SECURE DISTRIBUTED ESTIMATION IN CYBER-PHYSICAL SYSTEMS

Usman A. Khan and Aleksandar M. Stanković

Department of Electrical and Computer Engineering, Tufts University, Medford, MA, 02155.
{khan,astankov}@ece.tufts.edu

ABSTRACT

Distributed estimation is where the state of a dynamical system is to be estimated via a collection of geographically dispersed measurements over a sensor network. In order to implement the estimator, the sensors, in addition to sensing, implement a simple data fusion protocol that relies on inter-sensor communication. In this paper, we study distributed estimation of cyber-physical systems when there is an adversarial attack on the sensed and communicated information. We propose a novel methodology to address the detection of such attacks, and further incorporate appropriate remedial actions in the estimator. Our methodology is based on the notions of local consistency and nodal consistency and is further reinforced by the exploiting the underlying physical-layer in the cyber-physical description.

Index Terms— Distributed estimation, cyber-physical systems, information security, dynamical systems

1. INTRODUCTION

A cyber-physical system (CPS) features a tight combination of, and coordination between, the system's physical and computational elements, for example, the integration of the energy and information layer in electric power grids. Today, a pre-cursor generation of cyber-physical systems can be found in many diverse areas and is often referred to as embedded systems. In embedded systems, the emphasis tends to be more on the computational elements, and less on an intense link between the computational and physical elements. Unlike more traditional embedded systems, a full-fledged cyber physical system is typically designed as a network of interacting elements with a strong dependence on the underlying physical-layer.

The problem of dynamical system estimation is of key significance in CPS. Since the CPS may span a large geographical region, e.g., power grids, environment monitoring, and transportation models, estimation is to be considered when the measurements (observations) of the underlying dynamics are distributed over spatially diverse sensors that are able to communicate with each other. Future cyber-physical systems (CPS) have been envisioned to have an intricate cyber-layer over which the data is exchanged between essential system components for the purposes of control, estimation, and other systemic analyses. The wide-scale operation and socio-economic impacts of CPS demands such a cyber-layer to be secure and robust to communication and sensing threats.

Numerous results have been published within the broad area of networked estimation and control [1–3]. Most of these have focused on the effects of dropped communication packets or, more generally, the impact of irregular sensor sampling time patterns (see, e.g. [4–7]). The effect of the network in estimation and control has been considered traditionally using average-consensus [8]. A consensus-based estimator requires a very large number of messages exchanged within the sensor network between every two time-steps of the dynamics–implying the communication time-scale to be much faster than the dynamics [9–12]. To elaborate this, consider Fig. 1

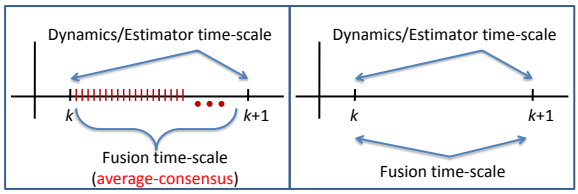

Fig. 1. (Left) Average-consensus based estimator. (Right) Proposed fusion approach.

(Left), where a large number of data fusion iterations are implemented between every two successive time-steps of the dynamics. This data exchanged is only on the measurements. To address this issue, estimators with finite messages exchanged have been proposed [13, 14]–a compromise between the two where only a finite messages are exchanged has been studied in [14].

In this paper, we consider estimators where the data (prior state-estimates and measurements) fusion is implemented with only one message exchanged, Fig. 1 (Right), and focus on the cyber-security aspects. We model the adversarial threat to a CPS as *compromised communication*–the communication link between two sensors is compromised, *compromised sensing*–the sensing modalities at a sensor are compromised, or a combination of both. To study distributed estimation under such attack categories, we propose statistical notions of *local consistency* and *nodal consistency*. The local consistency notion relies on the commonness among neighboring sensors, whereas, the nodal consistency notion exploits the patterns in the sensed information over time. We show that an appropriate attack detection can be cast using these statistical constructs, and further provide appropriate estimator adjustments in the presence of attacks. Finally, we exploit the physical-layer evident in the CPS description to improve the attack detection protocols.

