termination*); and
- the algorithm is able to guarantee restoration and termination at all times (*validity*).

Algorithm 3.1: SELF-HEALING MECHANISM $(\mathscr{G}_w(V,E),\mathscr{G}_w^r(V,E),\mathbf{N}_D,gateway,R_e)$

```
output (N_D, G_w(V,E), G_w^r(V,E), N ← V)
local S ← ∅, or_2 ← false ;

while (N ≠ ∅ and v_i ≠ gateway)
  do
{ v_i ← randomly choose a node v_i in N;
{G_w(V,E), G_w^r(V,E), done} ← REDUNDANCY_RR2(G_w(V,E), G_w^r(V,E), N_D, R_e, v_i)[a];
if ( not done)
    then { comment: Direct reconnection to the gateway and verification of the fulfilment of C3.
           G ← obtain the children of the gateway in A;
           N_DG [b] ← G ∩ N_D;
           O_G [c] ← G \ N_DG;
           if (((v_i ∈ N_D) and ((| O_G | ≥ 2 and | N_DG | ≥ 0) or (| O_G | = 0 and | N_DG | ≥ 0)))
           ((v_i ∉ N_D) and ((| O_G | ≥ 1 and | N_DG | ≥ 0) or (| O_G | = 0 and | N_DG | = 0))))
             then
           {done ← true ;
           if ( not done)
             then {N_D ← v_i ∪ N_D;
           {G_w(V,E), G_w^r(V,E)} ← CONNECT TO GATEWAY_RR2(G_w(V,E), G_w^r(V,E))[d];
           G ← obtain the children of the gateway in A;
           N_DG ← G ∩ N_D;
           O_G ← G \ N_DG;
           if ((| O_G | = 1) and (| N_DG | ≥ 2))
             then
           { o_i ← obtain the observed node in O_G;
             N_D ← o_i ∪ N_D;
             O_i ← obtain the children of the node o_i in A;
             if (O_i ≠ ∅)
               then
             or_2 ← true ;
return (VERIFYOR2(G(V,E), N_D, or_2)))[e]
```

[a] REDUNDANCY$_{RR_2}$ corresponds to the process of relinking via a father driver node as declared and specified in [3]. This call also contains the suboptimal case where no father driver node is able to reconnect, using for this, the minimum diameter. This procedure extracts the minimum set of driver nodes with the highest degree ($max(d_{v_i}^+ + d_{v_i}^-)$) and the highest strength ($max(\sum_{i\in E}(E_{EB}(v_i,i)+E_{EB}(i,v_i)))$) as defined in Section 2 and declared for **C2**.

[b] N_{D_G} refers to the set of children driver nodes of the gateway.

[c] O_G corresponds to the set of children observed nodes of the gateway.

[d] CONNECT TO GATEWAY$_{RR_2}$ reconnects the unobserved node to the gateway and seeks the new redundant pathway via a father driver node as specified in [3].

[e] VERIFYOR2 is a verification procedure of **OR2** defined in [13].

As the system is always able to find a driver node capable of establishing connectivity, either through a redundant link, a driver node with the minimum diameter (with the highest degree and strength), or through the gateway, the former requirement is satisfied. This also signifies that **OR1** is met, and **OR2** is proved by verifying the conditions given in **C3.1** and **C3.2**, and, in the worst scenario, by executing VERIFYOR2 [13]. Regarding the termination of the algorithm, we first

define the initial and final conditions, to later specify the base cases required for the induction:

Pre-condition: there are nodes in V that satisfy $U \neq \oslash$ such that $U \leftarrow F_{v_i} \cap N_D$, being F the set of father nodes of a given vertex v_i.

Post-condition: $\forall v_i \in V$, $U = \oslash$ such that $U \leftarrow F_{v_i} \cap N_D$, and both **OR1** and **OR2** are correctly met (**C1**, **C2**, **C3**).

Case 1: $\mid U \mid = 1$, and there is a redundant pathway (**optimal solution**) that ensures structural controllability according to the commissioning phase specified in [3]. In these circumstances, the system (i) activates the reconnection with the father driver node ($n_{d_{father}}$) of the affected node v_i in U such that $(n_{d_{father}}, v_i) \in E$; (ii) updates $\mathscr{G}_w(V,E)$ taking into account $\mathscr{G}_w^r(V,E)$; and (iii) adds the new link in R_e for future repairs. This new reconnection with an $n_{d_{father}}$ makes the system update $U \leftarrow \{v_i\} \setminus U$, complying with the post-condition.

Case 2: $\mid U \mid = 1$, there is not an optimal solution that guarantees **C1**, **C2** and **C3**, probably because the redundant edge is being used (in R_e). To resolve this, the system tries to find a driver node with the minimum diameter and with the highest centrality and degree [3], thereby ensuring the power-law degree. If the system is able to find an n_d in these conditions, then it reconnects $(n_d, v_i) \in E$, (ii) and updates $\mathscr{G}_w(V,E)$ and $\mathscr{G}_w^r(V,E)$ to include the new redundancy with respect to one of its father driver nodes [3]. Once the structural controllability has been repaired, the system updates $U \leftarrow \{v_i\} \setminus U$ to meet the post-condition. But in the extreme case where this first solution is not possible, the next alternative would be to pin up the communication via the gateway, forcing the system to verify the compliance of **OR2**, through **C3.1** and **C3.2**, or through VERIFYOR2.

