SIMULTANEOUS DISTRIBUTED ESTIMATION AND ATTACK DETECTION/ISOLATION IN SOCIAL NETWORKS: STRUCTURAL OBSERVABILITY, KRONECKER-PRODUCT NETWORK, AND CHI-SQUARE DETECTOR

Mohammadreza Doostmohammadian[y?], Themistoklis Charalambous[y], Senior Member, IEEE, Miadreza Shafie-khah, Senior Member, IEEE, Nader Meskin, Senior Member, IEEE, and Usman A. Khan[z], Senior Member, IEEE

[y] School of Electrical Engineering, Aalto University, Espoo, Finland.
[?] Faculty of Mechanical Engineering, Semnan University, Semnan, Iran.
School of Technology and Innovations, University of Vaasa, Vaasa, Finland
Electrical Engineering Department, Qatar University, Doha, Qatar
[z] Electrical and Computer Engineering Department, Tufts University, Medford, MA, USA.

2021 IEEE International Conference on Autonomous Systems (ICAS) | 978-1-7281-7289-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICAS49788.2021.9551162

ABSTRACT

This paper considers distributed estimation of linear systems when the state observations are corrupted with Gaussian noise of unbounded support and under possible random adversarial attacks. We consider sensors equipped with single time-scale estimators and local chi-square (^{2}) detectors to simultaneously observe the states, share information, fuse the noise/attack-corrupted data locally, and detect possible anomalies in their own observations. While this scheme is applicable to a wide variety of systems associated with full-rank (invertible) matrices, we discuss it within the context of distributed inference in social networks. The proposed technique outperforms existing results in the sense that: (i) we consider Gaussian noise with no simplifying upper-bound assumption on the support; (ii) all existing ^{2}-based techniques are centralized while our proposed technique is distributed, where the sensors locally detect attacks, with no central coordinator, using specific probabilistic thresholds; and (iii) no local-observability assumption at a sensor is made, which makes our method feasible for large-scale social networks. Moreover, we consider a Linear Matrix Inequalities (LMI) approach to design block-diagonal gain (estimator) matrices under appropriate constraints for isolating the attacks.

Index Terms— Attack detection and isolation, Kronecker-product network, distributed estimation, ^{2}-test.

1. INTRODUCTION

The unprecedented large size of social networks mandates distributed sensing, inference, and detection [1–7], where the information is collected and processed locally while meeting certain security concerns. Recent distributed estimation protocols [6–11] are prone to faults/attacks that may result in inaccurate state estimates. Different attack detection and FDI (fault detection and isolation) strategies are thus proposed in the literature, ranging in applications from biological modeling [12] to smart-grid monitoring [13, 14], and from centralized approaches [15–20] to more recent distributed methods [21–23]. Among the centralized solutions, deterministic FDI and attack detection methods design decision thresholds based on the upper-bound on the noise support [17, 18], while, in contrast, probabilistic ^{2}-test with no such assumption on the noise is proposed in [15] and further developed in [19, 20]. Among the distributed strategies, [23] requires injecting a watermarking input signal conceding to a loss in the control/estimation performance, which is not applicable to autonomous systems (such as the social network model in this paper). In order to close this gap, this paper aims at developing a technique for distributed inference of autonomous (social) systems while simultaneously detecting and isolating adversarial attacks locally with no central coordinator.

The main contributions of this paper are as follows. (i) This work considers a windowed ^{2} benchmark to locally design probabilistic decision thresholds based on certain false alarm rates (FARs). This is in contrast to existing deterministic thresholds assuming certain upper-bound on the noise support [17, 18], which results in faulty outcome when the noise upper-bound is considerably larger than the attack/fault magnitude. (ii) This work extends the recent centralized ^{2} detectors [19, 20] to distributed ones, where the sensors are widespread over a large social network and, thus, the centralized solutions are infeasible/undesirable due to heavy communication loads or inability for parallel processing. In this direction, the notion of Kronecker-product network [24] is used to perceive (structural) observability of the composite social/sensor network, which allows to find