Secure estimation of *dynamical* systems is largely unexplored in the literature. In the context of state-estimation, this problem is typically cast as bad data detection, see [15–18] and references therein, where the estimation is of a static parameter. Recent extensions to dynamic estimation have been proposed in the purview of information-theoretic security constructs, where analytical results are restricted to point-to-point communication, for example, see [19–22]. Of particular relevance is [23], which describes data-injection attacks and detection in smart grid, but is restricted to static estimation of dc power flow model and only considers a subset, i.e., the sensing model has an unknown constant shift, of what we categorize as *compromised sensing*. On the contrary, we place no such assumptions while the notions of *local* and *nodal consistency* can also be verified to be novel in the context of *dynamic* estimation.

We now describe the rest of the paper. Section 2 describes the distributed estimator and the cyber attack classification. We provide the secure estimation protocol in Section 3 with an illustrative example in Section 4. Finally, Section 5 concludes the paper.

2. ESTIMATOR AND ATTACK CLASSIFICATION

This section presents the dynamical system, distributed estimator, and the proposed cyber-attack models.

2.1. Distributed estimator

Networked estimation is to estimate the state variable, $\mathbf{x}_k$, in the CPS with distributed observations, $\mathbf{y}_k^i$, where the superscript denotes the geographically distributed nodes, $i = 1, \ldots, N$. The node here implies a workstation that has measurements, and is connected to nearby nodes via wireless–or wired–communication, see Fig. 2. To cast the proposed formulation in a proper mathematical context, we assume the following discrete-time LTI dynamics, perhaps after linearization and discretization. The system state, $\mathbf{x}_k \in \mathbb{R}^n$, at time $k \geq 0$ is given by

$$\mathbf{x}_{k+1} = A\mathbf{x}_k + \mathbf{v}_k, \qquad \mathbf{y}_k^i = C_i\mathbf{x}_k + \mathbf{r}_k^i, \tag{1}$$

where A is the system matrix–possibly linearized and discretized, and $\mathbf{v}_k \sim \mathbb{N}(0, Q)$ is the normally distributed system noise; whereas at each node i: $\mathbf{y}_k^i \in \mathbb{R}^{m_i}$ is the local observation vector, $C_i \in \mathbb{R}^{m_i \times n}$ is the local observation matrix and $\mathbf{r}_k^i \sim \mathbb{N}(0, R_i)$ is the local normally distributed observation noise.

We consider the single message exchanged state-estimator as proposed in [13]. Let $\widehat{\mathbf{x}}_{k+1}^i \in \mathbb{R}^n$ denote the estimate of $\mathbf{x}_k$ at node i and time $k+1$, given by

$$\widehat{\mathbf{x}}_{k+1}^i = A \sum_{j \in \mathcal{N}_i} w_{ij} \widehat{\mathbf{x}}_k^j + AB_i \sum_{j \in \mathcal{N}_i} C_j^T \left(\mathbf{y}_k^j - C_j \widehat{\mathbf{x}}_k^i \right), \tag{2}$$

for $w_{ij} \in \mathbb{R}_{\geq 0}$ such that $\sum_{j \in \mathcal{N}_i} w_{ij} = 1, \forall\, j$, and $B_i \in \mathbb{R}^{n \times n}$. At each node, the *consensus update*–first term in the sum, averages the prior estimates over the neighbors, whereas, the *innovation update*–second term in the sum, collects the observations at node i and its neighbors ($j \in \mathcal{N}_i$) to form the innovation, where B_i is the local innovation gain. Note that in (2), both the consensus step and the innovation step are implemented at the same time-step unlike the multiple consensus-steps schemes based on the seminal work in [9]. To keep the simplicity of the presentation, we make the following assumptions:
(i) Each node has direct state observations, i.e., the local matrices, $C_i^T C_i$'s, are diagonal.
(ii) The overall system is observable in 1 time-step, i.e, $\sum_{j=1}^N C_j^T C_j$ is invertible.
Both of these assumptions can be easily relaxed and the proposed estimator can be generalized accordingly, details can be found in [24]. The following result is from [13].

