Detecting and Isolating Attacks of Deception in Networked Control Systems

Kiriakos Kiriakidis, Tracie Severson, and Brian Connett
Department of Weapons and Systems Engineering
United States Naval Academy
Annapolis, MD 21402
{kiriakid, severson, connett}@usna.edu

Abstract—This paper investigates a category of cyber-attacks on control systems, which regulate processes of a single plant while sharing a communication network. The design of these attacks aims to deceive conventional fault detectors that test locally generated residuals for inconsistent statistics. The authors propose a network-wide attack detector and isolator that collects information from other neighborhoods subject to availability of locality and network resources. Their method relies on estimating the output of a process, whose regulator may be under attack, from measurements gathered at other processes connected to the one under examination through links existing at the physical layer. Next, a notional consensus network coalesces all of these estimates into information that is independent of possibly deceptive sensory data at the suspect locality. The thesis of this paper is that residuals generated from far-flung estimates will reveal an anomaly (even if the statistics of local residuals are consistent). A necessary condition is the existence of an observable subsystem within the physical network of interconnected processes. The authors employ graph theory techniques to identify the subsystem and optimize its observability.

I. Introduction

Critical and non-critical global infrastructures have evolved into Cyber-Physical Systems (CPS) as expounded in [1]. Inherent in CPS are vulnerabilities that can be exploited at the lower physical level rather than at traditional attack-surface levels which exists in the upper layers of Open Source Interconnection (OSI) model [2]. The highest level of the OSI seven-layer model consists of all application-entities that operate inside the OSI environment, whereas the lowest levels provide the services through which those applications operate. Supervisory Control and Data Acquisition or SCADA systems are gaining attention in literature as those types of control and management systems which epitomize the aforementioned weakness in an ever-aging national and global automated system of utilities and accommodations [3]. Specifically, energy and transportation sectors are postured to realize the greatest effects of tangible cyber-effects delivered upon its command, control, and actuation systems. While well-known examples of electrical blackouts, air-gapped zero-day worms, and industrial security incidents are often used for introduction and motivation, it is important to remain vigilant and continue exploration of the cyber realm that is seemingly ubiquitous.

As a category of CPS, Networked Control Systems (NCS) are consistent with established Wireless Integrated Network Sensors (WINS) which provide the ability to define and operate clustered or distributed communication methods over various distances and protocols required for a System of Systems or SoS to behave as directed [4], [5]. One of the most attractive features of WINS is its rapid deployment, low-costs and scalability, but the same provides for adversarial actors who desire access to any network node assigned to a controller, actuator, or sensor. Furthermore, it is possible that malicious agents interfere with the behavior of any given node on the system without an apparent effect; herein lay the motivations of addressing attacks of deception on NCS.

The fly-by-wire aircraft used by most today are in many ways the most vulnerable of CPS examples available. A Federal Register submitted through the Department of Transportation to the Federal Aviation Administration [6], identifies commercial aircraft that will have "increased connectivity with external network sources and will have more interconnected networks and systems, such as passenger entertainment and information services than previous airplane models." The growth and scaling of NCS allow direct access between components of functionally separate subsystems such as control and navigation, operator information services, and passenger entertainment.

The United States Navy is quickly evolving into a cyber-consumer and cyber-target simultaneously. The advanced naval capabilities described in the Hull, Mechanical and Electrical (HM&E) roadmap are advanced sensors, directed energy weapons, and hypersonic technologies [7]. Together these three major topics of the future should require wireless sensor nodes and edges that are countless and immeasurable. The attack surfaces that would exist due to complexity of the architecture could result in vulnerability to interference with the programmable logic controllers connecting shipboard physical systems. Resilient Hull, Mechanical and Electrical Security or RHIMES system "aims to prevent" such schemes [8].

In each of these motivating examples, it is evident that detection and identification of attacks at the lower physical

This work was supported by the Office of Naval Research under the Cyber Innovation Grant N0001415WX01529.

level is critical to the well-being of the overall system. The ultimate goal is to improve upon established fault tolerance of distributed systems that succumb to known Byzantine failures [9].

In view of numerous possibilities of attacks, the scope of the present work is narrow addressing specifically attacks of deception. These attacks manage to introduce an anomaly in one of the sensor nodes of the NCS without any of the statistical characteristics of a fault. The proposed method lies within the system-theoretic framework for cyber-attacks presented in [10]–[12]. Furthermore, the present paper focuses solely on anomaly detection and identification leaving other facets of the problem such as its effect on the performance of the NCS for future work.

