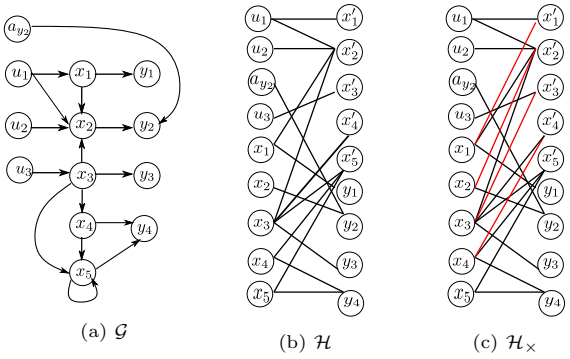
Security index based on perfectly undetectable attacks: Graph-theoretic conditions- Supplementary Material ☆

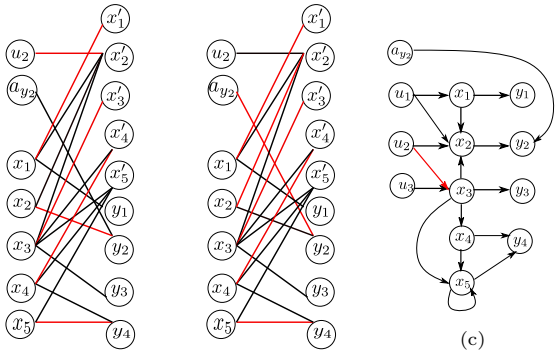
Sebin Gracy[1], Jezdimir Milošević[1], Henrik Sandberg[1]

[a] *The Division of Decision and Control Systems, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden.*



(a) $\mathcal{G}$ (b) $\mathcal{H}$ (c) $\mathcal{H}_\times$

Figure 1: With respect to Example 1,(a): graph $\mathcal{G}$, with $\mathcal{I} = \{u_1, u_2, u_3, a_{y_2}\}$; (b):bipartite graph $\mathcal{H}$; and (c): bipartite graph $\mathcal{H}_\times$, with the edges in red being the newly-added edges. $\mathcal{I} = \{u_1, u_2.u_3.a_{y_2}\}$. $\mathcal{S} = \{y_1, y_3.y_4\}$.



(a) (b) (c)

Figure 2: (a): bipartite graph $\tilde{\mathcal{H}}_\times$ corresponding to set $\mathcal{I}_a = \{a_{y_2}, u_2\}$, with edges in red forming a matching of size 6, but not covering a_{y_2}; (b): bipartite graph $\tilde{\mathcal{H}}_\times$ corresponding to set $\mathcal{I}_a = \{a_{y_2}, u_2\}$, with edges in red forming a matching of size 5, but not covering u_2 ; and (c): With respect to Example 1, graph $\hat{\mathcal{G}}$. The edges in red denote the extra edges added to $\mathcal{G}$, while the edges in black are the same as those in $\mathcal{G}$.

1. Example 1 (contd.)

1.1. Generic index

With respect to the example in Figure **??**, $\mathcal{I} = \{u_1, u_2, a_{y_2}, u_3\}$. Consider the vertex set $\mathcal{I}_a = \{u_2, a_{y_2}\}$. Since vertices u_2, a_{y_2} and x_2 are connected to x'_2 and/or y_2, and to no other vertices in the right vertex set of $\tilde{\mathcal{H}}_\times$, the maximum size of a matching in $\tilde{\mathcal{H}}_\times$ is 6; see, for instance, Figures **??** and **??**. Observe that the matching in Figure **??** does not cover a_{y_2}, and, hence, $\delta_s(a_{y_2}) = 2$. Similarly, for vertex u_2, it can be observed from Figure **??** that there exists a maximum matching that does not cover u_2, and, hence, $\delta_s(u_2) = 2$. To compute $\delta_s(u_1)$ (resp. $\delta_s(u_3)$), consider the vertex set $\mathcal{I} = \{u_1, u_2, u_3, a_{y_1}\}$. Note that the associated bipartite graph is same as $\mathcal{H}_\times$; see Figure **??**. It can be easily verified that the size of a maximum matching in $\mathcal{H}_\times$ equals 8, while the size of a maximum matching in $\mathcal{H}_{\times -u_1}$ (resp. $\mathcal{H}_{\times -u_3}$) equals 7. This implies that every maximum matching in $\mathcal{H}_\times$ covers u_1 (resp. u_3). Hence, since condition (i)in Theorem 3 is satisfied for $p = |\mathcal{I}|$, it follows from Remark 1 that $\delta_s(u_1) = +\infty$ (resp. $\delta_s(u_3) = +\infty$). ■