Lemma 1 *Let the network be strongly-connected and Assumption (ii) holds. The estimator in Eq.* (2) *has a bounded error* 2*-norm if* $\|A\|_2 < (\min_{W,B} \|W \otimes I - BD_C\|)^{-1}$*, where* $W = \{w_{ij}\}$ *and* $D_c = blkdiag\{\sum_{j \in \mathcal{N}_i}^N C_j^T C_j\}$*. Further the RHS of the above equation is*[1] > 1.

[1]In other words, under the Lemma's hypotheses, there are unstable dynamics that can be tracked with bounded error with estimator in Eq. (2). This particular result provides significant insights in distributed estimation as the rate at which the system evolves (potentially in an unstable direction) has to be less than the rate at which the information evolves–some function of the network communication and observation models.

2.2. Cyber-attack classification

As a starting point for the formulation of secure protocols, we assume the cyber threats have the following properties, see Fig. 2:

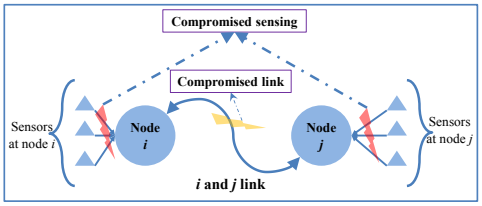

Fig. 2. Security concerns at distributed nodes.

(i) *Compromised communication*: An adversary gets control of one or more of the outgoing links at node i and sends meaningless information to one or more neighbors of node i. This is shown as the lightning symbol on the inter-sensor communication link in Fig. 2.
(ii) *Compromised sensors*: An adversary gets control of the sensors at node i and sends meaningless sensing information to node i. This is shown as the lightning symbol on the sensors in Fig. 2

This classification is further appended with the following two assumptions: (a-i) The number of compromised nodes (in either sensing or communication sense) in any neighborhood is much less than the number of non-compromised nodes; and (a-ii) The adversary is not an oracle in the context of the underlying system. In other words, the adversary does not have the complete physical and/or cyber knowledge of the underlying dynamics. Note that (a-i) is widely used on the adversaries, e.g., consider the F-local and F-global standard Byzantine adversary models [25–27]. Whereas, assumption (a-ii) is also natural as an adversary may obtain the seasonal variations, historical data, and other high-level system descriptors, but does not know the system transients and current operating points etc.

In the following, we will focus specifically on the *compromised communication* scenario. The case of *compromised sensing* will be considered elsewhere.

3. SECURE ESTIMATION

The aforementioned cyber-attack classification entails a large set of practical threats that can be targeted towards a CPS. Our philosophy towards designing secure protocols is to exploit the underlying physical models that are "in some sense" common across different CPS modules and provide a means to verify the information exchanged over the cyber-layer. We can broadly based the proposed solution on the following ideas.
(a) *Nodal consistency*: Any node i with an information (data)set $\mathcal{I}_i$ may declare its own dataset to be *trusted* if the evolution of this dataset is *statistically consistent* over time.
(b) *Local consistency*: Consider two directly connected nodes i and j with information (data)sets, $\mathcal{I}_i$ and $\mathcal{I}_j$. Assuming that the two datasets have information about a few common elements, node i may declare the entire $\mathcal{I}_j$ to be trusted if $\mathcal{I}_j$ is *statistically consistent* with $\mathcal{I}_i$ over the common elements.
(c) *Physical-layer feedback*: Any node i may declare itself, i, (or a neighbor j) to be *trusted* if the dataset, $\mathcal{I}_i$, (or $\mathcal{I}_j$ at node j) is *statistically consistent* with the physical-layer feedback from its neighbors.