The contributions of the present paper to the aforementioned system-theoretic framework are the following: 1) a novel scheme for detection of anomalies such as Attacks of Deception—not merely detection of faults or bad data; 2) a graph-theoretic method for the identification of observable subgraphs (on the physical layer of the NCS), which constitute the basis for anomaly detection; and 3) the application of consensus techniques to weigh in estimates from subgraph-based observers and, eventually, to resolve the anomaly detection. The scope of the present work has been further limited to consider the possibility of one attack at a time, as the authors aim is proof of concept. In future, the authors will extend their work to multiple attacks and address the question of existence of a "core" of trusted sensor nodes.

In Section II-B, the authors introduce anomaly detection from far-flung observations. Predictions the output of the sensor–suspect of anomalous behavior–are based on measurements gathered at other processes connected to the one under examination through links existing at the physical layer. This is a departure from reliance on local predicted residuals, which the basis of fault detection literature [13]–[15]. Section II-C investigates the feasibility of estimating a state variable–whose direct measurement is suspect–from available sensors elsewhere in the NCS. Drawing upon the theory of observable subgraphs [16], [17], the authors develop an approach to identify observable albeit reduced-order models as bases for state reconstruction. The fusion of multiple estimates of the state variable of interest is presented in Section II-D. There is variability in the estimates due to differences in model fidelity as well as sensory modality. The authors introduce a strongly connected ad hoc network and implement an average consensus algorithm [18]. Consensus algorithms are tolerant to time-varying, directed communication links [19] and time-delayed communication [20]. Of the two tangible components of the proposed system, the ad hoc consensus network adds to the overhead cost of the NCS; the far-flung observers can run on existing hardware, in lieu of local fault detectors, and incur no additional cost to overhead.

The final cause of the work has been inspired by the "fast" and "slow" architectures describing two modes of human reasoning: heuristic and rational decision-making [21]. For many years, the dichotomy has been the central thesis of research in the field of psychology. Furthermore, these systems of thought as stimulated by external and internal events express various degrees of environmental and self awareness, respectively. In the field of engineering, where artificial intelligence remains elusive, designs that emulate "fast" and "slow" behavior may lead to autonomic decision-making by degree of awareness.

II. NCS with Self-Awareness

Figure 1 depicts NCS with multiple processes. Shown is a typical SISO loop including sensor, $\mathbf{S}_i$, controller, $\mathbf{CON}_i$, and actuator, $\mathbf{ACT}_i$. The horizontal double solid line represents the communication layer of the NCS. The sensor $\mathbf{S}_i$ is shown under Attack of Deception (AoD). Specific to the proposed approach, unit $\mathbf{O}_j^{(i)}$ is an estimator of process i from data collected at location j. The NCS interface with the physical network modeled in the next section.

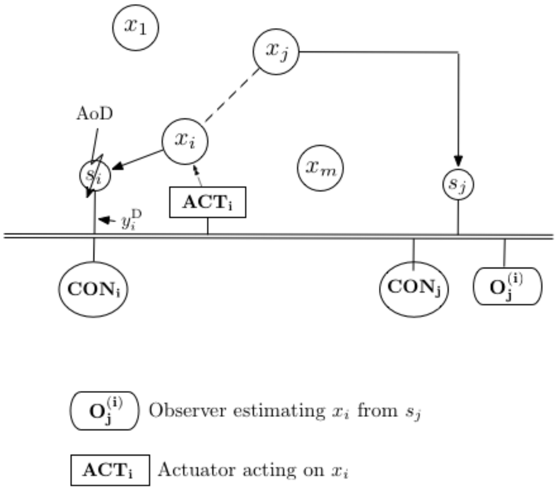

Fig. 1: Networked Control Systems

A. The Physical Network

The variables x_i, $i = \{1,\ldots,n\}$, in Fig. 1 represent, respectively, the states of processes under the NCS. Without loss of generality, each state is scalar and its value equals the deviation of the physical variable of the process from its operating point. Normally, the deviation from the operating point of a process is expected to settle at zero. Interconnections between any two processes at the physical layer (e.g., dashed line in Fig. 1), are captured by the adjacency matrix $M = [m_{ji}]$. By convention, $m_{ji} = 1$ indicates an edge issued from x_j to x_i; $m_{ji} = 0$ no edge. Let x be the vector of the states of all processes. Assuming linearity, the aggregate state evolves as follows:

$$\dot{x} = Ax \tag{1}$$

The state matrix A is decomposed as follows:

$$A = M^T \circ P \tag{2}$$

where $\circ$ denotes the Hadamard product and P the matrix of model parameters.