Case 3: $\mid U \mid = 1$, there is neither a redundant pathway nor an $n_d \in N_D$ with the minimum diameter that satisfies **C2**. In these cases, the system considers the alternative seen in Case 1 together with the verification process of **OR2** to force the dominance. However, if after the reparation through $(n_{d_{gateway}}, v_i) \in E$ and updating of $\mathscr{G}_w(V,E)$ and U under the same conditions as Case 2, there exists a child driver of the gateway (included in the set C) that fulfils with $\mid O_G \mid = 1$ and $\mid N_{D_G} \mid \geq 2$, such that $N_{D_G} \leftarrow C \cap N_D$ and $O_G \leftarrow C \cap N_{D_G}$ (the observed children by the gateway), then the system has to include $n_i \in O_G$ in N_D to comply with **OR2**. However, in the worst case scenario, this new change entails checking whether **OR2** has been perturbed in the rest of the network by using the variable or_2, which acts as an indicator in VERIFYOR2, as detailed in [13].

Induction: in step k of the *while* (with $1 \leq k \leq \mid V \mid$) with $|N_D| \geq 1$, we randomly select a node v_i in V so as to determine the observation degree with respect to surroundings ($U \leftarrow F_{v_i} \cap N_D$). If $U \neq \oslash$, the system has to realize in which cases it is found to update $\mathscr{G}_w(V,E)$, $\mathscr{G}_w^r(V,E)$, R_e and N_D according to the three base cases mentioned above. In the next state, with $k-1$, the procedure adopted is still valid, indicating that the post-condition has not yet been satisfied (because $k \leq \mid V \mid$), and the loop must be repeated for the next state k until $k = 0$. When this occurs, the variable or_2 is checked to determine the launching of VERIFYOR2 (its correcteness proof and termination are specified in [13]). In either case, the proof concludes, which means that the post-condition is true and Algorithm 3.1 ends.

Therefore, the latter requirement, associated with the validity, is also met since Algorithm 3.1 terminates and guarantees **OR1** and **OR2** at all times, complying further with **C1**, **C2** and **C3**. As for the computational costs, Algorithm 3.1 may reach the optional values $\mathrm{O}(n)$, as long as R_e can be updated with an existing and unique edge in E'. To the contrary, the worst case scenario is subject to quadratic values, due in part to the computation of the minimum diameter with the highest degree and interaction strength (a cost of $\mathrm{O}(n^2)$) [3] and the VERIFYOR2 [13] (with an order of $\mathrm{O}(n^2)$). The spatial cost may also increase if the restoration phase depends on Case 3, in which at least two new drivers in N_D may appear in the worst case scenarios.

4 CONTEXT ATRIBUTES: SEVERITY AND OBSERVABILITY

A new functionality to the self-healing mechanism proposed in Section 2 is presented in this section, the goal of which consists in allowing the system to know when and how its resilience capacities must be activated. These capacities are not only restricted to the CPS itself, but rather they are expanded throughout the entire interconnection system in which each PDP must be able to dynamically manage the access according to the 'real state' of the application context. In this way, extremely critical scenarios can be only assisted by specialized entities with specific roles and rights. Some of these roles and permissions have already been defined by the IEC-62351-8 standard, which comprises: (i) seven roles for power and control applications, (ii) 32.760 reserved for security applications within the IEC-62351, and (iii) 32.767 for private use [2]. From these roles, we only consider the first seven whose assignations are also declared in Table 1.

Table 1: Roles and rights belonging to IEC-62351-8

	Rights associated with IEC-62351-8 roles										
	View	**Read**	**Dataset**	**Reporting**	**Fileread**	**Filewrite**	**Filemgnt**	**Control**	**Config**	**Settinggroup**	**Security**
Viewer[a]	✓			✓							
Operator[b]	✓	✓		✓				✓			
Engineer[c]	✓	✓	✓	✓		✓	✓		✓		
Installer[d]	✓	✓		✓		✓			✓		
SECADM[e]	✓	✓	✓			✓	✓	✓	✓	✓	✓
SECAUD[f]	✓	✓		✓	✓						
RBACMNT	✓	✓					✓		✓	✓	

[a] **Viewer**: capacity to view data objects.

[b] **Operator**: capacity to lead control actions, and handle data objects and values.

[c] **Engineer**: capacity to access databases and files, configure servers, and handle data objects and values.

[d] **Installer**: capacity to write files, configure servers, and handle data objects and values.

[e] **SECADM**: ability to manage users-roles-rights, security setting. In relation to this role, **RBACMNT** only manages roles and rights.

[f] **SECAUD**: capacity to read audit logs, and audit the system.