It can be readily seen that the attack modeling (i-ii) and trust notions (a-c) are highly relevant to CPS, where the nodes are different modules that share, possibly very few, common elements and are inter-connected via a, possibly low-bandwidth, physical-layer feedback. Similarly, the trust notion (c) above exploits the fact that the information sets at any agent are highly coupled to the physical-layer interconnections. It is worth mentioning that the trust notions (a-c) are statistical. Finally, the notion of *statistically consistency* may refer to distribution shifts over time in (a), hypothesis testing towards establishing a level of trust in (b), and the statistical coupling between the physical-layer feedback and cyber data in (c).

Note that the above cyber attack classification is novel and is different from predominant models in the literature. This is because most of the cyber attack modeling is restricted to computer networks where an underlying physical-layer is either not present or ignored. For example, recent work on communication and consensus in the presence of adversaries, [25, 26, 28–30], does not consider the underlying physical-layer; primarily because the system is only driven by information and there is no physical phenomenon.

We now describe our approach to address the cyber security issue in networked estimation, however, the solution can be extended to other related problems.

3.1. Compromised communication

The following establishes the notion of *local consistency* introduced before. From Eq. (1), note that any two local observation vectors, $\mathbf{y}_k^i \in \mathbb{R}^{m_i}$ and $\mathbf{y}_k^j \in \mathbb{R}^{m_j}$ are not directly comparable as: (i) the dimensions may be different; and (ii) the corresponding elements of $\mathbf{y}_k^i$ and $\mathbf{y}_k^j$ may represent different state-variables. To circumvent this issue, we construct the auxiliary observations, $\widetilde{\mathbf{y}}_k^i \in \mathbb{R}^n$ as $\widetilde{\mathbf{y}}_k^i = C_i^T \mathbf{y}_k^i$, which does not only make each local observation to have the same dimension, but corresponding elements of $\mathbf{y}_k^i$ and $\mathbf{y}_k^j$ now represent the same state-variable across all auxiliary observations. The secure estimation that we propose exploits the *commonness* among the auxiliary observations.

Remark 1: It can be easily verified that node i can perform a meaningful estimation of the state-variables corresponding to the non-zeros in the auxiliary observation from its own measurements without relying on its neighbors. *However*, in order to estimate the state variables corresponding to the zeros in the auxiliary observations, node i has to rely on its neighbors; this is where compromised communication can be detrimental.

With the commonness among auxiliary observations and Remark 1, we describe the following protocol at each node. Let $\mathcal{N}_i$ denote the neighborhood of nodes i, i.e., $\mathcal{N}_i = \{i\} \cup \{j \mid j \to i\}$, where $j \to i$ means that node j can send information to node i. For each $j \in \mathcal{N}_i$, node i tabulates the commonness in the auxiliary observations, defined as $X_{ij} = \{x_\ell \mid \widetilde{\mathbf{y}}^i(\ell) \neq 0 \text{ and } \widetilde{\mathbf{y}}^j(\ell) \neq 0\}$, i.e., the collection of state variables for which both node i and node j has measurements. Subsequently, node i assigns a *trust index*, $t_{ij}(k)$, to every neighboring node as follows:

$$t_{ij}(k) = \frac{1}{K|X|_{ij}} \sum_{x_\ell \in X_{ij}} \sum_{m=1}^{k} (\widehat{x}_{m,\ell}^i - \widehat{x}_{m,\ell}^j), \tag{3}$$

where $\widehat{x}_{m,\ell}^i$ is the estimate of the ℓth state-variable at node i and time k. Note that the trust index is only defined on the common estimable states among node i and j. With the help of the trust index, $t_{ij}(k)$, node i declares the *trusted neighbors* at time k as $\overline{\mathcal{N}}_i(k) = \{j \in \mathcal{N}_i \mid t_{ij}(k) < \varepsilon_{ij}\}$, and the *compromised neighbors* as $\underline{\mathcal{N}}_i(k) = \mathcal{N}_i \setminus \overline{\mathcal{N}}_i(k)$. Finally, node i updates its state-estimate by assigning more weight to the trusted neighbors and less (or zero) to the compromised. The following results follow from Lemma 1, where $\overline{\mathcal{N}}(k) = \cup_i \overline{\mathcal{N}}_i(k)$ is the set of trusted nodes in the entire network, and the matrices $\overline{W}$ and $\overline{D_C}$ are W and D_C restricted to the nodes in $\overline{\mathcal{N}}(k)$.