A subset of $r < n$ processes is regulated by means of SISO control systems. The remainder of processes are unregulated. Denote regulated states as x_{i_q} where $q = \{1, \ldots, r\}$ and i_q takes values in $\{1, \ldots, n\}$. The anatomy of the i-th row of the state matrix A reveals the equation below:

$$\dot{x}_i = a_{ii} x_i + \sum_{j \neq i} a_{ij} x_j$$

For the regulated i_q-th process, the diagonal entry of A is as follows:

$$a_{i_q i_q} = a_{i_q} + b_{i_q} u_{i_q}$$

The input u_{i_q} is produced by the controller $\mathbf{CON}_{i_q}$ below:

$$u_{i_q} = -k_{i_q} y_{i_q}$$

Normally, the output y_{i_q} of the sensor $\mathbf{S}_{i_q}$ is an ideal measurement of the state

$$y_{i_q} = c_{i_q} x_{i_q}$$

The following is a working assumption for the proposed approach. The state matrix A is diagonally dominant by row when all of the state variables x_{i_q} are regulated. For the attacks of deception considered, it remains diagonally dominant (and hence stable) after the event of attack.

B. Anomaly Detection via Physical Network

Consider the replay attack introduced in [22]. Suppose sensor $\mathbf{S}_{i_q}$ reports a recorded version of its output, $y^{\mathrm{D}}_{i_q}$, to the fault detector while it is feeding back an attack signal, $y^{\mathrm{A}}_{i_q}$, to the controller $\mathbf{CON}_{i_q}$. Such deception attack on the regulated process i_q achieves two objectives. First, the equation of the i_q-th process becomes:

$$\dot{x}_{i_q} = a_{i_q} x_{i_q} - b_{i_q} k_{i_q} y^{\mathrm{A}}_{i_q} + \sum_{j \neq i_q} a_{i_q j} x_j$$

and, as a result, the process is no longer regulated. At minimum, absence of regulating action will allow x_{i_q} to deviate from its operating point at zero.

Second, by sending back past recordings of data, the sensor $\mathbf{S}_{i_q}$ evades detection. Typically, fault detection is based on the predicted residuals:

$$y_{i_q} - \hat{y}_{i_q}$$

where $\hat{y}_{i_q}$ is the output of the estimator. Then, a fault would be detected should these residuals be inconsistent with their theoretical statistics [23]. Clearly, such is not the case for $y^{\mathrm{D}}_{i_q} - \hat{y}^{\mathrm{D}}_{i_q}$.

The present work posits that anomalous behavior of sensor $\mathbf{S}_{i_q}$ is detectable from data available elsewhere in the physical network. Indeed, there will be repercussions due to the first objective of the deception attack that other regulated process are able to sense. Using data from those sensors, the authors propose the anomaly detector as an alternative. Multiple estimators $\mathbf{O}^{(i_q)}_{i_s}$, $s \neq q$, produce local estimates $\hat{y}_{(i_q, i_s)}$, respectively. Potentially, there could be as many observers as regulated states hence $s = \{1, \ldots, r\}$ and i_s takes values in $\{1, \ldots, n\}$. The next section identifies such observers using a graph-theoretic criterion; in the section after, the identified estimators form an ad hoc sub-network whose objective is to reach consensus regarding the $\hat{y}_{i_q}$.

C. Identifying the Observable Subgraph

To be able produce estimates, $\hat{y}_{(i_q, i_s)}$, locally, the state variable x_{i_q} must be reconstructable from data gathered at $\mathbf{S}_{i_s}$ and local knowledge of the model. In general, the model (A, C_{i_s}) is not observable; here, the matrix C_{i_s} maps the aggregate state, x, to the output y_{i_s}. The authors develop an approach to identify observable albeit reduced-order models $(A^{(i_q)}_{i_s}, C^{(i_q)}_{i_s})$ as bases for state reconstruction.