This work has been supported by the European Commission through the H2020 project FinEst Twins under grant agreement No 856602. The work of U. Khan was supported by NSF under awards #1903972 and #1935555. The work of T. Charalambous was supported by the Academy of Finland under Grant 317726. Corresponding email: doost@semnan.ac.ir, mohammadreza.doostmohammadian@aalto.fi.

minimal connectivity requirement on the sensor network for distributed estimation/detection. (iii) Our distributed technique, as in [21, 22], does not require local-observability at every sensor. However, unlike fixed biasing faults/attacks on sensor outputs in [21, 22], this work extends the results to general anomalies in the form of a random variable. In particular, we adopt the notion of distance measure [19], a scalar variable to compare the residual variance in presence and absence of attacks.

2. PROBLEM FORMULATION

We consider the interaction of individuals in a social network as a linear-structure-invariant (LSI) autonomous model [4–7],

$$x_{k+1} = Ax_k + {}_k; \qquad k \ 0; \tag{1}$$

where k is the time-step, A is the social system matrix associated with social digraph G, ${}_k \ N(0; Q)$ is additive i.i.d noise vector, and vector $x_k = x^1; : : : ; {}_k x^n{}^> \ 2 \ {}_k R^n$ represents the global social state. Note that n is the size of social network and x^i represents the i'th individual's social state, e.g., opinion, rumor, or attitude [1–7]. The state x^i of individual i at time k is a weighted average of the states $x^j_{k\ 1}$ of its in-neighbors in G and its own previous state $x^i_{k\ 1}$. This is well-justified for opinion-dynamics in social systems, and particularly implies that matrix A is (structurally) full-rank [7]. Consider N social sensors (agents or information-gatherers [5]) sensing the state of some individuals as,

$$y^i_k = H_i x_k + {}_k{}^i + {}_k{}^i \tag{2}$$

with H_i as the measurement matrix, ${}^i_k$ as possible attack and ${}^i_k \ N(0; R_i)$ as Gaussian noise at sensor i at time k. Define $R = diag[R_i]$ as the covariance matrix of the i.i.d noise vec-tor ${}_k$. Throughout this paper, without loss of generality, we assume every sensor observes one state variable, i.e., $y^i \ 2 \ R$. Further, as in similar works [15, 19, 20], we assume the sys-tem and measurement noise covariance (Q and R) are known. Then, sensors share their information over a sensor network G_N. Clearly, system A is not locally observable to any sen-sor, but globally observable to all sensors. The condition on $(A; H)$-observability is given in the following lemma.

Lemma 1 [7] Given a social network G (with structurally full-rank adjacency matrix A), if at least one social state is sensed in every strongly-connected-component (SCC) in G, then, the pair $(A; H)$ is (structurally) observable.

Given (social) system (1) and state observations (2) satisfying Lemma 1, we aim to design a distributed iterative procedure to simultaneously estimate the (social) state x^i_k while detecting adversary attacks at (social) sensors. The attack by the adversary is modeled as an additive random term ${}^i_k$ at sensor i in (2). The proposed distributed estimation makes the entire system observable to every sensor, and the attack-detection technique enables each sensor to locally detect anomalies in its observation with a certain FAR (false-alarm rate).

3. MAIN ALGORITHM

We consider a modified version of the single time-scale distributed estimator in [7] with one step of averaging on a-priori estimates (similar to DeGroot consensus model [8]) and one step of measurement update (also known as innovation [8]),

$$\hat{x}^i_{kjk\ 1} = \sum_{j \ 2 \ N(i)} w_{ij} A\hat{x}^j_{k\ 1jk\ 1}; \tag{3}$$

$$\hat{x}^i_{kjk} = \hat{x}^i_{kjk\ 1} + K_i H_i{}^> \ y^i_k \quad H_i \hat{x}^i_{kjk\ 1} : \tag{4}$$

with stochastic matrix $W = fw_{ij}g$ as the adjacency matrix of the sensor network G_N representing the fusion weights among the sensors, K_i as the local gain matrix at agent i, and $\hat{x}^i_{kjk\ 1}$ and $\hat{x}^i_{kjk}$ as the state estimate at time k given all the information of agent i and its in-neighbors $N(i)$, respectively, at time $k \ 1$ and k. In contrast to double time-scale estimators/observers [11] with many consensus iterations between every two consecutive time-steps $k \ 1$ and k of social dynamics (1), the estimator (3)-(4) performs one iteration of information fusion between steps $k \ 1$ and k, which is more efficient in terms of computation/communication loads.

