Structural Resilience of Cyberphysical Systems Under Attack* +

Bhaskar Ramasubramanian¹, M. A. Rajan,² and M. Girish Chandra²

Abstract—The resilience of cyberphysical systems (CPS) to denial of service (DoS) and integrity attacks is studied. The CPS is modeled as a linear structured system, and its resilience to various attack scenarios is interpreted in a graph theoretical framework. The structural resilience of the CPS to DoS and integrity attacks is characterized in terms of unmatched vertices in maximum matchings of the bipartite graph and connected components of directed graph representations of the CPS under attack. Further, we prove that if a system is structurally resilient to a DoS attack for some defender input matrix $[B_{def}]$, with zero structure $Z(B_{def})$, then there exists a $[B'_{def}]$ with $Z(B'_{def}) \subseteq Z(B_{def})$ for which it will also be structurally resilient to a state feedback integrity attack. If an additional condition holds, we show that the same $[B_{def}]$ will ensure structural resilience to a state feedback integrity attack.

I. INTRODUCTION

Cyberphysical systems (CPS) are entities in which the working of the physical system is intimately linked to the functioning of computers controlling interactions between the system and a controller, or among subsystems. Since these systems are often controlled via a network, computational resources and bandwidth also affect their working. Examples of large scale CPS include power systems, water distribution networks, and medical devices. While computer controlled systems are more efficient, the integrated system is more vulnerable to attacks. An attack could be carried out on the physical system itself, on the computer controlling the system, or on the communication links between the system and the computer. A compilation of vulnerabilities in existing systems, and means of mitigating threats is found in [1], [2], [3].

A large part of the current literature in this area assumes full knowledge of the system parameters, and analyzes the consequences of attacks on these systems. Parameters in CPS with large number of state and measured variables are prone to variations, albeit, in a small range of values. Conventional methods of analysis based on these models might thus be computationally infeasible. The structural systems approach, introduced by Lin in [4], offers a way out of this conundrum. This technique presumes knowledge of just the zero structures (that is, the positions of zero and nonzero entries) of the system matrices to infer system properties. This approach is attractive since these properties will hold for almost all valid numerical realizations.

In this paper, the CPS is modeled as a linear structured system, and structural conditions for an attack to be successful, in terms of disrupting or obtaining controllability of a (modified) linear structured system are provided. The structural resilience of the system to denial of service (DoS) attacks and integrity attacks is characterized in terms of the structural controllability of an associated linear structural system.

A. Related Work

CPS are modeled as linear descriptor systems subject to unknown inputs in [5], [6]. System and graph theoretic conditions are formulated and proved for an attack on the CPS to be
undetectable and unidentifiable by monitors. The structural design of large scale systems is studied in [7]. The input and output matrices are designed to select the smallest number of actuated and sensed variables to ensure structural controllability and observability. The state feedback matrix is then designed to ensure the minimum number of input-output interconnections and such that the closed loop system has no structural fixed modes.

The success of various attacks on linear time invariant (LTI) systems in terms of the ability to obtain or disrupt controllability of a suitably modified LTI system is characterized in [8]. It is this approach that we wish to extend to structured linear systems. Interpreting security properties in this framework will allow for a more rigorous analysis of complex, networked cyberphysical systems that are vulnerable to attacks. We note that [8] also models classes of attacks using notions from game theory, but do not provide an analogue in this work.

For an LTI system, given the system matrix, the minimal controllability problem aims to find the sparsest input matrix that will ensure controllability. In the unconstrained case, [9] showed that this problem was \( NP \)-hard. Interestingly, [7] showed that the minimal structural controllability problem was polynomially solvable. [10] studied the minimal controllability problem for single input structured systems, and showed that the problem was solvable when a rank condition was satisfied. Further, [11] showed that the minimum constrained input selection problem was \( NP \)-hard. In this problem, given the structures of the system and input matrices, the goal was to determine a minimal set of indices of columns of the input matrix to ensure structural controllability.

In [12], given the costs of actuating each state, the minimum cost structural controllability problem was shown to be polynomially solvable. [13] extended this work to the constrained case, and the minimum cost constrained structural controllability problem was shown to be \( NP \)-hard by deriving a reduction from the constrained minimum input selection problem. This problem was polynomially solvable when the system matrix was irreducible.