However, the dynamic assignation of roles in critical contexts obliges us to incorporate an expert system capable of handling not only the different roles of each entity together with its different access policies in each device and the CPS, but also the access attributes according to the context. To do this, our approach expands the rule-based expert system proposed in [2] and its observability-based context management module, to add a new protection functionality in the DSD [12]. This new functionality is related to the level of deterioration of the network, the value of which is computed according to the maximum load capacity of the whole network [20]:

$$H_{i,j} = (1+\alpha) \times L^0_{i,j} \tag{2}$$

of size $n \times n$ and where α represents a tolerance parameter with value $\alpha > 0$ and $L^{t\geq 0}_{i,j} \leq H_{i,j}$, being $L^{t\geq 0}_{i,j}$ the load capacity of $\mathscr{G}_w(V,E)$ at state t. Through H it is possible to map the entire network and determine the redistribution degree of the control loads, the diameter variation between two peers and the deviation of the shortest paths. This also means that even if the system is under continuous threat and process of restoration, the control loads may end up completely disintegrated and deviated with respect to the original control loads, probably requiring the general repair of the entire system. To control this anomalous scenario, two context attributes are considered in this paper: the *observability degree* and the *severity degree*. When the observability degree is low but the severity degree high, the

problem can be detected; whilst when the observability degree is high and the severity degree low, the restoration can remain in a local state without observing a great disintegration of control.

For the sake of clarity, the former attribute uses two fundamental criticality thresholds: **MaxCCont** and **MinCCont**, both declared in [2]. Their values delimit the level of accessibility to particular cyber-physical elements, and establish the border (**MaxCCont**) to activate the DSD accordingly. This also means that the value of the context and its limitation to **MaxCCont** must periodically be monitored by the context managers integrated in each PDP, testing the criticality degree of each CPS and calculating the accessibility degree of the objects demanded. The computation of these data is based on the information received from their closest gateways, which estimate the rate of unobserved nodes through Algorithm 4.1. To the contrary, **MinCCont** states the critical point at which the system must immediately invoke a restoration of the affected CPS, avoiding any type of access, including the secondary roles so as not to collapse the system.

Algorithm 4.1: UNOBSERVED NODES $(\mathscr{G}(V,E),\mathbf{N}_D)$

output (U)
local $n_d, U \leftarrow V \setminus \mathbf{N}_D, DS^a \leftarrow \oslash, N^b \leftarrow \oslash$;
while $(U \neq \oslash)$
do {
  Randomly choose a vertex $n_d \in \mathbf{N}_D$;
  if $n_d \notin (\mathbf{N}_D \cup N)$
    then {
      $DS \leftarrow DS \cup \{n_d\}$;
      for each $v \in V$
        do {
          if $(n_d, v) \in E$
            then {
              $N \leftarrow N \cup \{v\}$;
              $U \leftarrow U \setminus \{v\}$;
            }
        }
      $U \leftarrow U \setminus \{n_d\}$;
    }
}
return (U)

[a] DS comprises N_D that satisfies with **OR1**.
[b] N includes the neighborhood of a determined node.

Regarding the degradation of the network, several thresholds of gravity can be defined, ranging from the least serious threshold (**MinSev**) to the most critical (**MaxSev**), and the values of which are subject to $L_{i,j}^{t\geq 0} > H_{i,j}$. So when $L_{v_i,v_j}^{t\geq 0}$, belonging to two network nodes (v_i and v_j), clearly exceeds its value to H_{v_i,v_j}, it is easy to confirm that the initial configuration for both nodes in $t = 0$, is completely degraded. If in addition, we calculate this value for each node in V, we can compute the rate of degradation for the entire network, and therefore its severity

level. This level could even allow the system to restrict the access to avoid congestion and activate the DSD to attend to critical situations. Thus, members with specific roles could take on certain control rights to lead specific actions in devices whose security policies can follow the IEC-62351-3 standard − declaring the type of key exchange algorithm (TLS_DH/DHE/RSA), encryption (AES-128, 3DES, RC4-128) and hash function with SHA. As a result, each PDP can then manage the access according to the type of role, rights, attributes related to the context and the security policies defined for each protected device, resulting in an RBAC + ABAC + PBAC, and helping the underlying system rapidly assist any situation in the field.

Extreme situations, e.g. the rate of observation $\leq$ **MaxCCont** and/or the rate of degradation $\geq$ **MinSev**, are led by specific control entities or through DSD. In these circumstances the system must adopt an access policy, such as: *to only allow the access to Operators and SECADM, and temporarily refuse access to other entities (e.g. Viewers, Engineers or Installers)*, thereby avoiding bottlenecks and saturation of the channels. All these parameters related to the subject (roles, rights, and action in the destination), the object and its context are processed by the decision managers of each PDP, equipped with a rule-based expert system written in JESS (Java™ Expert System Shell) for the automation. However, to integrate the new context attribute within the rule-based engine, the construction of <**rule**> **:=** <**condition**>⇒<**action**> (where <condition> holds the predicates belonging to <subject><object>), has been extended from the original work [2] to add a new predicate associated with the <object>:

$$<\text{severity}> := \textbf{MinSev} \leq rate_{deg} \leq \textbf{MaxSev},$$

such that $rate_{deg}$ refers to the rate of network degradation admissible by the system. Concretely, we declare in JESS, twelve new states for the eight rights outlined in Table 1 and in [2], and modeled as follows:

Control: we define three further exceptional cases for control:

- Normal situation: <severity>:= 0.0 < **MinSev**.
- Critical Situation (DSD): <severity>:= **MaxSev** $\geq rate_{deg} \geq$ **MinSev**.
- Extremely critical situation (no access): <severity>:= **MaxSev** $\leq rate_{deg}$.

For the rest of the rights: <severity>:= 0.0 $\leq$ *priorRight*, where *priorRight* specifies the accepted severity threshold for a determined right (e.g. priorControl, priorRead, priorView, etc.).