Define the estimation error at agent i as $e^i_k = x_k \quad \hat{x}^i_{kjk}$ and the error vector $e_k = e^{1>}_k; : : : ; e^{n>}_k{}^>$. Following similar procedure as in [6], the error dynamics is as follows,

$$e_k = (W \quad A \quad KD_H(W \quad A))e_{k\ 1} + q_k; \tag{5}$$

with $D_H = diag[H_1{}^> H_i]$, $K = diag[K_i]$ as the feedback gain matrix, and q_k as the collective vector of noise-related terms $q_k = q^{1>}_k; : : : ; q^{n>}_k{}^>$ as,

$$q^i_k = {}_{k\ 1} \quad K_i \ H_i \ {}^>_k + {}^i \ H_i \ {}_k{}^> + {}^i H_i \ H_i{}^> {}_{k\ 1} ; \tag{6}$$

$$q_k = 1_N \ {}_{k\ 1} \quad KD_H(1_N \ {}_{k\ 1}) \quad K\overline{D}_{H\,k} \quad K\overline{D}_{H\,k}; \tag{7}$$

with 1_N as the vector of 1's of size N and $\overline{D}_H = diag[H_i{}^>]$. Following Kalman theory, for bounded steady-state estimation error, $(W \ A; D_H)$ needs to be observable, charac-terizing the distributed observability condition for network of estimators/observers [25]. Using structured system the-ory, this condition can be investigated via graph theoretic no-tions. In this direction, the associated network to $W \ A$ is a Kronecker-product network, whose observability condi-tion relies on the structure of both G and G_N. Given the social network G, the conditions on the sensor network G_N to satisfy distributed observability follows the recent results on composite-network theory and network observability dis-cussed in [24], which is summarized in the following lemma.

Lemma 2 [24] Given $(A; H)$-observability via Lemma 1, minimal sufficient condition for $(W A; D_H)$-observability is that matrix W be irreducible, i.e., the network G_N be strongly-connected (SC).

For an observable pair $(W A; D_H)$, the feedback gain matrix K can be designed to stabilize the error dynamics (5). Mathematically, for $\bar{A} = W A - K D_H (W A)$, we need to design K such that $(\bar{A}) < 1$ (Schur stability of error dynam-ics (5)) for general social systems with $(A) > 1$ with $()$ as the spectral radius. As mentioned before, for distributed case, K needs to be further block-diagonal such that each sensor only uses local information in its own neighborhood. The iterative LMI-based algorithm to design such block-diagonal gain K is given in [26]. In attack-free scenario, the distributed estimator/observer (3)-(4) with proper gain K ensures track-ing the global social state with bounded steady-state error as discussed in [6, 7]. Next, in this section, we further study the performance of the proposed protocol in the presence of non-zero random attack signals. Define $y^i_k = H_i x^i_k + b^i_k$ as the estimated output at sensor i at time k. To detect possible at-tacks, each sensor calculates its residual as the difference of its original output and the estimated one,

$$r^i_k = y^i_k - \hat{y}^i_k = y^i_k - H_i \hat{x}^i_{k|k} = H_i e^i_k + \nu^i_k - H_i \hat{b}^i_{k|k}. \quad (8)$$

Having $(\bar{A}) < 1$, the steady-state error in (5) only relies on the term q^i_k defined in (6) as,

$$H_i q^i_k = H_i \bar{A} q^i_{k-1} + H_i K_i H_i \nu^i_k - H_i K_i H_i \nu^i_{k-1}. \quad (9)$$