Lemma 2 *Let $\sum_{j \in \overline{\mathcal{N}}(k)} C_j^T C_j$ be invertible for each k, and the trusted nodes are strongly-connected; the state-estimator described in Eq.* (2) *results in bounded estimation error if*

$$\|A\|_2 < \frac{1}{\min_{\overline{W},B} \|\overline{W} \otimes I - B\overline{D_C}\|}. \tag{4}$$

The following result can also be shown but the analysis is more involved than Lemma 2.

Lemma 3 *Let $\sum_{j \in \overline{\mathcal{N}}(k)} C_j^T C_j$ be invertible for infinitely many indices, k's, and the trusted nodes form a strongly-connected network, then the state-estimator described in Eq.* (2) *results in bounded estimation error if Eq.* (4) *holds.*

The proofs of the above lemmas are beyond the scope of this paper. However, an avid reader may notice that as the nodes start to become compromised they have to be taken out of the network, and the results on stable estimation error from [13] should be restricted to the set of trusted nodes alone. Furthermore, it can be seen that the above results can be extended to random topologies.

Computation of ε_{ij}: A significant question in the above formulation is how to compute ε_{ij} as this *threshold* is a significant contributor to the set of trusted neighbors. With some care, the design of ε_{ij}'s can be cast in a precise statistical context. For this purpose, let us analyze the statistics of the trust index, $t_{ij}(k)$, in Eq. (3). Assuming that each state-estimate, $\widehat{x}_{k,\ell}^i$, for all i's, is distributed as $\mathbb{N}(x_{k,\ell}, \sigma^2)$, one can show that $t_{ij}(k)$ is distributed as $\mathbb{N}\left(0, \sigma^2|X_{ij}|\right)$. Finally, the computation of ε can be cast in terms of the false alarm rate of the following hypothesis testing problem:

$$H_0 : t_{ij}(k) \sim N\left(0, \sigma^2|X_{ij}|\right),\ H_1 : t_{ij}(k) \sim N\left(\neq 0, \sigma^2|X_{ij}|\right).$$

The case when $\widehat{x}_{k,\ell}^i \sim \mathbb{N}(x_{k,\ell}, \sigma_i^2)$ can be easily adjusted in the above scenario. Finally, it is noteworthy that σ_i^2 can be estimated using the signal-to-noise-ratio at node i, i.e., from Eq. (1).

Remarks

(i) We provide a sliding window (type) approach to compute the trust index, $t_{ij}(k)$. However, an instantaneous computation can also be justified and the statistics can be adjusted accordingly.

(ii) Due to space limitations, we do not explore the compromised sensing scenario in this paper. However, note that the statistical notion of nodal consistency described earlier holds the key to address this particular cyber attack.

(iii) The proposed strategies of local and nodal consistency can be further refined by using the physical-layer feedback.

4. SIMULATIONS

Consider a simple $n = 5$ state, $\mathbf{x}_k = [x_{k,1}, x_{k,2}, \ldots, x_{k,5}]^T$, DT-LTI system with 5 nodes such that the ith node observes the ith state, $x_{k,i}$, and the $i+1$th state, $x_{k,i+1}$, except node 5 which observes $x_{k,5}$ and $x_{k,1}$. The nodes are connected as in Fig. 3. For example, node 3's observation model, $\mathbf{y}_k^{(3)} \in \mathbb{R}^2$, is

$$\mathbf{y}_k^{(3)} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \mathbf{x}_k + \mathbf{r}_k^{(3)}, \tag{5}$$