To illustrate, consider the following model representative of fluid flow through a cascade of chemical reactors:

$$A = \begin{bmatrix} a_{11} & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & a_{32} & a_{33} & 0 \\ 0 & 0 & a_{43} & a_{44} \end{bmatrix}$$

The state variables x_1, x_2, and x_3 are regulated; x_4 is not regulated. The regulated state variables are sensed by $\mathbf{S}_1$, $\mathbf{S}_2$, and $\mathbf{S}_3$ with output matrices respectively

$$C_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}$$
$$C_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}$$
$$C_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}$$

State variable x_4 is not sensed. To test the hypothesis that sensor $\mathbf{S}_1$ is under deception attack, the proposed approach seeks to reconstruct state variable x_1 from available sensors $\mathbf{S}_2$ and $\mathbf{S}_3$. Neither model (A, C_2) nor (A, C_3), however, is observable. Figure 2 depicts the digraph of the process. Next, the approach employs the main result of an early work on controllable subspaces [16]. The graph of an unobservable model contains a maximal subgraph whose number of edges determines the dimension of the model's observable subspace. For single output models—here, (A, C_2) or (A, C_3), candidate subgraphs consist of one simple directed path, which ends at the output node.

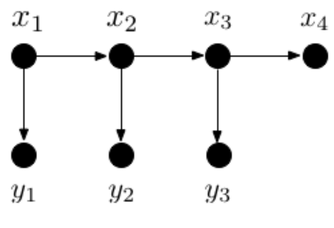

Fig. 2: Digraph representation of a process

The proposed approach constrains the number of candidate subgraphs to ones that contain the node of the state variable to be estimated—here, x_1. Such candidate subgraphs are associated with reduced-order models that could be used to reconstruct the state variable and hence the sensor output in the hypothesis.

As stated here, the problem of finding the maximal subgraph is a constrained version of the one in [16]. To the best of the authors knowledge, there is no algorithm to solve for the maximum single path that ends at the output node and includes the node of interest. Alternatively, one could aim for the maximum path that starts at the node of interest and ends at the output node. Since the maximum cannot be computed in polynomial time for every graph, the authors solve for the minimum path instead. Once these minimum paths have been identified, one collects all of the nodes in their corresponding subgraphs and forms reduced-order models.

Equivalently, the reduced-order models are obtained from the state matrix A by eliminating rows and columns associated with those state variables not included in their respective subgraph. Here, the resulting reduced-order models $(A_2^{(1)}, C_2^{(1)})$ and $(A_3^{(1)}, C_3^{(1)})$ are

$$A_2^{(1)} = \begin{bmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{bmatrix}, \quad C_2^{(1)} = \begin{bmatrix} 0 & 1 \end{bmatrix}$$

$$A_3^{(1)} = \begin{bmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ 0 & a_{32} & a_{33} \end{bmatrix}, \quad C_3^{(1)} = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$$

Then, local estimates of y_1, namely, $\hat{y}_{(1,2)}$ and $\hat{y}_{(1,3)}$ can be reconstructed from data gathered at $\mathbf{S}_2$ and $\mathbf{S}_3$, respectively.

D. The Consensus ad hoc Network

Suppose that a number of $t < r-1$ observable reduced-order models $(A_{i_s}^{(i_q)}, C_{i_s}^{(i_q)})$ have been obtained. To test the hypothesis that sensor $\mathbf{S}_{i_q}$ is under AoD, the group of observers $\mathbf{O}_{i_s}^{(i_q)}$ reaches agreement on the global estimate, $\hat{y}_{i_q}$, by means of the average consensus algorithm [18]. The consensus algorithm requires information exchanges between each observer and its neighbors in the group necessitating an ad hoc network within the existing NCS [24]. Consensus algorithms are guaranteed to converge even under very mild assumptions on the communication network [25]. They are tolerant to time-varying, directed communication links [19] and time-delayed communication [20].

Following on the AoD defined in Section II-B, each observer's estimate evolves according to the continuous-time dynamics [24]

$$\dot{\hat{y}}_{(i_q,i_s)} = \sum_{i_p} (\hat{y}_{(i_q,i_s)} - \hat{y}_{(i_q,i_p)}) \tag{3}$$

where the cardinal number of the index set for i_p is equal to t. The initial "far-flung" estimate solved for by each $\mathbf{O}_{i_s}^{(i_q)}$ is updated in way to reach agreement on a single global estimate. Foreshadowing the example in the next section, Fig. 3 illustrates the ad hoc consensus network comprising three observers $\mathbf{O}_3^{(1)}$, $\mathbf{O}_5^{(1)}$, and $\mathbf{O}_9^{(1)}$ depicted by their respective indices 3, 5, and 9. The pieces of information passed from node to node are estimates of the output, y_1, of the process under attack in order to reach consensus.