From (8) and (9), it is clear that for $\nu^i_k = 0$, only the residual r^i_k at sensor i is biased with no effect on the residual of other sensors $j \neq i$. This allows to isolate the attacked sensor as r^i_k only depends on ν^i_k and not on ν^j_k's. To detect a possible attack at agent i via residual r^i_k, the non-zero term $\nu^i_k - H_i K_i H_i \nu^i_k$ needs to be sufficiently larger than other noise terms. This ensures that the residual in attacked case is large enough to be distinguished from the noise terms in attack-free case. Clearly, the detecting probability of an at-tack depends on the magnitude of ν^i_k which justifies the probabilistic threshold design. In this direction, we consider a distributed probability-based χ^2-test which outperforms the deterministic fault/attack detection methods as it considers noise of unbounded support. In this case, instead of a deterministic threshold with 0 (no attack) or 1 (attack detected) outcome, different probabilistic thresholds (with different sensitivities) are defined each assigned with an FAR. In fact, higher residual-to-noise ratio (RNR) stimulates the threshold with lower FAR. In this direction, first the covariance of error e_k and (attack-free) residuals need to be calculated, which are tied with the noise covariance Q and R. Let $_k = E(e_k e_k^\top)$ and $= E(q_k q_k^\top)$. Then, from (5),

$$_k = \bar{A}^k \, _0 (\bar{A}^k)^\top + \sum_{j=1}^{k} \bar{A}^{j-1} (\bar{A}^{j-1})^\top + \cdots \quad (10)$$

Knowing that $(\bar{A}) < 1$, the first term in (10) goes to zero. Therefore, it can be proved from [4] that for $_1 = \lim_{k \to \infty} _k$,

$$\|_1\|_2 = \| \sum_{j=1}^{\infty} \bar{A}^{j-1} (\bar{A}^{j-1})^\top \|_2 + \|_2 \, \|\bar{K}\|_2^2 \, \|\bar{R}\|_2 \, / \, (1 - b^2) \quad (11)$$

with $b = \|\bar{A}\|_2 < 1$. For attack-free case ($_k = 0_N$ in (6)),

$$q_k q_k^\top = (I_{Nn} - K D_H)(1_{NN} \otimes _{k-1}) (I_{Nn} - K D_H)^\top + (K D_C)_k (K D_H)^\top; \quad (12)$$

where 1_{NN} is the 1's matrix of size N. Applying the $E()$ and 2-norm operators,

$$\|_k\|_2 = \| (I_{Nn} - K D_H)(1_{NN} \otimes Q) (I_{Nn} - K D_H)^\top \|_2 + \| (K \bar{D}_H) R (K \bar{D}_H)^\top \|_2. \quad (13)$$

Then, the upper-bound on $\|_k\|_2$ is,

$$\|_k\|_2 \leq \|I_{Nn} - K D_H\|_2^2 N \|Q\|_2 + \|K\|_2^2 \|\bar{R}\|_2,$$

with $\bar{R} = \mathrm{diag}[H_i^\top R_i H_i]$. Then, using (11),

$$\frac{\|_1\|_2}{N} \leq \frac{a_1 N \|Q\|_2 + a_2 a_3 \|R\|_2}{N(1 - b^2)} = ; \quad (14)$$

where $\|I_{Nn} - K D_H\|_2^2 = a_1$, $\|K\|_2^2 = a_2$, and $\|\bar{R}\|_2 = a_3 \|R\|_2$. Note that in (14) the error covariance is scaled by the number of sensors N. From (14), assuming no attack is present ($\nu^i_k = 0$), a conservative approximation for er-ror variance at sensor i is $E(e^i_k e^{i\top}_k) = _k = $. Then, follow-ing the discussion in [19], the residual r^i_k in (8) can be as-sumed as a zero-mean Gaussian variable with maximum vari-ance $_i = E(r^i_k r^{i\top}_k) = H_k^\top _k H_i + R_i$, i.e., $r^i_k \sim N(0; _i)$. Define,