5 RESULTS AND DISCUSSION

For the practical validation of the self-healing approach described in Section 4 and the interconnection architecture described in [2], a set of experiments in Matlab and Java were planned according to the different kinds of attacks detailed in Section 2. Specifically, the Matlab part corresponds to the implementation of two types of scenarios based on the interconnection of three PLOD distributions (three CPS $-$ CPS_1, CPS_2 and CPS_3) with $\alpha = 0.1$, and the Java part comprises the architecture of PDP taking into account the IEC-62351-8 standard. The CPS were produced for small and large distributions with 50, 300 and 900 nodes, where all control was centralized in their respective gateways and the access relies exclusively on seven software entities. These entities, whose profiles are characterized in Table 2, were implemented to periodically request access in one of the three CPS, taking into account their privileges and the type of action in the destination nodes. For the authentication of these entities and the management of access token in each PDP, the simulation required of a LDAPv3 server linked to the Apache Directory Studio^{TM} [24] under the RFC-2798 [25] and the attribute *inetOrgPerson:userCertificate* to manage X.509 certificates.

Table 2: Software entities together with their roles and permissions (IEC-62351-8)

Entity	Primary rol	Sec. rol	Access to	Action	CCont - *priorRight*	Severity threshold
E1	Operator	–	$CPS_{1,2,3}$	Control	$priorControl \geq 0.10$	$0.0 \leq rate_{deg} \leq 90.0$
	Operator, SECADM (DSD)	–	$CPS_{1,2,3}$	Control	$priorControl \geq 0.10$	$20.0 \leq rate_{deg} \leq 90.0$
E2	SECAUD	–	$CPS_{1,2,3}$	Read	$priorRead \geq 0.60$	$0.0 \leq rate_{deg} \leq 70.0$
E3	Installer, Operator	–	$CPS_{1,2,3}$	Filewrite	$priorFilewrite \geq 0.10$	$20.0 \leq rate_{deg} \leq 80.0$
E4	Installer, SECADM	–	$CPS_{1,2,3}$	Report	$priorReport \geq 0.30$	$20.0 \leq rate_{deg} \leq 80.0$
E5	Engineer, Installer Viewer, Operator	–	$CPS_{1,2,3}$	Config	$priorConfig \geq 0.10$	$20.0 \leq rate_{deg} \leq 80.0$
E6	Viewer	–	$CPS_{1,2,3}$	View	$priorView \geq 0.60$	$0.0 \leq rate_{deg} \leq 70.0$
E?	–	–	$CPS_{1,2,3}$	–	–	–

To model realistic scenarios, we randomly assigned roles to the control devices (e.g. sensors, actuators, servers and RTU) also under arbitrary security policies of the IEC-62351-3. Each experiment was designed for 20 minutes, where more than 20% of the nodes of the network were massively perturbed each time. The first experiment focused on the arbitrary combination of target attacks ([**T1**, **T2**, **T3**]), whereas the second experiment was planned for random attacks of type [**R1**, **R2**,

R3]). For the context management, we establish **MinCCont** $<$ **MaxCCont** $<$ 100.0% as specified in [2], such that 100.0% states the best case scenario in which the risks to isolation of nodes become insignificant or null; whereas **MinCCont** delimits the point of major criticality of the system.

As for severity thresholds, we assume that **MinSev** = 20% refers to the threshold where the system needs to activate the DSD, **MaxSev** = $\{60\%, 70\%, 80\%\}$ as unstable severity levels, **MaxSev** = 80% as critical situation, and **MaxSev** = 90% as completely disintegrated scenarios. For example, we assume that Operators and SECADM (see Table 2) are able to enter in the requested field if and only if **MinSev** $\leq$ 0.0%, and **MaxSev** $\leq$ 90%; in contrast, Viewers are constrained to **MinSev** $\leq$ 0.0% and **MaxSev** $\leq$ 70% with preference given to those primary/secoundary roles based on Operators and SECADM in critical situtations (**MinSev** $\leq$ 20%, and **MaxSev** $\leq$ 90%). Moreover, each entity defined in Table 2 is not only limited to the criticality of the context but also to the reachability of a destination node from the gateway, denying all those accesses that may collapse the communications. This feature was also described in [2], the value of which can be computed through the observation rate and the diameter, and both restricted according to the type of operation in the field. Namely, this restriction is declared as *priorRight* in Table 2 and in [2], the value of which is linked to the type of permitted action, and in relation to the information assigned in Table 1 corresponding to IEC-62351-8.

Table 3 together with the figures, characterizes the results obtained from the two experiments designed: perturbation of target nodes and arbitrary nodes. Each experiment computes a set of data such as the number of access requests, the rate of normal access, denied access and the DSD. Observing Figures 3 and 4, it is also possible to see that the system is able to self-heal except for those small networks, where the observation degree and the global efficiency (the inverse of the average shortest path, whose value is inversely related to the path length) practically become null. The diameter, to the contrary, remains in continuous change, indicating the influence of the attacks and effectiveness of the restoration mechanism specified in Section 4. For large distributions, the behavior is just the opposite. The severity degree reaches extreme values due to the frequency of the threats and the type of threat ([**T1**, **T2**, **T3**]), whereas the observation degree of the network reaches optimal values, close to **MaxCCont**. This feature reaffirms our initial findings: *the observation degree can become satisfactory but the predetermined*