1.2. Bounds on the security index

Recall that $\mathcal{I} = \{a_{y_2}, u_1, u_2, u_3\}$. For a given vertex i_1 and a given p, a set $\mathcal{I}_a$ that satisfies both a) $|\mathcal{I}_a| = p$, and b) $i_1 \in \mathcal{I}_a$ will be referred to as a *candidate* set. Consider vertex u_1. Note that for $p = 1$, there is only one candidate set, namely $\mathcal{I}_a^1 = \{u_1\}$. Figure **??** exhibits a uniquely restricted matching of size 6 in the associated bipartite graph $\tilde{H}_\times$. Thus, the condition in item (ii) in Corollary 2 is satisfied, and therefore, for all nonzero choices of edge weights of the graph in Figure **??**, $\delta(u_2) \geq 2$.
Next, we check for $p = 2$. Observe that there are three candidate sets, say $\mathcal{I}_a^2$, $\mathcal{I}_a^3$ and $\mathcal{I}_a^4$, where $\mathcal{I}_a^2 = \{u_1, u_2\}$, $\mathcal{I}_a^3 = \{a_{y_2}, u_1\}$, and $\mathcal{I}_a^4 = \{u_1, u_3\}$. The bipartite graph $\tilde{\mathcal{H}}$ (resp. $\tilde{\mathcal{H}}_\times$) corresponding to set $\mathcal{I}_a^2$ is as depicted in Figure **??** (resp. Figure **??**), with the edges highlighted in red forming a uniquely restricted matching, $\tilde{\mathcal{M}}^{\mathcal{I}_a^2}$ (resp. $\tilde{\mathcal{M}}_\times^{\mathcal{I}_a^2}$), of size equals 6 (resp. 7). Observe that in $\tilde{\mathcal{H}}$ vertices x_4 and x_5 are connected to both x'_5 and y_4, and to no other vertices. Therefore, by definition of uniquely restricted matching, any uniquely restricted matching in $\tilde{\mathcal{H}}$ can cover x_4 or x_5 but not both. Thus, the maximum size of a uniquely restricted matching in $\tilde{\mathcal{H}}$ equals 6. Since ver-

☆This paper was not presented at any IFAC meeting. Corresponding author: Sebin Gracy. This work was supported in part by the Swedish Civil Contingencies Agency (project CERCES), and the Swedish Research Council (project 2016-00861).

tex u_1 is involved in every maximum uniquely restricted matching in $\tilde{\mathcal{H}}$, it follows that the maximum size of a uniquely restricted matching in $\tilde{\mathcal{H}}_{-u_1}$ is less than 6. Observe that since $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^2}$ does not involve the edge (x_5, x_5'), it follows that $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^2} \cap \mathcal{E}_{\text{loop}} = \emptyset$. Since $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^2}$ covers all the edges in the left vertex set of $\tilde{\mathcal{H}}_{\times}$, it follows that any matching in $\tilde{\mathcal{H}}_{\times -u_1}$ will have size smaller than 7. Thus, with respect to set $\mathcal{I}_a^2$, conditions (i) and (ii) in Theorem 5 are satisfied. Next, we consider the set $\mathcal{I}_a^3$. The bipartite graph $\tilde{\mathcal{H}}$ (resp. $\tilde{\mathcal{H}}_{\times}$) corresponding to set $\mathcal{I}_a^3$ is as depicted in Figure **??** (resp. Figure **??**), with the edges highlighted in red forming a uniquely restricted matching, $\tilde{\mathcal{M}}^{\mathcal{I}_a^3}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^3}$), of size equals 5 (resp. 7). Indeed, the maximum size of a uniquely restricted matching in $\tilde{\mathcal{H}}$ is 5, since, a) as previously discussed, either x_4 or x_5, but not both, can be covered by a uniquely restricted matching in $\tilde{\mathcal{H}}$, and b) since a_{y_2} and x_2 are connected to, and only to, y_2, by definition of matching, a matching can cover either a_{y_2} or x_2, but not both. Since u_1 is covered by every maximum uniquely restricted matching in $\tilde{\mathcal{H}}$, it follows that the maximum size of a uniquely restricted matching in $\tilde{\mathcal{H}}_{-u_1}$ is less than 5. By reasoning analogous to that for matching $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^2}$ in set $\mathcal{I}_a^2$, it can be seen that a) $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^3} \cap \mathcal{E}_{\text{loop}} = \emptyset$, and b) any matching (and therefore any uniquely restricted matching) in $\tilde{\mathcal{H}}_{\times -u_1}$ will have size smaller than 7. Next, we check for set $\mathcal{I}_a^4$. The bipartite graph $\tilde{\mathcal{H}}$ (resp. $\tilde{\mathcal{H}}_{\times}$) corresponding to set $\mathcal{I}_a^4$ is as depicted in Figure **??** (resp. Figure **??**), with the edges highlighted in red forming a uniquely restricted matching, $\tilde{\mathcal{M}}^{\mathcal{I}_a^4}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^4}$), of size equals 6 (resp. 7). Due to similar reasoning as with sets $\mathcal{I}_a^2$ and $\mathcal{I}_a^3$, it can be seen that, with respect to set $\mathcal{I}_a^4$ also, the conditions in Theorem 5 are satisfied. Therefore, by Theorem 5, for all nonzero choices of edge weights, $\delta(u_1) \geq 3$.