**B. Outline of Paper**

Section (II) provides an introduction to linear structured systems and graph theory. The problem to be solved is stated in Section (III), and the main results are stated in Sections (IV-B) and (IV-C). Section (V) presents illustrative examples. We conclude by presenting possible directions for future research in Section (VI).

**II. Preliminaries**

Consider the LTI system \( \dot{x}(t) = Ax(t) + Bu(t) \), where \( x \in \mathbb{R}^n \), \( u \in \mathbb{R}^p \), \( A \in \mathbb{R}^{n \times n} \) and \( B \in \mathbb{R}^{n \times p} \). This system is controllable, if for every initial state \( x(0) = x_0 \) and final state \( x(t_f) = x_f \), there exists a control \( u(\cdot) \) on \([0, t_f] \) that transfers the system from \( x_0 \) to \( x_f \).

The notions of structured linear systems and structural controllability was introduced by Lin in [4]. This framework assumes knowledge of just the zero structures, \( [A] \in (0, \ast)^{n \times n} \) and \( [B] \in (0, \ast)^{n \times p} \), of \( A \) and \( B \) respectively. That is, every entry in \( [A] \) and \( [B] \) is either a fixed zero or a free parameter. A matrix \( H \) with the same zero structure as \( [H] \) is called an admissible numerical realization.

**Definition 2.1:** \( ([A],[B]) \) is structurally controllable if there exists an admissible numerical realization \( (A,B) \) that is controllable.

**Remark 2.2:** If \( ([A],[B]) \) is structurally controllable, then almost every admissible numerical realization will be controllable.

Directed graphs provide an elegant means to represent linear structured systems [7]. System properties (e.g., controllability, observability) can be inferred from the digraph associated with the system, and independently of numerical values of parameters. This makes it an attractive tool to study large scale, complex systems. Consider the linear structured system

\[ \dot{x}(t) = [A]x(t) + [B]u(t) \]  

where, \( x \in \mathcal{X} \subseteq \mathbb{R}^n \), \( u \in \mathcal{U} \subseteq \mathbb{R}^p \), \( [A] \in (0, \ast)^{n \times n} \) and \( [B] \in (0, \ast)^{n \times p} \). The directed graph (digraph)
of the structured system is \( D = (V,E) \), where 
\( V = \mathcal{U} \cup \mathcal{X} \) and \( E = \mathcal{E}_A \cup \mathcal{E}_B \), where \( \mathcal{E}_A = \{(x_j,x_i)\mid [A]_{ji} \neq 0\} \), \( \mathcal{E}_B = \{(u_j,x_i)\mid [B]_{ij} \neq 0\} \).

A sequence of directed edges with distinct vertices \( \{(v_1,v_2),(v_2,v_3),\ldots,(v_{k-1},v_k)\} \) is a simple path from \( v_1 \) to \( v_k \). The simple path, with an additional edge, \( (v_k,v_1) \) or a vertex with a self loop is called a cycle. A vertex \( v_2 \) is reachable from another vertex \( v_1 \) if there exists a simple path from \( w_1 \) to \( w_2 \). Let \( \mathcal{V}_1, \mathcal{V}_2 \subseteq \mathcal{V} \). Two paths from \( \mathcal{V}_1 \) to \( \mathcal{V}_2 \) are disjoint if they consist of a disjoint set of vertices. A set of \( v \) mutually disjoint and simple paths from \( \mathcal{V}_1 \) to \( \mathcal{V}_2 \) is a linking of size \( v \). A cycle family is a set of mutually disjoint cycles. A \( \mathcal{U} \)-rooted path is a simple path with source vertex in \( \mathcal{U} \). A \( \mathcal{U} \)-rooted path family is a set of mutually disjoint \( \mathcal{U} \)-rooted paths.

A digraph \( D_\delta = (\mathcal{V}_\delta, \mathcal{E}_\delta) \) is a subgraph of \( D \) if \( \mathcal{V}_\delta \subset \mathcal{V} \) and \( \mathcal{E}_\delta \subset \mathcal{E} \). If \( \mathcal{V}_\delta = \mathcal{V} \), then \( D_\delta \) is said to span \( D \). A subgraph \( D_\delta \) satisfying a property \( P \) is maximal if there is no other subgraph \( D_\delta' \) such that \( D_\delta \) is a strict subgraph of \( D_\delta' \) and property \( P \) holds for \( D_\delta \).