Table 3: Target and random attacks: small, medium and large networks

		Entities taking access to restricted networks						
	Access	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E?**
Target attacks	**Network 1 - 50 nodes**							
	Total	66	48	74	65	73	52	66
	Normal	3.030	0.0	2.702	3.076	5.479	0.0	0.0
	Denied	96.969	100.0	97.297	96.923	94.520	100.0	100.0
	DSD	0.0	0.0	100.0	100.0	100.0	0.0	0.0
	Network 2 - 300 nodes							
	Total	68	65	53	91	68	74	65
	Normal	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	Denied	100.0	100.0	100.0	100.0	100.0	100.0	100.0
	DSD	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	Network 3 - 900 nodes							
	Total	80	68	57	60	64	49	68
	Normal	16.250	0.0	17.543	11.666	17.187	0.0	0.0
	Denied	83.750	100.0	82.456	88.333	82.812	100.0	100.0
	DSD	0.0	0.0	100.0	100.0	63.636	0.0	0.0

	Access	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E?**
Random attacks	**Network 1 - 50 nodes**							
	Total	28	37	47	54	45	32	38
	Normal	21.428	5.405	4.255	1.851	13.333	0.0	0.0
	Denied	78.571	94.594	95.744	98.148	86.666	100.0	100.0
	DSD	0.0	0.0	100.0	100.0	100.0	0.0	0.0
	Network 2 - 300 nodes							
	Total	33	42	43	43	40	37	43
	Normal	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	Denied	100.0	100.0	100.0	100.0	100.0	100.0	100.0
	DSD	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	Network 3 - 900 nodes							
	Total	34	33	34	37	32	49	40
	Normal	2.941	0.0	0.0	0.0	0.0	0.0	0.0
	Denied	97.058	100.0	100.0	100.0	100.0	100.0	100.0
	DSD	0.0	0.0	0.0	0.0	0.0	0.0	0.0

control links (to transfer the main control loads) can completely disintegrate requiring a complete restoration of the entire system. Table 3 also shows the ability of the system to activate the DSD mechanism when **MaxCCont** and **MinSev** are surpassed. The entities **E3**, **E4** and **E5** are precisely those software agents capable of activating their secondary roles to assist in extreme scenarios (see Table 2).

Both Figure 3 and Figure 6 present similar results to previous ones but, this time attacking a combined number of nodes of types [**R1**, **R2**, **R3**]. The results show that the DSD is only activated for entities **E3**, **E4** and **E5**, and for small networks. However, the approach proposed in this paper is quite effective for large scenarios in which the reconstruction of the control is concentrated on redundancy

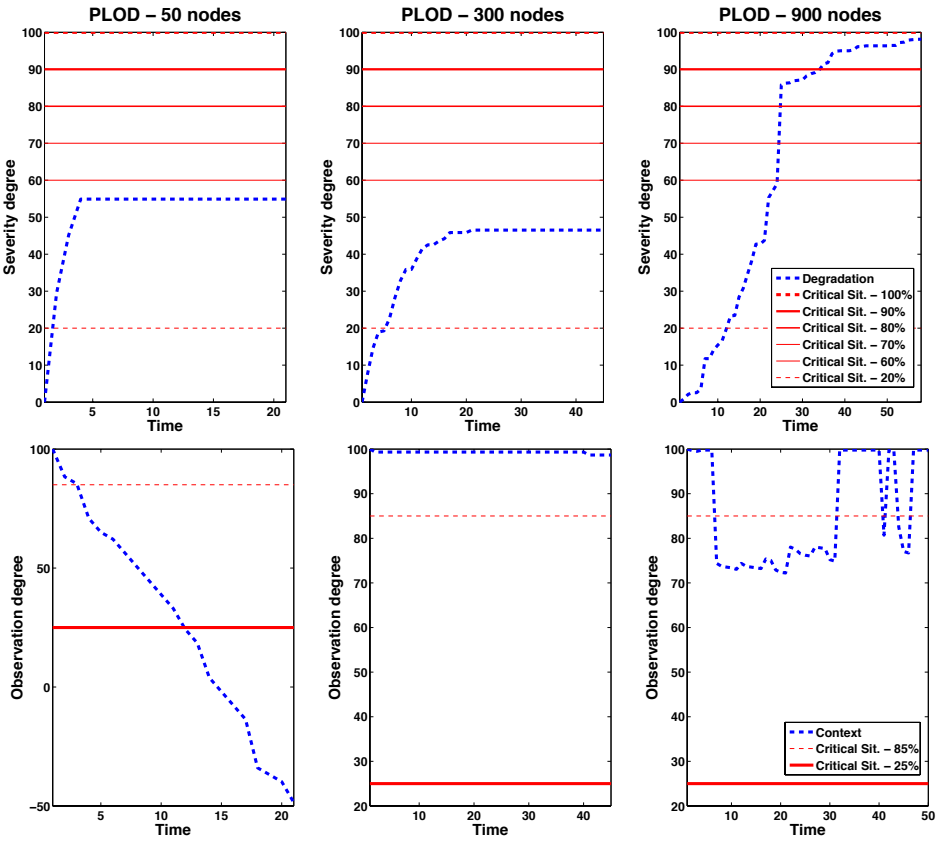

Figure 3: Target attacks: severity and observation

measures, and this capacity of resilience can be due in part, to the implicit network connections as outlined in [20, 26]. For this reason, it is recommended that restoration mechanisms are configured, taking into account the dimension of the networks and the frequency of the repairs, to be configured as part of the maintenance and security policies. It would also be good practice to force the system to execute repair measurements in relation to the warnings produced by alarm managers (probably integrated inside PDP or gateways), and schedule maintenance following strict auditing procedures.