We increment p, i.e., we check for $p = 3$. Observe that there are three candidate sets, say $\mathcal{I}_a^5$, $\mathcal{I}_a^6$ and $\mathcal{I}_a^7$, where $\mathcal{I}_a^5 = \{u_1, u_2, u_3\}$, $\mathcal{I}_a^6 = \{a_{y_2}, u_1, u_2\}$, and $\mathcal{I}_a^7 = \{u_1, a_{y_2}, u_3\}$. The bipartite graph $\tilde{\mathcal{H}}$ (resp. $\tilde{\mathcal{H}}_{\times}$) corresponding to set $\mathcal{I}_a^5$ is as depicted in Figure **??** (resp. Figure **??**), with the edges highlighted in red forming a uniquely restricted matching, $\tilde{\mathcal{M}}^{\mathcal{I}_a^5}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^5}$), of size equals 7 (resp. 8). The bipartite graph $\tilde{\mathcal{H}}$ (resp. $\tilde{\mathcal{H}}_{\times}$) corresponding to set $\mathcal{I}_a^6$ is as depicted in Figure **??** (resp. Figure (**??**)), with the edges highlighted in red forming a uniquely restricted matching, $\tilde{\mathcal{M}}^{\mathcal{I}_a^6}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^6}$), of size equals 6 (resp. 7). The bipartite graph $\tilde{\mathcal{H}}$ (resp. $\tilde{\mathcal{H}}_{\times}$) corresponding to set $\mathcal{I}_a^7$ is as depicted in Figure **??** (resp. Figure **??**), with the edges highlighted in red forming a uniquely restricted matching, $\tilde{\mathcal{M}}^{\mathcal{I}_a^7}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^7}$), of size equals 6 (resp. 7). For reasons, as discussed previously, each of the uniquely restricted matchings $\tilde{\mathcal{M}}^{\mathcal{I}_a^5}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^5}$), $\tilde{\mathcal{M}}^{\mathcal{I}_a^6}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^6}$), and $\tilde{\mathcal{M}}^{\mathcal{I}_a^7}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^7}$) are maximum. Moreover, each of these cover vertex u_1, thus implying that removal of u_1 reduces the maximum size of a uniquely restricted matching in the concerned bipartite graphs. Hence, the conditions of Theorem 5 are met, and therefore, for all nonzero choices of edge weights, $\delta(u_1) \geq 4$.

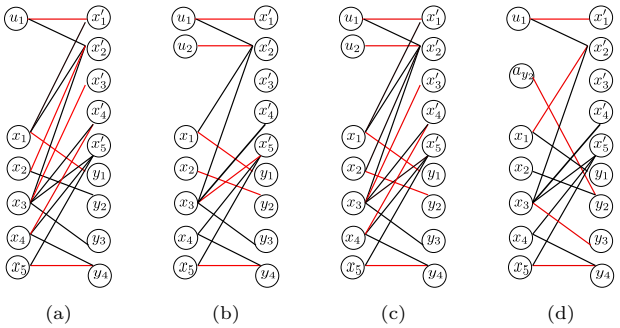


Figure 3: For vertex u_1 (a): with $p = 1$, bipartite graph $\tilde{\mathcal{H}}_{\times}$, with edges in red highlighting a uniquely restricted matching having size equals 6; (b): with $p = 2$, bipartite graph $\tilde{\mathcal{H}}$ corresponding to set $\mathcal{I}_a^2$, with edges in red forming a uniquely restricted matching of size 6; (c): with $p = 2$, bipartite graph $\tilde{\mathcal{H}}_{\times}$ corresponding to set $\mathcal{I}_a^2$, with edges in red forming a uniquely restricted matching of size 7. (c): bipartite graph $\tilde{\mathcal{H}}$, with edges in red forming a uniquely restricted matching of size 6; (d): with $p = 2$, for set $\mathcal{I}_a^3$ bipartite graph $\tilde{\mathcal{H}}$, with edges in red forming a uniquely restricted matching of size 5.