\( D \) is strongly connected if there is a simple path between every pair of vertices of the graph. A strongly connected component (SCC) is a maximal subgraph \( D_S \), of \( D \) such that \( D_S \) is strongly connected. With SCCs as supernodes, one can generate a directed acyclic graph (DAG) in which each supernode corresponds to an SCC, and there exists a directed edge between two SCCs if and only if there exists a directed edge connecting vertices in the SCCs in the original digraph. An SCC is non top (bottom) linked if it has no incoming (outgoing) edges to (from) its vertices from (to) vertices of another SCC.

For any \( \mathcal{V}_1, \mathcal{V}_2 \), a bipartite graph \( \mathcal{B}(\mathcal{V}_1, \mathcal{V}_2, \mathcal{E}_{\mathcal{V}_1, \mathcal{V}_2}) \) is a digraph with vertex set \( \mathcal{V}_1 \cup \mathcal{V}_2 \) and edge set \( \mathcal{E}_{\mathcal{V}_1, \mathcal{V}_2} \subseteq \{(v_1,v_2)\mid v_1 \in \mathcal{V}_1, v_2 \in \mathcal{V}_2\} \). Given \( \mathcal{B}(\mathcal{V}_1, \mathcal{V}_2, \mathcal{E}_{\mathcal{V}_1, \mathcal{V}_2}) \), a matching is a subset of edges that do not share vertices. A maximum matching is a matching that has the largest number of edges. Vertices not belonging to a maximum matching are called unmatched. An unmatched vertex \( v_2 \in \mathcal{V}_2 \) (respectively, \( v_1 \in \mathcal{V}_1 \)) is called a right unmatched vertex (left unmatched vertex). A perfect matching is maximum matching with no unmatched vertices. The bipartite graph associated with \( \mathcal{B}(\mathcal{V}, \mathcal{E}) \) is denoted \( \mathcal{B}(\mathcal{V}, \mathcal{E}) \).

III. PROBLEM FORMULATION

Let the input in \( 1 \) be written as \( u = \left(u_{\text{def}}^T, u_{\text{att}}^T\right)^T \), where \( u_{\text{def}} \in \mathbb{R}^d \) and \( u_{\text{att}} \in \mathbb{R}^a \) (with \( d + a = p \)) represent the inputs available to the system (defender) and attacker respectively. Then, the system model is:

\[
\dot{x}(t) = [A]x(t) + [B_{\text{def}}]u_{\text{def}}(t) + [B_{\text{att}}]u_{\text{att}}(t) \quad (2)
\]

The attacker is assumed to have knowledge of the zero structure of the system matrix \( [A] \), and possesses unlimited computational capabilities. We further assume that the set of attacked nodes remains unchanged with time. The system will be resilient to an attack if it can maintain controllability, or it does not allow the attacker to obtain controllability of the system.

Problem 3.1: Given the system \( 2 \) with \( ([A],[B]) \) structurally controllable before an attack, verify the system’s structural resilience to denial of service (DoS) and integrity attacks. This problem for a given numerical realization, \( ([A],[B]) \) was solved in [8] for various attack scenarios. Assuming that the inputs before an attack are not rogue, structural controllability ensures that the cardinality of the input set is greater than the minimum required [14]. This will play an important role in determining the attack resilience of the system.

IV. MAIN RESULTS

Before stating and proving our main results, some intermediate results will be required. Some proofs are omitted for brevity.

A. Structural Controllability

Given the digraph representation of \( 2 \), define the following [7], [15]:

- **State stem**: simple path comprising only state vertices, or an isolated state vertex.
- **Input stem**: an input vertex linked to the root of a state stem.
• **Input cactus:** An input stem with at least one state vertex is an input cactus. An input cactus connected to a cycle (comprising state vertices only) from a state or input vertex is also an input cactus.

• **Top assignable SCC of** \( \mathcal{D}(A) = (\mathcal{X}, E_A) \) **is a non-top-linked SCC which contains at least one right unmatched vertex in a maximum matching.**

• **Maximum top assignability index of** \( \mathcal{D}(A) \) **is the maximum number of top assignable SCCs among the maximum matchings associated with** \( \mathcal{H}(A) \).