Moreover, the two experiments detail that the accesses effectuated by entities **E6** and **E?** are always refused since entity **E?** is not known by the authorization

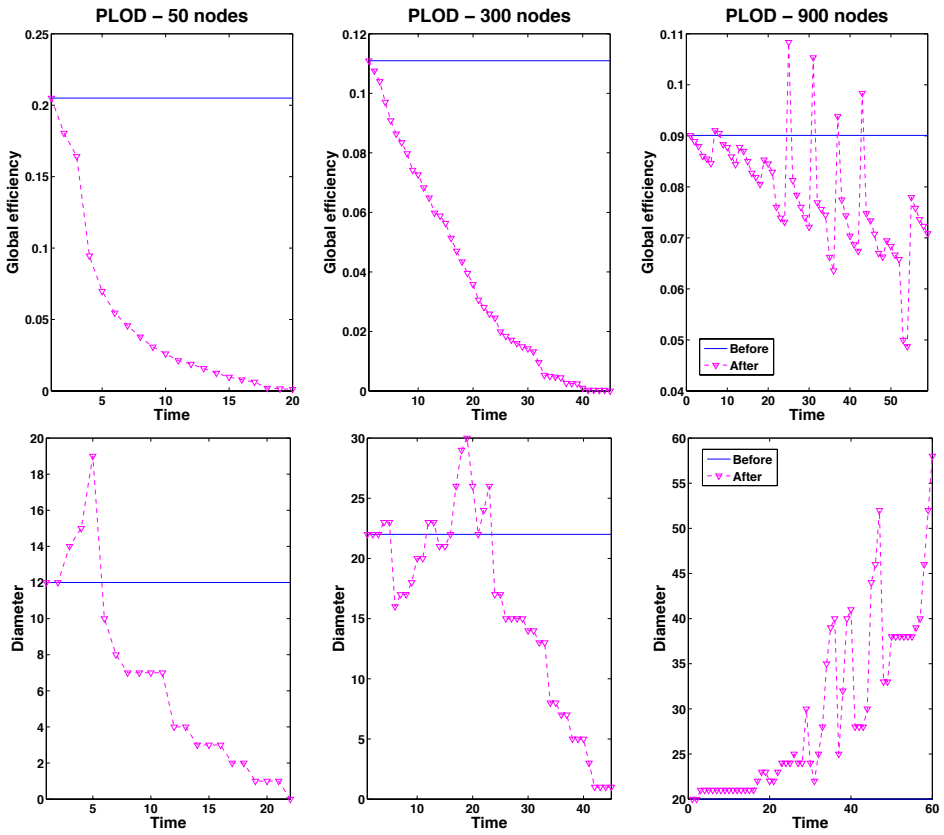

Figure 4: Target attacks: global efficiency and diameter

system at all times, and the priorities predefined for **E6** and the critical nature of the context have not allowed it. This characteristic is also notable in the number of accesses permitted for entities **E1** to **E5**. The vast majority of the accesses fall to minimum values because of the rate of perturbations each time, causing the network to significantly vary its diameter and its shortest paths. These findings therefore show the suitability of implementing our approach in critical scenarios, in which the use of policy enforcement systems based on automated authorization managers can be an effective solution to interconnect multiple cyber-physical systems with specific interconnection requirements and security policies [27].