where $\mathbf{r}_k^i$ is chosen to be $\mathbb{N}(0, \sigma_i^2 I)$, $\forall i$ for simplicity. Similarly, $\mathbf{y}_k^{(2)}$ is also a vector in $\mathbb{R}^2$ but observes $x_{k,2}$ and $x_{k,3}$ and thus $\mathbf{y}_k^{(2)}$ and $\mathbf{y}_k^{(3)}$ cannot be compared directly. To avoid this issue, we construct auxiliary observations so that each $\widetilde{\mathbf{y}}_k^i \in \mathbb{R}^n$, e.g., $\widetilde{\mathbf{y}}_k^{(2)} = C_2^T(C_2\mathbf{x}_k + \mathbf{r}_k^{(2)})$, $\widetilde{\mathbf{y}}_k^{(3)} = C_3^T(C_3\mathbf{x}_k + \mathbf{r}_k^{(3)})$, where $C_2^T C_2$ is diagonal with 1's at $(2,2)$ and $(3,3)$ locations and zeros everywhere else; and $C_3^T C_3$ is diagonal with 1's at $(3,3)$ and $(4,4)$ locations and zeros everywhere else. This establishes the commonness among each node as the common non-zeros on the auxiliary observation matrices, $C_i^T C_i$. From Fig. 3, it is clear that node i and $i+1$ share an observation on the state $x_k^{\max(i,i+1)}$ (except for node 1 and 5, which share the first state, $x_{k,1}$).

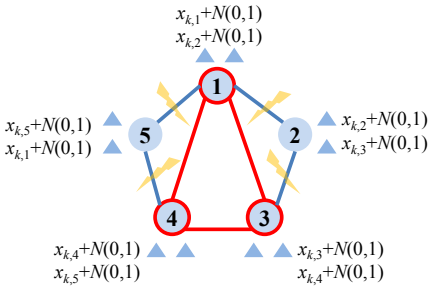

Fig. 3. Simulation setup.

We assume that the communication links from node 2 and node 5 are compromised such that instead of sending meaningful information to their neighbors, the adversary sends $\mathbb{N}(0, \sigma_a^2)$. In order for the (un-compromised) nodes $1, 3, 4$ to continue uninterrupted operation, node 1, for example, proceeds as the following, with respect to node 2: Let the local estimates of the common state between node 1 and node 2 be denoted by $\widehat{x}_{k,2}^{(1)}$ and $\widehat{x}_{k,2}^{(2)}$, respectively. Since the estimator in Eq. (2) is linear and unbiased [13], we have $\widehat{x}_{k,2}^{(\cdot)} \sim \mathbb{N}(x_{k,2}, \times)$, where $\times$ represent that the variance is ignored. This further leads to $t_{12}(k) =$

$$\begin{cases} \sum_{m=1}^{k} \left(\widehat{x}_{m,2}^{(1)} - \widehat{x}_{m,2}^{(2)}\right)^2 \sim \mathbb{N}(0, \times), & \text{No attack,} \\ \sum_{m=1}^{k} \left(\widehat{x}_{m,2}^{(1)} - \mathbb{N}(0, \sigma_a^2)\right)^2 \sim \mathbb{N}(\neq 0, \times), & \text{Attack.} \end{cases}$$

Over a sequence of time-steps k, node 1, thus, keeps track of the quantity $t_{12}(k)$ and follows the local consistency procedure described in Section 3.1. The precise hypothesis testing formulation requires a detailed computation of the corresponding co-variances (denoted as $\times$) that is beyond of the scope of this paper. However, regardless of the knowledge of σ_a^2, an effective zero-mean comparison can be devised on the sequence of $t_{ij}(k)$'s, see Fig. 5.

We simulate an $n = 5$-dimensional DT-LTI system with $\sigma_i^2 = \sigma_a^2 = 1$ and plot the sum of squared errors at each agent using the non-secure estimator, Eq. (2) in Fig. 4 (Top and Middle) for stable and unstable dynamics. Subsequently, Fig. 4 (Bottom) shows the secure estimation established in Section 3.1. Finally, we show a typical evolution of $t_{12}(k)$ from Eq. (3) in Fig. 5 under attack and no attack cases. It can be verified that for stable dynamics (Fig. 4 (Top)), attack or no-attack results in bounded estimation error (the performance under no attack is obviously better); this is because stable dynamics will eventually die out and the state itself remains bounded and hence a trivial estimate (e.g., 0) results in bounded estimation error.