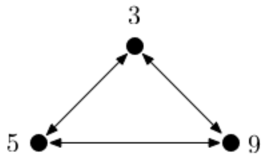

Fig. 3: Consensus ad hoc network.

III. Example: Attack of Deception

Consider an NCS interfacing with $n = 9$ processes interconnected at the physical layer according to the adjacency matrix below:

$$M = \begin{bmatrix} - & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & - & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & - & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & - & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & - & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & - & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & - & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & - & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & - \end{bmatrix}$$

State variables x_i, for $i = \{1,\ldots,9\}$, are deviations of the physical variable of each process from its respective operating point. Under normal conditions, then, x_i are expected to settle at zero. For the purposes of the example, there are as many sensors, $\mathbf{S}_i$, with outputs y_i, $i = \{1,\ldots,9\}$.

Consider the hypothesis that sensor $\mathbf{S}_1$ is under attack of deception, as defined in Section II-B. Accordingly, sensor $\mathbf{S}_1$ reports $y_1^{\mathrm{D}} = 0$ to the anomaly detector; it feeds back the attack signal y_1^{A} to controller $\mathbf{CON}_1$. Therefore, the process is no longer regulated and x_1 deviates from its operating point at zero. Through the interconnections at the physical layer the deviation of x_1 can be assessed from other sensors across the NCS.

First, one searches among available sensors for those sensors connected to state variable x_1 via simple paths. The method of the present paper uses minimum paths. There are three sensors, namely, $\mathbf{S}_j$, $j = \{3,5,9\}$, whose respective outputs y_j, $j = \{3,5,9\}$, are end nodes on three paths starting at state variable node x_1.

Second, from each of the resulting paths, one constructs a reduced order model $(A_j^{(1)}, C_j^{(1)})$, $j = \{3,5,9\}$, which is observable. Figure 4 represents the "observability adjacency" graph for state variable x_1, where the minimum paths are depicted as edges.

Third, one designs observers $\mathbf{O}_j^{(1)}$, $j = \{3,5,9\}$, to estimate the state x_1 from outputs y_j, $j = \{3,5,9\}$. The estimates of y_1, namely, $\hat{y}_{(1,j)}$, $j = \{3,5,9\}$ are the initial values of the respective nodes of the consensus ad hoc network on Fig. 3, which is connected and undirected. Fig. 5 shows the original estimates as well as convergence to the final global estimate of state $\hat{y}_1 = 1.48$. The result supports the hypothesis that the report of sensor $\mathbf{S}_1$ is an anomaly.

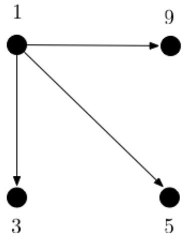

Fig. 4: Observability adjacency matrix for x_1.

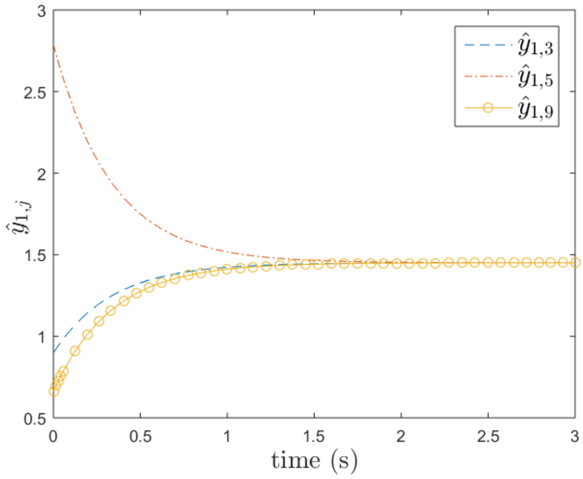

Fig. 5: Consensus of estimates for the output of suspect sensor $\mathbf{S}_1$.

IV. Conclusion and Future Work

The authors have proposed a method for detecting and isolating Attacks of Deception (AoD) on Networked Control Systems (NCS). The main novelty of the approach is the leveraging of the interconnections between processes at the physical layer. Its success relies on the identification of observable subgraphs in the adjacency matrix of the Physical Network. The ad hoc consensus network adds to the overhead cost of the NCS; the far-flung observers can run on existing hardware, in lieu of local fault detectors, and incur no additional cost to overhead. The preliminary results in the present paper demonstrate proof of concept for the case of a single attack at a time. In future, other facets of the problem such as the effect of AoD on the performance of the NCS will be investigated. Furthermore, the authors will extend their work to multiple attacks and address the question of existence of a “core” of trusted sensor nodes.