$$z^i_k = \frac{(r^i_k)^2}{_i}; \quad v^i_k = \sum_{t=k-T+1}^{k} z^i_t; \quad (15)$$

with T as the length of the sliding window[1]. It is known that, for a Gaussian variable r^i_k, scalars z^i_k and v^i_k follow χ^2_1-distribution with degree 1 and T respectively ($E[z^i_k] = 1$ and $E[v^i_k] = T$) [27]. In fact, these so-called distance measures z^i_k and v^i_k give an estimate of variance of r^i_k relative to the attack-free variance $_i$ [19], and are known to outperform simple detectors comparing absolute residual to a threshold as in [21, 22]. Next, we determine the decision threshold on v^i_k based on a pre-specified FAR p. It can be shown that

[1] In general, each agent can consider a different length for the horizon T.

$p = 1 \quad F(\,)$ where $F(\,)$ is the cumulative distribution function (CDF) of $_1^2$-distribution. Then,

$$= 2 \quad {}^{1}(1 \quad p; \frac{T}{2}); \tag{16}$$

with $\quad {}^{1}(;)$ as the inverse regularized lower incomplete gamma function [27]. Using (16), our attack detection logic at each sensor i is as follows,

$$\text{If} \quad v_k^i \quad \text{Then} \quad \begin{matrix} H_1^i : \text{Attack Detected} \\ H_0^i : \text{No Attack} \end{matrix} \tag{17}$$

It should be noted that the existing ^{2}-based attack detection scenarios in literature are all centralized [15, 19, 20] and in this work, using distributed estimation, we enable detection of attacks locally at every sensor with no need of a central unit. We summarize our proposed simultaneous distributed estimation and attack detection technique in Algorithm 1.

Algorithm 1: Proposed iterative methodology.

Given: System matrix A, Network G_N, Fusion matrix W, Measurements y_k, Measurement matrix H, System/Measurement noise covariance Q/R, false-alarm probability (FAR) p, sliding window T
Choose block-diagonal gain K via LMI in [26];
Find $_{k\,jk}^{i}$ at every sensor i via (3)-(4);
Find $_i$ based on R, Q, and (14);
Find residuals r_k^i at every sensor i via (8);
Find z_k^i and v_k^i at every sensor i via (15) ;
Define threshold based on p and T via (16);
If v_k^i return H_1^i : Attack Detected with FAR p;
If $v_k^i \leqslant$ return H_0^i : No Attack;
Return: Hypothesis H_0^j or H_1^j for $i = f1; :::; Ng$.

Note that after detecting a malicious attack with low FAR, the strategy in [28] can be adopted to remove unreliable data and replace the compromised sensor with its observationally equivalent counterpart to regain distributed observability.

4. SIMULATION RESULTS

We evaluate our theoretical results on an example social network G of 10 state nodes with 4 sensor observations shown in Fig. 1. The network G_N of 4 sensors is considered as a cycle (satisfying Lemma 2). The fixed non-zero entries of A and W are chosen randomly in $(0; 1:1]$. Further, $(A) = 1:1$ imply-ing a potentially unstable system, $^i ; ^i \quad N_k(0; 0:06)$, and non-zero entries of H are set as 1. Using MATLAB CVX, the stabilizing block-diagonal gain K is designed via the iterative LMI in [26] subject to $j1 \quad H_i K_i H^{>} j > 0:2$, which results in $(A) = 0:97$, $b = 1:42$, $= 4:82$, and $_i = 4:88$. ^{i} In attack-free case, each sensor is able to track the global social state x_k over time via protocol (3)-(4). The time-evolution

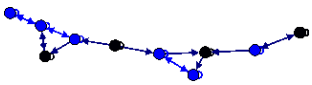

Fig. 1: The small social network G considered for simulation. The black state nodes are observed by the sensors (satisfying Lemma 1).