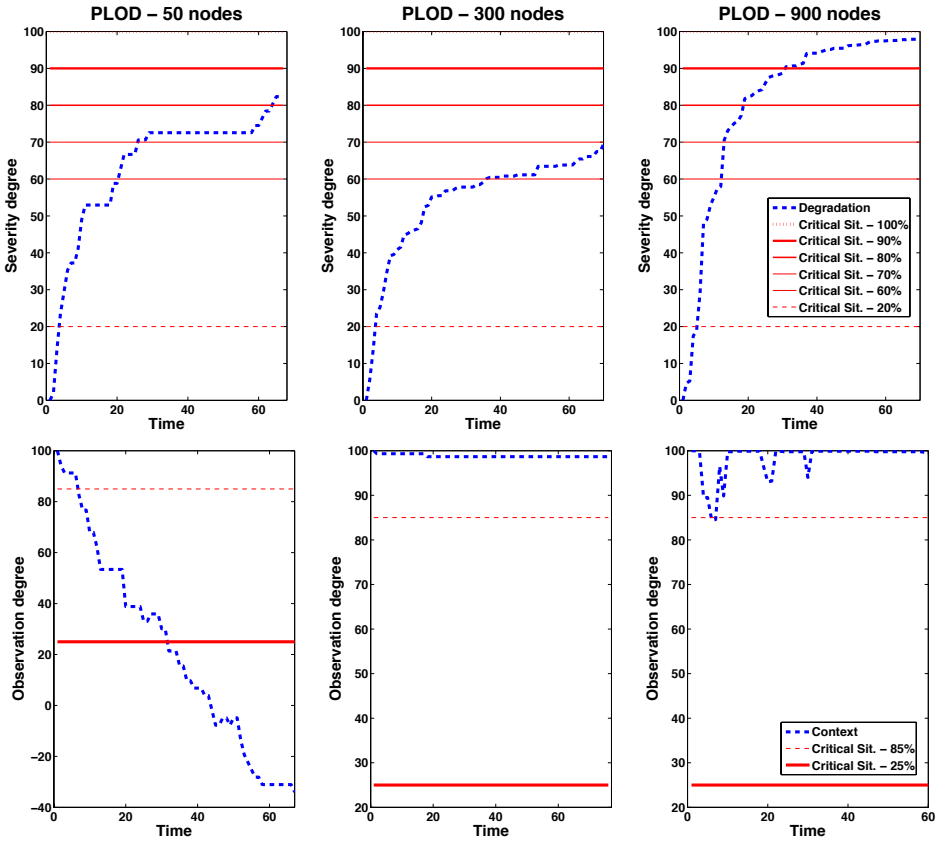

Figure 5: Random attacks: severity and observation

6 CONCLUSION

This paper has extended the policy enforcement system described in [2] to incorporate optimal self-healing services, taking into account the control structural capacities, the supernode theory and the IEC-62351 standard. This new restoration capacity is also based on the redundant measurements presented in [3] in which the control is centralized in the main interfaces between cyber-physical systems and the policy decision points together with their main context managers. To automatize the restoration processes, one new context attribute has been proposed, which together with the observation degree defined in [2], makes it possible to determine the degree of severity of the context and when to repair the entire system. This feature also improves the restoration capacities described in [1] since a high observation degree is not enough to ensure a suitable controllability of the net-

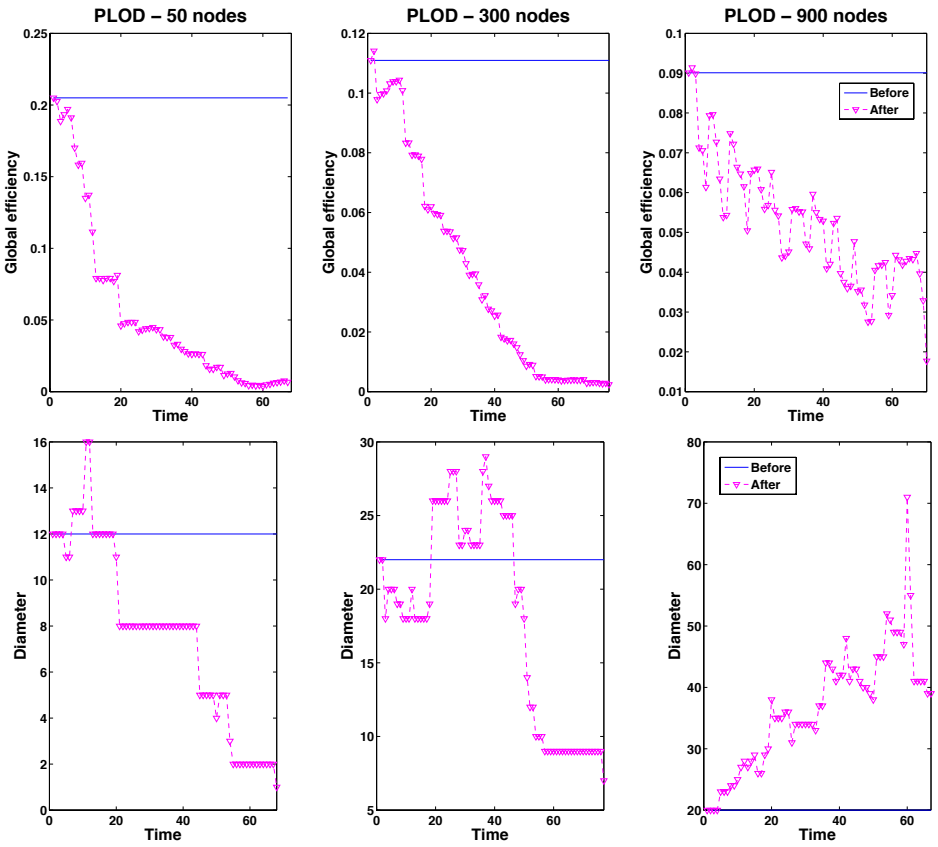

Figure 6: Random attacks: global efficiency and diameter

work and its dynamics, like, for example, the control loads linked to the diameter of the network and its shortest paths.

To show the effectiveness of the approach, several experiments have been carried out, taking into account a set of combined threats. The results show that large distributions are more resilient to target or random perturbations, but even so the perturbations can significantly corrupt the initial distributions and their edge centralities, varying the shortest paths and their control loads. As future work, we intend to incorporate the work presented here into a low-scale real-world system, with the goal of designing new improvements and interconnection approaches.

ACKNOWLEDGEMENTS

This work has been partially supported by the research projects PERSIST (TIN2013-41739-R) and SADCIP (RTC-2016-4847-8), both financed by the Ministerio de Economía y Competitividad, as well as by the project NECS (H2020-MSCA-ITN-2015), financed from the European Unions Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 675320.

References

[1] C. Alcaraz, J. Lopez, K. R. Choo, Dynamic restoration in interconnected rbac-based cyber-physical control systems, in: Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4: SECRYPT, Lisbon, Portugal, July 26-28, 2016., 2016, pp. 19–27.