**Theorem 4.1:** [7, 15] The following are equivalent:

1) \( (\mathcal{A}, \mathcal{B}) \) is structurally controllable.
2) \( \mathcal{D}(\mathcal{A}, \mathcal{B}) \) is spanned by a disjoint union of input cacti.
3) Every state vertex is the end of a \( \mathcal{U} \)-rooted path and there exists a union of a \( \mathcal{U} \)-rooted path family and cycle family containing all vertices in \( \mathcal{X} \).
4) Every right unmatched vertex of a maximum matching of \( \mathcal{H}(\mathcal{A}, \mathcal{B}) \) is connected to a distinct input, and one state variable from each non-top-linked SCC of \( \mathcal{D}(A) \) is connected to some input.

**Theorem 4.2:** [14] Let \( m \) be the number of right unmatched vertices in a maximum matching of \( \mathcal{H}(\mathcal{A}) \). Then, the minimum number of inputs to ensure structural controllability is one, if \( m = 0 \), and \( m \), otherwise.

**Theorem 4.3:** [7] Let \( \beta \) be the number of non-top-linked SCCs and \( \alpha \) the maximum top assignability index in \( \mathcal{D}(A) \). Then, the minimum number of input-state links to ensure structural controllability is \( p = m + \beta - \alpha \).

### B. Structural Resilience to DoS Attacks

During a DoS attack, the attacker blocks access to \( u_{\text{att}} \). The system still has access to \( u_{\text{def}} \). Structurally, this corresponds to designing \( [B_{\text{def}}] \), with \( [B_{\text{att}}] = 0 \), to ensure structural resilience. The system model is:

\[
\dot{x}(t) = [A]x(t) + [B_{\text{def}}]u_{\text{def}}(t) \tag{3}
\]

Let \( \mathcal{X}_{\text{def}} \) and \( \mathcal{X}_{\text{att}} \) be the (disjoint) sets of state vertices connected to inputs controlled by the defender and attacker inputs respectively. Let \( m_{\text{def}} \) and \( m_{\text{att}} \) be the number of right unmatched vertices in \( \mathcal{H}(A) \) corresponding to \( \mathcal{X}_{\text{def}} \) and \( \mathcal{X}_{\text{att}} \) (thus, \( m_{\text{def}} + m_{\text{att}} = m \)). Further, let \( m > 0 \). Let \( l(P \rightarrow Q) \) denote the set of links from \( P \) to \( Q \). Lemma [4.4] provides a sufficient condition for a DoS attack to be successful.

**Lemma 4.4:** A DoS attack on \( (2) \) is structurally successful if:

1) \( |\mathcal{U}_{\text{def}} \cup \mathcal{U}_{\text{att}}| \geq m + \beta - \alpha \) OR
2) \( |\mathcal{U}_{\text{def}} \cup \mathcal{U}_{\text{att}}| \geq m \) and \( |l(\mathcal{U}_{\text{def}} \cup \mathcal{U}_{\text{att}}) \rightarrow \mathcal{X}| \geq m + \beta - \alpha \) and \( |\mathcal{U}_{\text{def}}| < m_{\text{def}} \), where \( \mathcal{U}_{\text{def}} \) and \( \mathcal{U}_{\text{att}} \) are the defender and attacker input vertices.

The conditions of Lemma (4.4) are not necessary, for it could be the case that \( |\mathcal{U}_{\text{def}} \cup \mathcal{U}_{\text{att}}| \geq m + \beta - \alpha \) and \( |\mathcal{U}_{\text{def}}| \geq m_{\text{def}} \). Though the minimum input requirement is satisfied, the conditions to ensure structural controllability must be carefully checked.

**Lemma 4.5:** If \( |\mathcal{U}_{\text{def}}| \geq m_{\text{def}} \), a DoS attack is structurally successful if:

1) There exists an unreachable state from the vertices of \( \mathcal{U}_{\text{def}} \). OR
2) There does not exist a disjoint union of \( \mathcal{U}_{\text{def}} \) rooted path families and cycle families covering all the states. OR
3) \( |l(\mathcal{U}_{\text{def}} \rightarrow \mathcal{X})| < m_{\text{def}} + \beta - \alpha \). OR
4) Every maximum matching of \( \mathcal{H}(A) \) has a right unmatched vertex in \( \mathcal{X}_{\text{att}} \). OR
5) There is a non-top-linked SCC in \( \mathcal{D}(A) \) comprising only vertices from \( \mathcal{X}_{\text{att}} \).