Finally, we check for $p = 4$, in which case there is only one candidate set, namely $\mathcal{I}_a^8 = \{u_1, u_2, u_3, a_{y_2}\}$. The bipartite graph $\tilde{\mathcal{H}}$ (resp. $\tilde{\mathcal{H}}_{\times}$) corresponding to set $\mathcal{I}_a^8$ is as depicted in Figure **??** (resp. Figure **??**), with the edges highlighted in red forming a uniquely restricted matching, $\tilde{\mathcal{M}}^{\mathcal{I}_a^8}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^8}$), of size equals 7 (resp. 8). Due to similar reasons as before, it follows that $\tilde{\mathcal{M}}^{\mathcal{I}_a^8}$ (resp. $\tilde{\mathcal{M}}_{\times}^{\mathcal{I}_a^8}$) is also a maximum uniquely restricted matching, and that removal of u_1 reduces the maximum size of a uniquely restricted matching, thus satisfying the conditions in Theorem 5. Since conditions Theorem 5 are met for $p = 4$ (i.e., $p = |\mathcal{I}|$), it follows from Remark 1, that, for all nonzero choices of edge weights, $\delta(u_1) = +\infty$.

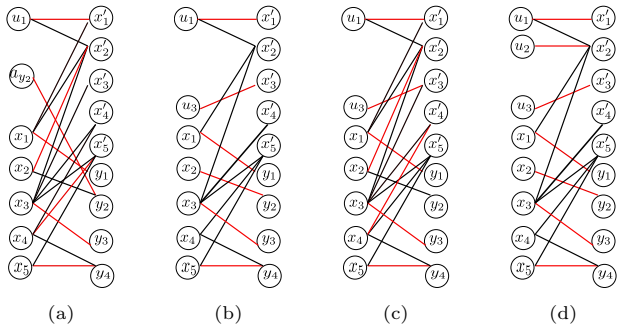
Analogously, we can obtain that for all nonzero choices of edge weights of the graph in Figure **??**, i) $\delta(a_{y_2}) \leq 2$, and $\delta(a_{y_2}) \geq 2$, thus implying $\delta(a_{y_2}) = 2$, ii) $\delta(u_2) \geq 2$, and iii) $\delta(u_3) = +\infty$. ■

2. Practical and Illustrative Examples

We consider two examples in this section. The purpose of the first example is to illustrate our theoretical findings in a more realistic setting, whereas the objective behind the second example is to illustrate the effectiveness of Algorithm 1 for a non-trivial system. Graphical representations of the examples in this section will be omitted in the interest of space.

2.1. Example 2: Water tanks

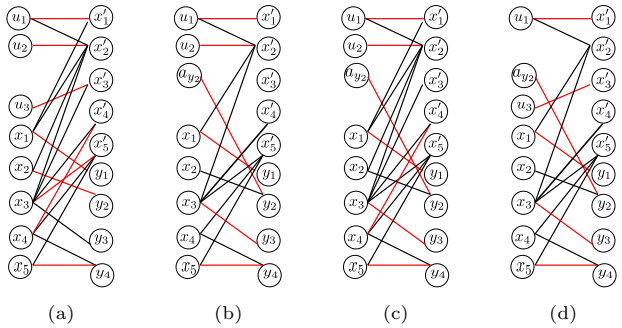
We consider the three-tank system from (**?**) shown in Figure **??**. The plant states x_1–x_3 are the levels in the three tanks. These levels are regulated using two actuators: Pump 1 (P_1) and Pump 2 (P_2). The measurements



(a) (b) (c) (d)