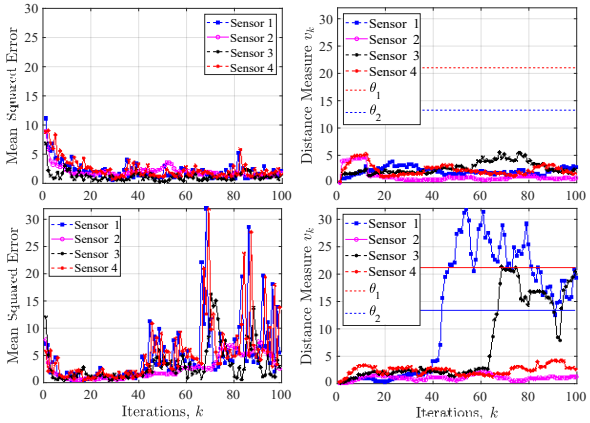

Fig. 2: (top) No attack: mean squared estimation error at all sensors are steady-state stable. (bottom) Attack at sensors 1 and 3: the non-zero attacks add bias to the estimation error at all sensors. Distance measures v_k^1 and v_k^3 exceeding $_2$ reveal possible attacks at sensors 1 and 3 with FAR $p_2 = 35\%$, while v_k exceeding $_1$ implies lower FAR $p_1 = 5\%$ for attack at sensor 1.

of mean squared errors $\frac{k e_k^i k^2}{n}$ and distance measures at all sensors are shown in Fig. 2(top). Next, considering two non-zero attack sequences as $_k^3 \quad N(0:2; 0:3)$ for $k \quad 60$ and $^1 N_k(0; 0:8)$ for $k \quad 40$, the distance measures v^i's over a sliding window of $T = 12$-step length are shown in Fig. 2(bottom). The figure clearly shows that the attacks af-fect the estimation error at all sensors. Setting two FARs $p_1 = 5\%$, $p_2 = 35\%$, the associated decision thresholds are $_1 = 21$, $_2 = 13:3$ via (16). From the figure, the less conser-vative threshold $_2$ reveals both attacks, while $_1$ only detects one and the other one remains stealthy most of the times.

5. CONCLUSION

We proposed an algorithm for simultaneous estimation of states and attack detection over a distributed sensor network. Using a windowed chi-square detector, every sensor is able to locally detect possible measurement anomalies causing the residuals to exceed an FAR-based threshold. As future research directions, the results in [5, 29] can be adopted to optimally locate the sensing nodes and design the network among the social sensors to reduce cost. Additionally, adopting the pruning strategies in [1, 2], one can change the social network structure and, in turn, tune its observability and information flow to improve estimation/detection properties.

6. REFERENCES

[1] M. Doostmohammadian, H. R. Rabiee, and U. A. Khan, "Centrality-based epidemic control in complex social networks," Social Network Analysis and Mining, vol. 10, pp. 1–11, 2020.

[2] P. Block, M. Hoffman, I. J. Raabe, J. B. Dowd, C. Rahal, R. Kashyap, and M. C. Mills, "Social network-based distancing strategies to flatten the COVID-19 curve in a post-lockdown world," Nature Human Behaviour, vol. 4, no. 6, pp. 588–596, 2020.

[3] H. Wai, A. Scaglione, and A. Leshem, "Active sensing of social networks," IEEE Transactions on Signal and Information Processing over Networks, vol. 2, no. 3, pp. 406–419, 2016.

[4] U. A. Khan and A. Jadbabaie, "Collaborative scalar-gain estimators for potentially unstable social dynamics with limited communication," Automatica, vol. 50, no. 7, pp. 1909–1914, 2014.

[5] S. Pequito, S. Kar, and A. P. Aguiar, "Minimum number of information gatherers to ensure full observability of a dynamic social network: A structural systems approach," in IEEE Global Conference on Signal and Information Processing. IEEE, 2014, pp. 750–753.

[6] M. Doostmohammadian, H. R. Rabiee, and U. A. Khan, "Cyber-social systems: modeling, inference, and optimal design," IEEE Systems Journal, vol. 14, no. 1, pp. 73–83, 2019.

[7] M. Doostmohammadian and U. Khan, "Graph-theoretic distributed inference in social networks," IEEE Journal of Selected Topics in Signal Processing, vol. 8, no. 4, pp. 613–623, Aug. 2014.