Gathering the results in Lemmas (4.4) and (4.5), we have the following result:

**Theorem 4.6:** Given \( [A] \) and the dimensions of \( [B_{\text{def}}] \), the system (3) is structurally resilient to a DoS attack if and only if \( ([A],[B_{\text{def}}]) \) is structurally controllable and there exists: i) a maximum matching of \( \mathcal{H}(A) \) that does not contain a right unmatched vertex in \( \mathcal{X}_{\text{att}} \); ii) a non-top-linked SCC of \( \mathcal{D}(A) \) not comprising vertices from only \( \mathcal{X}_{\text{att}} \).

**Proof:** If \( ([A],[B_{\text{def}}]) \) is not structurally controllable, then at least one of the first two
conditions of Lemma 4.5 will not be satisfied, and the system will not be structurally resilient to a DoS attack. Now, let \([A],[B_{def}]\) be structurally controllable. Any right unmatched vertex in \(X_{def}\) or a non-top-linked SCC consisting of only vertices in \(X_{def}\) will have to be assigned to a control in \(U_{def}\). This would violate the assumption that \(U_{def}\) can only access states in \(X_{def}\). This again means that the system will not be structurally resilient to a DoS attack. If \(\{A\}+[B_{def}]\) is structurally controllable, the absence of right unmatched vertices or non-top-linked SCCs in \(X_{def}\) corresponds to the existence of a control configuration such that \(|U_{def}| \geq m_{def}\) and \(|(U_{def} - X_{def})| \geq m_{def} + \beta - \alpha\), which ensures structural resilience to a DoS attack.

C. Structural Resilience to Integrity Attacks

In state feedback, the control is \(u = Kx\). \(K\) is a gain matrix used to arbitrarily place the poles of the modified state matrix \((A + BK)\). During an integrity attack, only control signals corresponding to the system maintain their integrity, while those of the attacker are arbitrary. The attacker is successful if it wrests control of the system. With \([A_{def}] := (A) + [B_{def}]K_{def}\), the system model is:

\[
\dot{x}(t) = [A_{def}]x(t) + [B_{att}]u_{att}(t)
\]

(4)

**Theorem 4.7:** The system \((A) + [B_{def}]\) is structurally resilient to an integrity attack if and only if there is a right unmatched vertex in \(X_{def}\) in every maximum matching of \(\mathcal{R}(A_{def})\) or there exists a non-top-linked SCC of \(\mathcal{R}(A_{def})\) comprising exclusively vertices in \(X_{def}\).

Alternatively, the attacker might gain access to a state. This would allow it to affect the controllability of the system. This is called a **state feedback integrity attack**. In this scenario, \(u_{att}(t) = K_{att}x(t)\), while \(u_{def}\) is arbitrary. For structural systems, this corresponds to designing \([B_{def}]\) to ensure structural controllability. With \([A_{att}] := (A) + [B_{att}]K_{att}\), we have:

\[
\dot{x}(t) = [A_{att}]x(t) + [B_{def}]u_{def}(t)
\]

(5)

The system will be structurally resilient if the attacker is unable to disrupt structural controllability. The next result gives certain guarantees on structural resilience to a state feedback integrity attack depending on its resilience to a DoS attack. Let \(m_A\) and \(m_{A_{att}}\) denote the number of right unmatched vertices in a maximum matching of \(\mathcal{R}(A)\) and \(\mathcal{R}(A_{att})\).

**Theorem 4.8:** If the system in \((A) + [B_{def}]\) is structurally resilient to a DoS attack for some \([B_{def}]\) with zero structure \(\mathcal{Z}(B_{def})\), then there exists a \([B'_{def}]\) with \(\mathcal{Z}(B'_{def}) \subseteq \mathcal{Z}(B_{def})\) for which it will also be structurally resilient to a state feedback integrity attack. Moreover, if

\[
m_{A_{att}} + \beta_{A_{att}} - \alpha_{A_{att}} = m_A + \beta_A - \alpha_A
\]

(6)

for some \([B_{def}]\) corresponding to the DoS case, then the same \([B_{def}]\) will ensure structural resilience to a state feedback integrity attack.

