COMPENSATION OF ATTACKS ON CONSENSUS NETWORKS

Mohsen Zamani[†] *Alireza Khosravian*[⋆] *Brett Ninness*[†]

[†] School of Electrical Engineering and Computer Science, University of Newcastle, Callaghan, NSW 2308, Australia. mohsen.zamani@newcastle.edu.au, brett.ninness@newcastle.edu.au.

[⋆] School of Computer Science, University of Adelaide, Australia.

alireza.khosravianhemami@adelaide.edu.au.

ABSTRACT

In this paper, we propose a methodology for compensation of attacks on consensus networks. We assume that the network achieves its desired consensus value under a normal operational setting i.e. when the networked system is not under attack. We propose an adaptive based technique to ensure that the networked system maintains its desired behavior when the system inputs are under some *false-date injection* attacks. The proposed method adaptively estimates attack signals and compensates their effects. We demonstrate the good performance of our proposed compensation scheme through simulation studies that consider both constant and time-varying attack signals.

Index Terms— Cyber-physical attacks, consensus, networked systems.

1. INTRODUCTION

Advances in technology during the past decades have made it possible to realize cyberphysical systems in which distributed sensing, communication, and computation technologies are embedded into physical systems in the hope of making them more efficient and reliable. This leads to the creation of complex networked systems consisting of numerous local command units that communicate with each other and with the environment to effectively maintaian the performance of individual systems such that the whole network achieves a certain goal. Due to their distributed nature, networked systems are highly vulnerable to attacks that are aimed to destabilize the whole network or at least degrade its performance. Moreover, networked systems have been increasingly using open communication channels, such as wifi, intranet, or internet channels, in their routine measurments and operations making them also vulnerable to the attacks that are launched in the *cyber* domain, though target the *physical* process [1, 2, 3]. This gives raise to the problem of *cyberphysical security* which investigates methods to design cyberphysical systems such that they are both robust to disturbances and resilient to attacks [4, 5, 6, 7, 8].

Different attack scenarios are discussed in [5] where attack paradigms are categorized based on the required model knowledge, disruption resources and disclosure resources. Motivated by reports in [1], the authors of [6] study a class of attack strategies known as *replay* attacks in a noisy environment. In these attacks, an attacker injects harmful signals into systems while replaying previously recorded healthy measurements to the operator. So called *covert* attacks are studied in [8] and a feedback strategy is proposed that allows an attacker to take over the command of a system inside the network without being detected by the network supervisory unit. It is shown in [8] that covert attacks are impossible to be detected if attackers have the complete knowledge of the plant model. *False-data injection* attacks are explored in [7] where an attacker injects false signals into the measurements in order to affect the system states. The authors of [4, 9] discuss *zero-dynamics* attacks that are impossible to detect and also demonstrate that complete knowledge of the network model as well as the corresponding initial conditions are required for these types of attacks. These types of attacks are further investigated in [10].

Most of the tools for detecting, identifying, and compensating attacks only consider attacks into an individual system within a network (see e.g. [9], [11], [8], [12], [13]). In a situation where there are multiple systems networked together, one can employ the developed tools suited for attack compensation of individual systems if there exist a centralized processing unit that has access to inputs and outputs of the whole network (by modeling the whole network as a single system). However, many practical networked systems consist of subsystems that are operated trough a *local* command unit yielding a decentralize scheme [14, 15]. To the authors' best knowledge there exist a gap in the literature regarding analysis of attacks on distributed networks. As a very first attempt, in this paper we investigate attack compensation for consensus networks with constant (or practically slowly time-varying) attacks. We particularly consider the problem of compensating the input attacks on a group of networked agents connected together through the consensus law. The considered framework for modeling input attacks allows com-

pensation of both cyber attacks (caused by interfering with the signals that are communicated from the command units to the system inputs) or physical attacks (caused by interfering with the physical actuator inputs). Given a consensus networked with a fixed topology that reaches its desired value in a normal operational situation, we propose a general methodology to modify the original consensus law such that the modified networked maintains its desired behavior in presence of hidden attack signals. Although our proposed methodology relies on simplifying assumptions such as constant attack signals and consensus networks, it is the first contribution that considers attack compensation in *decentralized* scheme. This paper shows that even under the above simplifying assumptions, the decentralized approach causes theoretical complications that do not exist in typical centralized scenarios and are not easy to handle without employing rigorous tools from adaptive and nonlinear system theory. This contribution paves the way to tackle more complicated decentralized scenarios in future.