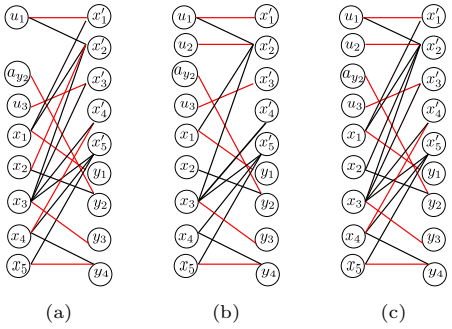
Figure 4: For vertex u_1 (a): with $p = 2$ bipartite graph $\tilde{\mathcal{H}}_\times$ corresponding to set $\mathcal{I}_a^3$, with edges in red forming a uniquely restricted matching of size 7; (b): with $p = 2$ bipartite graph $\tilde{\mathcal{H}}$ corresponding to set $\mathcal{I}_a^4$, with edges in red forming a uniquely restricted matching of size 6; (c): with $p = 2$ bipartite graph $\tilde{\mathcal{H}}_\times$ corresponding to set $\mathcal{I}_a^4$, with edges in red forming a uniquely restricted matching of size 7; (d):with $p = 3$ bipartite graph $\tilde{\mathcal{H}}$ corresponding to set $\mathcal{I}_a^5$, with edges in red forming a uniquely restricted matching of size 7

.



(a) (b) (c) (d)

Figure 5: For vertex u_1 with $p = 3$, (a): bipartite graph $\tilde{\mathcal{H}}_\times$ corresponding to set $\mathcal{I}_a^5$, with edges in red forming a uniquely restricted matching of size 8; (b):bipartite graph $\tilde{\mathcal{H}}$ corresponding to set $\mathcal{I}_a^6$, with edges in red forming a uniquely restricted matching of size 6; (c): bipartite graph $\tilde{\mathcal{H}}_\times$ corresponding to set $\mathcal{I}_a^6$, with edges in red forming a uniquely restricted matching of size 7; (d): bipartite graph $\tilde{\mathcal{H}}$ corresponding to set $\mathcal{I}_a^7$, with edges in red forming a uniquely restricted matching of size 6.



(a) (b) (c)

Figure 6: For vertex u_1 (a): with $p = 3$ bipartite graph $\tilde{\mathcal{H}}_\times$ corresponding to set $\mathcal{I}_a^7$, with edges in red forming a uniquely restricted matching of size 7. (b): with $p = 4$ bipartite graph $\tilde{\mathcal{H}}$, with edges in red forming a uniquely restricted matching of size 7. (c): bipartite graph $\tilde{\mathcal{H}}_\times$, with edges in red forming a uniquely restricted matching of size 8.

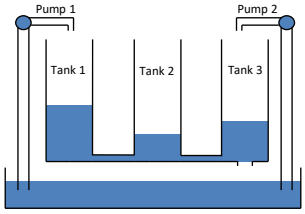


Figure 7: Three tank system (figure courtesy of (?))

corresponding to water levels in Tank 2 and Tank 3 are available. Our goal is to study how vulnerable are each of the actuators to attack from an adversary. Towards this end, so as to better account for the uncertainty in physical parameters, we take recourse to structured systems representation. The structural system matrices are given by:

$$W = \begin{bmatrix} w_{11} & w_{12} & 0 \\ w_{21} & w_{22} & w_{23} \\ 0 & w_{32} & w_{33} \end{bmatrix}, \quad B_a = \begin{bmatrix} b_{11} & 0 \\ 0 & 0 \\ 0 & b_{31} \end{bmatrix},$$
$$C = \begin{bmatrix} 0 & c_{12} & 0 \\ 0 & 0 & c_{23} \end{bmatrix}.$$

Considering these matrices, we can construct the corresponding graph $\mathcal{G}$. Observe that in this case, $N = 3$, $M = 2$ and $P = 2$, where N, M and P are as defined in the main manuscript. We assume that while both of the sensors are secured, the actuators are vulnerable to attacks by an attacker. Hence, the set of components that the attacker can compromise is given by $\mathcal{I} = \{u_1, u_2\}$.

We first compute the generic security index δ_s for the actuators u_1 and u_2. Using Algorithm 1, we obtain $\delta_s(u_1) = +\infty$ and $\delta_s(u_2) = +\infty$. In words, perfectly undetectable attacks targeting u_1 or u_2 do not exists for almost all realizations of system parameters, so this system is robust with respect to perfectly undetectable attacks. Indeed, we can see that by attacking P1, the attacker changes the level in Tank 1. This result in changes in the levels in Tanks 2 and 3. Hence, even if the attacker compromises P2, he/she cannot simultaneously maintain the levels in Tanks 2 and 3 on the same value as prior to the attack. Hence, any attack gets detected either through the first or the second sensor.