The more interesting case is when the dynamics are unstable as the nodes under attack cannot perform a meaningful estimation while further degrading the performance of the non-attacked nodes (Fig. 4 (Middle)). Finally, note that Fig. 4 shows an average over 5000 Monte Carlo trials.

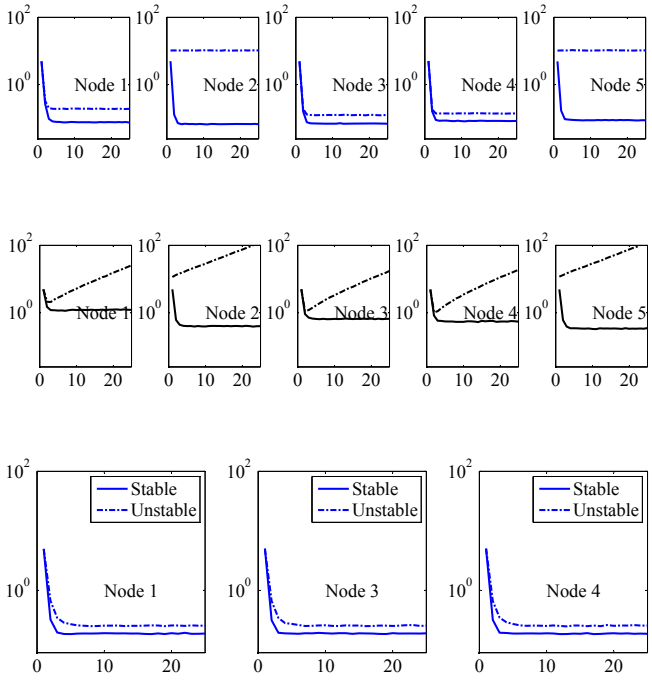

Fig. 4. Stable/unstable dynamics, largest eigenvalue of A is 0.5 (Top) and 1.05 (Middle). MSE (vertical) plotted against time-step, k (horizontal). (Top and Middle) Solid curve is no attack and dashed curve is cyber attack. (Bottom) Secure estimation: Solid curve is stable dynamics and dashed curve is unstable dynamics.

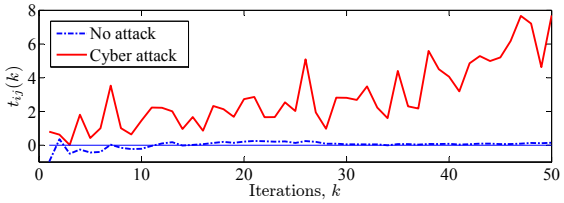

Fig. 5. Evolution of the trust index, $t_{12}(k)$.

5. CONCLUSIONS

This paper provides a novel security paradigm that is cast in a concrete setup of cyber attack models and the statistical consistency framework. The setup described has the potential to be generalized to nonlinear dynamics as the consistency notions and proposed trust indices are not restricted to linear models. As we described before, much of the related work in the literature assumes simplified cyber attacks and relatively simple attack detection strategies, while being restricted only to static estimation. Our formulation does not only provide a complete framework to describe and detect cyber attacks, but further derives appropriate estimator adjustments.

6. REFERENCES

[1] P. Antsaklis and J. Baillieul, "Special issue on technology of networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 5–8, Jan. 2007.

[2] O. C. Imer, S. Yűksel, and Tamer Başar, "Optimal control of LTI systems over unreliable communication links," *Automatica*, vol. 42, no. 9, pp. 1429–1439, 2006.

[3] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 163–187, Jan. 2007.

[4] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M.I. Jordan, and S.S. Sastry, "Kalman filtering with intermittent observations," in *42nd IEEE Conference on Decision and Control*, Dec. 2003, vol. 1, pp. 701–708.

[5] M. Micheli, *Random Sampling of a Continuous-time Stochastic Dynamical System: Analysis, State Estimation, and Applications:Research Project*, 2001.