References

[1] K.-D. Kim and P. R. Kumar, “Cyber-physical systems: A perspective at the centennial,” Proceedings of the IEEE, vol. 100, pp. 1287–1308, 2012.

[2] ISO, Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model. ISO/IEC 7498-1, 1994.

[3] C. Rieger, D. Gertman, and M. McQueen, “Resilient control systems: Next generation design research,” in 2nd Conference on Human System Interactions, May 2009, pp. 632–636.

[4] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, “A survey of recent results in networked control systems,” Proceedings of the IEEE, vol. 95, no. 1, pp. 138–162, 2007.

[5] J.-C. Chin, l H. Hou, J. C. Hou, C. Ma, N. Rao, M. Saxena, M. Shankar, Y. Yang, and D. Yau, “A sensor-cyber network testbed for plume detection, identification, and tracking,” in 6th International Symposium on Information Processing in Sensor Networks, Apr. 2007, pp. 541–542.

[6] FAA, “Dept. of Trans.” 14 CFR Part 25, vol. 78, no. 222, pp. 68 985–6, 2013.

[7] T. Martin, W. L. Gray, and J. M. Voth, Hull, Mechanical, and Electrical (HM&E) Roadmap: Revolutionizing Naval Warfare and Achieving Energy Security. Washington Navy Yard, DC, 20376: Naval Sea Systems Command, 2012.

[8] J. Hsu, “Navy diversifies ships’ cyber systems to foil hackers,” in http://spectrum.ieee.org/tech-talk/computing/software/navy-diversifies-ships-cyber-systems-to-foil-hackers, Retrieved on 29 September 2015.

[9] M. Castro and B. Liskov, “Practical byzantine fault tolerance and proactive recovery,” ACM Transactions on Computer Systems, vol. 20, pp. 398–461, 2002.

[10] Y. Mo and B. Sinopoli, “False data injection attacks in control systems,” in First Workshop on Secure Control Systems, Aug 2010.

[11] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” ACM Transactions on Information and System Security, vol. 14, no. 1, 2011.

[12] F. Pasqualetti, F. Dorfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715–2729, 2013.

[13] J. L. Tylee, “On-line failure detection in nuclear power plant instrumentation,” IEEE Transactions on Automatic Control, vol. 28, no. 3, pp. 406–415, 1983.

[14] R. Tarantino, F. Szigeti, and E. Colina-Morles, “Generalized luenberger observer-based fault-detection filter design: an industrial application,” Control Engineering Practice, vol. 8, pp. 665–671, 2000.

[15] F. Alrowaie, R. B. Gopaluni, and K. E. Kwok, “Fault detection and isolation in stochastic non-linear state-space models using particle filters,” Control Engineering Practice, vol. 20, pp. 1016–1032, 2012.

[16] S. Hosoe, “Determinaiton of generic dimensions of controllable subspaces and its application,” IEEE Transactions on Automatic Control, vol. 25, no. 6, pp. 1192–1196, 1980.

[17] T. Boukhobza, F. Hamelin, and S. Martinez-Martinez, “State and input observability for structured linear systems: A graph-theoretic approach,” Automatica, vol. 43, pp. 1204–1210, 2007.

[18] K. Cai and H. Ishii, “Average consensus on general strongly connected digraphs,” in Proc. of the 28th American Control Conference (ACC), 2012, pp. 14–19.

[19] W. Ren and R. Beard, “Consensus seeking in multi-agent systems under dynamically changing interaction topologies,” in IEEE Trans. Autom. Control, vol. 50, May 2005, pp. 655–661.

[20] R. Saber and R. Murray, “Consensus problems in networks of agents with switching topology and time-delays,” IEEE Transactions on Automatic Control, vol. 49, no. 9, September 2004.

[21] D. Kahneman, Thinking Fast and Slow. Farrar, Strauss, and Giroux, 2011.

[22] Y. Mo and B. Sinopoli, “Secure control against replay attacks,” in Forty-Seventh Annual Allerton Conference, Sept 2009.

[23] A. H. Jazwinski, Stochastic Processes and Filtering Theory. Dover Publications, Inc., 1970.

[24] R. Saber and R. Murray, “Consensus and cooperation in networked multi-agent systems,” in Proceedings of the IEEE, vol. 95, Jan 2007, pp. 215–223.

[25] W. Ren, R. Beard, and E. Atkins, “A survey of consensus problems in multi-agent coordination,” American Control Conference, pp. 1859–1864, June 2005.