**Proof:** Addition of edges corresponding to \([B_{att}]K_{att}\) to \([A]\) will ensure that the number of right unmatched vertices in a maximum matching of \([A_{att}]\) can only be as much as the number of right unmatched vertices in a maximum matching of \([A]\). Therefore, \(m_{A_{att}} \leq m_A\). From Theorem 4.2 and equation 3, structural resilience to a DoS attack implies \(|U_{def}| \geq m_A\) holds. This gives \(|U_{def}| \geq m_{A_{att}}\).

If the inequality (5) holds, then \(|(U_{def} - X)| \geq m_{A_{att}} + \beta_{A_{att}} - \alpha_{A_{att}}\), and no additional links between inputs and states will have to be added to ensure structural controllability, and \([B'_{def}] = [B_{def}]\). Additional links will have to be added if (6) does not hold. This corresponds to adding free parameters to \([B_{def}]\), giving \([B'_{def}]\), which satisfies \(\mathcal{Z}(B'_{def}) \subseteq \mathcal{Z}(B_{def})\).

It is important to note that structural resilience to DoS attacks guarantees structural resilience to only state feedback integrity attacks. It does not, in general, ensure structural resilience to arbitrary integrity attacks.

V. Examples

**Example 5.1:** Fig. 1a shows \(\mathcal{R}(A)\) with \(x_1,\ldots,x_6 \in X_{def}\) and \(x_7,\ldots,x_{10} \in X_{att}\). The SCCs are \((x_1,x_2,x_3),(x_8),(x_4,x_5,x_6,x_7)\), and \((x_9,x_{10})\), of
which the first two are not top linked. Every maximum matching of $\mathcal{D}(A)$ will have $x_8 \in \mathcal{X}_{\text{att}}$ as a right unmatched vertex. Thus, the system is not structurally resilient to a DoS attack. Now, add the edge $x_7 \rightarrow x_8$ to the digraph (Fig. (1b)). The SCCs are $(x_1, x_2, x_3), (x_4, x_5, x_6, x_7, x_8)$, and $(x_9, x_{10})$. Only the first SCC is not top linked, and there is only one right unmatched vertex in every maximum matching, and for some such matching, it is not in $\mathcal{X}_{\text{att}}$. Therefore, this system is structurally resilient to a DoS attack. If the edge, $x_6 \rightarrow x_7$ is removed (Fig. (1c)), then $(x_7, x_8)$ becomes a non-top-linked SCC, which necessitates the assignment of a control to it, making the system vulnerable to a DoS attack.

**Example 5.2:** In Fig. (1a), if a state feedback adds edges $x_7 \rightarrow x_8$ or $x_8 \rightarrow x_9$, then there exists a maximum matching of $\mathcal{D}(A_{\text{att}})$ with no right unmatched vertices or non-top-linked SCCs in $\mathcal{X}_{\text{att}}$, ensuring structural resilience to a state feedback attack. For the system in Fig. (1b), any state feedback $K_{\text{att}}$ will add edges to the set $\{x_7, x_8, x_9, x_{10}\}$. We know that this graph does not have right unmatched vertices in $\mathcal{X}_{\text{att}}$. This ensures structural resilience with the same $B_{\text{def}}$ as in the DoS case.

**Example 5.3:** For $A_{\text{def}}$ given by Fig. (1a, 1b, 1c), there is a non-top-linked SCC with vertices only in $\mathcal{X}_{\text{def}}$. Since controls in $\mathcal{U}_{\text{att}}$ cannot be assigned to vertices in $\mathcal{X}_{\text{def}}$, the systems are structurally resilient to an integrity attack. However, if $A_{\text{def}}$ is as in Fig. (2), all maximum matchings will have $x_8$ unmatched. An attacker can control the system by supplying an input to $x_8$, and the system will not be structurally resilient to an integrity attack.

**VI. Conclusion and Future Work**

The structural resilience of cyber physical systems to attacks was studied using linear structured systems and graph theory. Throughout this paper, we have assumed that the system and the attacker have access to disjoint sets of nodes. Analyzing structural resilience when there is a set of nodes accessible to both is a topic of interest. When the system successfully thwarts an attack, the attacker might want to ensure that the system incurs a high cost in maintaining resilience, while keeping its own cost of carrying out the attack low. Another problem of interest is the robustness of the system to the worst possible attack. We aim to formulate these scenarios as optimization problems. Finally, this analysis can be extended to distributed systems when the system as a whole is resilient, despite successful attacks to a set of its subsystems.
REFERENCES