[6] K. Plarre and F. Bullo, "On Kalman filtering for detectable systems with intermittent observations," *IEEE Transactions on Automatic Control*, vol. 54, no. 2, pp. 386–390, Feb. 2009.

[7] Y. Mo and B. Sinopoli, "A characterization of the critical value for Kalman filtering with intermittent observations," in *47th IEEE Conference on Decision and Control*, Dec. 2008, pp. 2692–2697.

[8] L. Xiao and S. Boyd, "Fast linear iterations for distributed averaging," *Systems and Controls Letters*, vol. 53, no. 1, pp. 65–78, Apr. 2004.

[9] R. Olfati-Saber, "Distributed Kalman filter with embedded consensus filters," in *European Control Conference*, Dec. 2005, pp. 8179–8184.

[10] R. Carli, A. Chiuso, L. Schenato, and S. Zampieri, "Distributed Kalman filtering using consensus strategies," in *46th IEEE Conference on Decision and Control*, Dec. 2007, pp. 5486–5491.

[11] U. A. Khan and J. M. F. Moura, "Distributing the Kalman filter for large–scale systems," *IEEE Transactions on Signal Processing*, vol. 56(1), no. 10, pp. 4919–4935, Oct. 2008.

[12] E. J. Msechu, S. D. Roumeliotis, A. Ribeiro, and G. B. Giannakis, "Decentralized quantized Kalman filtering with scalable communication cost," *IEEE Transactions on Signal Processing*, vol. 56, no. 8, pp. 3727–3741, Aug. 2008.

[13] U. A. Khan, S. Kar, A. Jadbabaie, and J. M. F. Moura, "On connectivity, observability, and stability in distributed estimation," in *49th IEEE Conference on Decision and Control*, Dec. 2010, pp. 6639–6644.

[14] U. A. Khan and A. Jadbabaie, "On the stability and optimality of distributed Kalman filters with finite-time data fusion," in *American Control Conference*, Jul 2011, pp. 3405–3410.

[15] F. F. Wu and W.-H. E.Liu, "Detection of topology errors by state estimation," *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 176–183, Feb. 1989.

[16] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation*, NewYork: Marcel Dekker, 2004.

[17] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM conference on Computer and communications security*, New York, NY, USA, 2009, pp. 21–32.

[18] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *2010 First IEEE International Conference on Smart Grid Communications*, Oct. 2010, pp. 214–219.

[19] L. Lai, K. Liu, and H. El Gamal, "The three-node wireless network: Achievable rates and cooperation strategies," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 805–828, Mar. 2006.

[20] L. Lai and H. El Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[21] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 476–486, Sep. 2011.

[22] V. Aggarwal, L. Sankar, R. A. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 1–14, Mar. 2009.

[23] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[24] U. A. Khan and A. Jadbabaie, "Coordinated networked estimation strategies using structured systems theory," in *49th IEEE Conference on Decision and Control*, Orlando, FL, Dec. 2011, pp. 2112–2117.

[25] C.-Y. Koo, "Broadcast in radio networks tolerating byzantine adversarial behavior," in *Proceedings of the twenty–third annual ACM symposium on Principles of distributed computing*, New York, NY, USA, 2004, pp. 275–282.

[26] N. H. Vaidya, L. Tseng, and G. Liang, "Iterative approximate byzantine consensus in arbitrary directed graphs," in *Proceedings of the 2012 ACM symposium on Principles of distributed computing*, New York, NY, USA, 2012, PODC '12, pp. 365–374.

[27] H. Zhang and S. Sundaram, "A simple median–based resilient consensus algorithm," in *50th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, Oct. 2012.

[28] R. M. Kieckhafer and M. H. Azadmanesh, "Low cost approximate agreement in partially connected networks," *Journal of Computing and Information*, 1993.

[29] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *J. ACM*, vol. 32, no. 2, pp. 374–382, Apr. 1985.

[30] S. Sundaram, S. Revzen, and G. J. Pappas, "A control-theoretic approach to disseminating values and overcoming malicious links in wireless networks," *Automatica*, vol. 48, no. 11, pp. 2894–2901, 2012.