[8] S. Kar and J. M. F. Moura, "Consensus + innovations distributed inference over networks: cooperation and sensing in networked systems," IEEE Signal Processing Magazine, vol. 30, no. 3, pp. 99–109, 2013.

[9] A. Mitra and S. Sundaram, "Distributed observers for LTI systems," IEEE Transactions on Automatic Control, vol. 63, no. 11, pp. 3689–3704, 2018.

[10] P. Duan, Z. Duan, G. Chen, and L. Shi, "Distributed state estimation for uncertain linear systems: A regularized least-squares approach," Automatica, vol. 117, pp. 109007, 2020.

[11] X. He, X. Ren, H. Sandberg, and K. H. Johansson, "Secure distributed filtering for unstable dynamics under compromised observations," in IEEE 58th Conference on Decision and Control (CDC), 2019, pp. 5344–5349.

[12] M. Mansouri, M. N. Nounou, and H. N. Nounou, "Improved statistical fault detection technique and application to biological phenomena modeled by s-systems," IEEE Transactions on Nanobioscience, vol. 16, no. 6, pp. 504–512, 2017.

[13] H. Karimipour, A. Dehghantanha, R. M. Parizi, K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," IEEE Access, vol. 7, pp. 80778–80788, 2019.

[14] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H V. Poor, "Machine learning methods for attack detection in the smart grid," IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773–1786, 2015.

[15] B. Brumback and M. Srinath, "A chi-square test for fault-detection in Kalman filters," IEEE Transactions on Automatic Control, vol. 32, no. 6, pp. 552–554, 1987.

[16] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," IEEE Transactions on Automatic control, vol. 59, no. 6, pp. 1454–1467, 2014.

[17] J. Kim, C. Lee, H. Shim, Y. Eun, and J. H. Seo, "Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors," IEEE Transactions on Automatic Control, vol. 64, no. 3, pp. 1162–1169, 2018.

[18] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observabil-ity of linear systems under adversarial attacks," in American Control Conference (ACC). IEEE, 2015, pp. 2439–2444.

[19] R. Tunga, C. Murguia, and J. Ruths, "Tuning windowed chi-squared detectors for sensor attacks," in American Control Conference (ACC). IEEE, 2018, pp. 1752–1757.

[20] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," IEEE Transactions on Control of Network Systems, vol. 4, no. 1, pp. 4–13, 2017.

[21] M. Doostmohammadian and N. Meskin, "Sensor fault detection and isolation via networked estimation: Full-rank dynamical systems," IEEE Transactions on Control of Network Systems, 2020.

[22] M. Deghat, V. Ugrinovskii, I. Shames, and C. Langbort, "Detection and mitigation of biasing attacks on distributed estimation networks," Automatica, vol. 99, pp. 369–381, 2019.

[23] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber–physical systems," Proceedings of the IEEE, vol. 105, no. 2, pp. 219–240, 2016.

[24] M. Doostmohammadian and U. A. Khan, "Minimal sufficient conditions for structural observability/controllability of composite networks via kronecker product," IEEE Transactions on Signal and Information Processing over Networks, vol. 6, pp. 78–87, 2019.

[25] M. Doostmohammadian and U. A. Khan, "On the characterization of distributed observability from first principles," in 2nd IEEE Global Conference on Signal and Information Processing, 2014, pp. 914–917.

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

[27] P. E. Greenwood and M. S. Nikulin, A guide to chi-squared testing, John Wiley & Sons, 1996.

[28] M. Doostmohammadian, H. R. Rabiee, H. Zarrabi, and U. A. Khan, "Distributed estimation recovery under sensor failure," IEEE Signal Processing Letters, vol. 24, no. 10, pp. 1532–1536, 2017.

[29] M. Doostmohammadian, H. R. Rabiee, and U. A. Khan, "Structural cost-optimal design of sensor networks for distributed estimation," IEEE Signal Processing Letters, vol. 25, no. 6, pp. 793–797, 2018.