[2] C. Alcaraz, J. Lopez, S. Wolthusen, Policy enforcement system for secure interoperable control in distributed smart grid systems, Journal of Network and Computer Applications 59 (2016) 301 – 314.

[3] C. Alcaraz, J. Lopez, Safeguarding structural controllability in cyber-physical control systems, in: The 21st European Symposium on Research in Computer Security (ESORICS 2016), Vol. 9879, Springer, Springer, Crete, Greece, 2016, pp. 471–489.

[4] C.-T. Lin, Structural Controllability, IEEE Transactions on Automatic Control 19 (3) (1974) 201–208.

[5] H. Samuel, W. Zhuang, , B. Preiss, Improving the dominating-set routing over delay-tolerant mobile ad-hoc networks via estimating node intermeeting times, in: EURASIP Journal on Wireless Communications and Networking, Hindawi Publishing Corporation, 2011, pp. 1–12.

[6] NIST, A survey of access control models, Working Draft, `http://csrc.nist.gov/news_events/privilege-management-workshop/PvM-Model-Survey-Aug26-2009.pdf`, National Institute of Standards and Technology, retrieved on Dec. 2016. (2009).

[7] IEC-62351-8, Power systems management and associated information exchange - data and communications security - part 8: Role-based access control, international electrotechnical commission, 2011, http://www.iec.ch/smartgrid/standards/, retrieved on Dec. 2016. (2011).

[8] IEC-62351, IEC-62351 parts 1-8: Information security for power system control operations, international electrotechnical commission, http://www.iec.ch/smartgrid/standards/, retrieved on Dec. 2016. (2007-2011).

[9] IEC-62351-3, Power systems management and associated information exchange - data and communications security - part 3: Communication network and system security - profiles including TCP/IP, international electrotechnical commission, 2007, http://www.iec.ch/smartgrid/standards/, retrieved on Dec. 2016. (2007).

[10] IEC-61850, Power utility automation - communication networks and systems in substations - parts 1-10, TC 57 - Power systems management and associated information exchange (2003).

[11] E. Coyne, T. R. Weil, ABAC and RBAC: Scalable, flexible, and auditable access management, Insecure IT Pro, IEEE Computer Society (2013) 14–16.

[12] V. C. Hu, D. F. Ferraiolo, D. R. Kuhn, Assessment of access control systems (NISTIR 7316), National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf, retrieved on Dec. 2016. (2006).

[13] C. Alcaraz, S. Wolthusen, Recovery of structural controllability for control systems, in: Eighth IFIP WG 11.10 International Conference on Critical Infrastructure, Vol. 441, Springer, 2014, pp. 47–63.

[14] K. Nakayama, N. Shinomiya, H. Watanabe, An autonomous distributed control method for link failure based on tie-set graph theory, Circuits and Systems I: Regular Papers, IEEE Transactions on 59 (11) (2012) 2727–2737.

[15] M. Marchese, M. Mongelli, Simple protocol enhancements of rapid spanning tree protocol over ring topologies, Computer Network 56 (4) (2012) 1131–1151.

[16] T. Haynes, S. M. Hedetniemi, S. T. Hedetniemi, M. A. Henning, Domination in graphs applied to electric power networks, SIAM Journal on Discrete Mathematics 15 (4) (2002) 519–529.

[17] J. Kneis, D. Mölle, S. R., P. Rossmanith, Parameterized power domination complexity, Information Processing Letters 98 (4) (2006) 145–149.

[18] Y.-Y. Liu, J.-J. Slotine, A.-L. Barabasi, Controllability of complex networks, Nature 473 (7346) (2011) 167–173.

[19] R. E. Kalman, Mathematical description of linear dynamical systems, Journal of the Society of Industrial and Applied Mathematics Control Series A 1 (1963) 152–192.

[20] S. Nie, X. Wang, H. Zhang, Q. Li, B. Wang, Robustness of controllability for networks based on edge-attack, PLoS ONE 9 (2) (2014) 1–8.

[21] R. Albert, A. Barabási, Statistical mechanics of complex networks, Reviews of Modern Physics 74 (1) (2002) 4797.

[22] C. Palmer, J. Steffan, Generating network topologies that obey power laws, in: Global Telecommunications Conference (GLOBECOM '00), Vol. 1, 2000, pp. 434–438.

[23] G. A. Pagani, M. Aiello, The power grid as a complex network: A survey, Physica A: Statistical Mechanics and its Applications 392 (11) (2013) 2688–2700.

[24] Apache Directory Studio, `http://directory.apache.org/studio/`, retrieved on Dec. 2016 (2006-2016).

[25] M. Smith, Definition of the inetOrgPerson LDAP object class, RFC-2798,, `http://www.ietf.org/rfc/rfc2798.txt`, retrieved on Dec. 2016 (2010).

[26] C. Alcaraz, E. E. Miciolino, S. Wolthusen, Structural controllability of networks for non-interactive adversarial vertex removal, in: 8th International Conference on Critical Information Infrastructures Security, Vol. 8328, Springer, 2013, pp. 120–132.

[27] C. Alcaraz, J. Lopez, Secure interoperability in cyber-physical systems, in: Security Solutions and Applied Cryptography in Smart Grid Communications, IGI Global, USA, IGI Global, USA, 2017, Ch. 8, pp. 137–158.