Observe that although $\delta_s(u_1) = +\infty$ and $\delta_s(u_2) = +\infty$, there might be non-zero choices of free parameters of matrices W, B_a and C for which $\delta(u_1)$ (resp. $\delta(u_2)$) might be small. Hence, we seek to compute the bounds on $\delta(u_1)$ (resp. $\delta(u_2)$) for all non-zero choices of free parameters in W, B_a and C, respectively. Towards this end, we construct the bipartite graphs $\mathcal{H}$ and $\mathcal{H}_\times$ associated with this system (see Section 2.3 of the main manuscript). With respect to component u_1 (resp. u_2), it can be seen that, for $p = 2$ (i.e., $p = |\mathcal{I}|$), condition (i) in Corollary 2 is satisfied. Hence, for all non-zero choices of free parameters of W, B_a and C, $\delta(u_1) = +\infty$ (resp. $\delta(u_2) = +\infty$). Note that, unlike Example 1, in this example we appealed to the graphical condition in Corollary 2 for computing the bounds on $\delta(u_1)$ (resp. $\delta(u_2)$). Since the condition

in Corollary 2 with respect to each set can be checked in polynomial-time, this example exhibits a scenario where the deterministic guarantees of security may be available in a shorter time.

2.2. Example 3: Generic Security index for risk assessment

Consider a control system used for regulating temperatures within five identical areas (**?**) (see Figure **??**). Each area is modelled with the states $x_i = [T_{ai}\ T_{wi}\ P_i]^T$, where T_{ai} is the temperature of the i^{th} area, T_{wi} is the temperature of the i^{th} evaporator's lumped coil wall, and P_i is the refrigerant's pressure after leaving the i^{th} evaporator. These states are regulated through the control actions $u_i = [\omega_{fi}\ \ a_{vi}]^T$, where ω_{fi} is the speed of the i^{th} evaporator's fan, and a_{vi} is the control action that changes the fluid resistance of the i^{th} Electronic Expansion Valve (EEV). The compressor is modelled with a single state $x_c = P_C$, where P_C is the refrigerant pressure after leaving the compressor. The pressure P_C is regulated through the control action $u_c = \omega_K$, where ω_K is the speed of the compressor. We assume that: 1) The states in Area 1 and Area 2 are not measured; 2) The states in Area 3 and Area 4 are measured by one sensor; and 3) The states in Area 5 are measured by two sensors.

To evaluate security level of the evaporators and EEVs, we computed the structured index δ_s of these components using Algorithm 1 (see Table **??**). We point out that this computation took 239.2 seconds, which shows that, for moderate-sized systems, generic security index can be computed reasonably quickly using Algorithm 1.

It is immediate that the most vulnerable components in the system are Evaporator 1 and Evaporator 2. This is in line with the physics of the system: by manipulating Evaporator 1, the attacker affects temperatures T_{w1} and T_{a1}. Since these states are not measured, the attacker can compromise only Evaporator 1 while remaining perfectly undetectable in almost any realization of the system. The same explanation holds for Evaporator 2. The most protected actuators are EEVs. The reason for this can also be found in the physics of the system. Namely, besides the states within the corresponding area, every EEV affects the states in all other areas. Hence, conducting a perfectly undetectable attack against an EEV requires more compromised components. Moreover, it turns out that all EEVs have equal security index. Hence, although the states in Area 1 and Area 2 are not measured, EEV 1 and EEV 2 get protected due to the physical coupling present in the system.

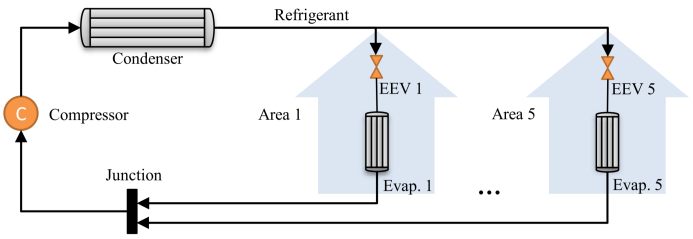


Figure 8: System used in simulations.

Table 1: Generic Security index of the actuators for the system shown in Figure **??**.

Actuator	δ_s	Actuator	δ_s
EEV 1	7	Evap. 1	1
EEV 2	7	Evap. 2	1
EEV 3	7	Evap. 3	3
EEV 4	7	Evap. 4	3
EEV 5	7	Evap. 5	5