The structure of this paper is as follows. The problem is formulated and the proposed compensation scheme is presented in Section 2. Simulation studies in Section 3 demonstrate the performance of our proposed scheme and concluding remarks in Section 4 complete the paper.

2. PROBLEM FORMULATION AND MAIN RESULTS

Consider a network of N linear systems, which we refer to as *agents*. Each agent is assumed to have simple dynamics as

$$\dot{x}_i(t) = u_i(t) \in \mathbb{R},\ i = 1, 2 \ldots, N. \tag{1}$$

Assume that the agents are connected together through the following consensus law in nominal conditions when attack signals do not exist.

$$u_i(t) = \sum\nolimits_{j=1}^{N} a_{ij}(x_j(t) - x_i(t)), \tag{2}$$

where (a_{ij}) represents an entry of the adjacency matrix of the network [16].

Now, suppose that the consensus network is under additive input attacks by some signals $u_i^a(t), i = 1, \ldots, N$, which cannot be detected by an anomaly detector operating on the network [17]. Suppose that

$$u_i(t) = u_i^c(t) + u_i^a(t), \tag{3}$$

where $u_i^c(t) \in \mathbb{R}^{m_i}$ is the output of our proposed compensator that is to be designed later and $u_i^a(t)$ is the attack signal. In this paper, we analyze attack signals that are constant or slowly time-varying, i.e. their variation with time is slower than the response time of the closed loop system[1]. Assume

$$\dot{u}_i^a(t) = 0. \tag{4}$$

[1]This is an standard simplifying assumption commonly imposed in adaptive systems design [18, 19].

Note that $u_i^a(t)$ can model both cyber attacks caused by interfering the signals that are communicated from the some command units to the system inputs, or physical attacks caused by interfering the physical actuator inputs. For instance, in a robotic application, $u_i^a(t)$ might represent an interference in the command signals sent through some open channels to the robot's motors (cyber attack) or a physical force that is applied to the robot through some means of direct manipulation (physical attack). The attack signals aim to destruct the consensus of the network. Our main objective in this paper is to modify the nominal law (2) by adding a compensator to mitigate the effect of the attack signals. We propose the following compensator

$$u_i^c(t) = \sum\nolimits_{j=1}^{N} a_{ij}(x_j(t) - x_i(t)) - \hat{u}_i^a(t), \tag{5}$$

$$\dot{\hat{u}}_i^a(t) = -\gamma_i \sum\nolimits_{j=1}^{N} a_{ij}(x_j(t) - x_i(t)), \tag{6}$$

where γ_i are positive scalars. The following theorem summarizes the properties of the above attack compensation scheme.

Theorem 1 *Consider a network of agents with dynamics (1). Suppose that attack signals exist according to (3) and (4). Define $\tilde{u}_i^a(0) := \hat{u}_i^a(0) - u_i^a(0)$. Given the compensator (5)-(6) and assuming that the the topology of the network is connected and undirected, we have*

(a) $x_i(t) \to x_j(t)$ for all $i = 1, \ldots, N$ and $\dot{x}_i(t) \to \mathring{x}^* := -\frac{\sum_{i=1}^{N} \gamma_i^{-1} \tilde{u}_i^a(0)}{\sum_{i=1}^{N} \gamma_i^{-1}}$ for all $i = 1, \ldots, N$, i.e. velocities of agents reach the consensus value of $\mathring{x}^*$. In addition, the estimates $\hat{u}_i^a(t)$ are all bounded for all $t \geq 0$ and converge to the limit $\hat{u}_i^a(\infty) = u_i^a - \mathring{x}^*$ for all $i = 1, \ldots, N$.

(b) If $\gamma_i = \gamma > 0$ for all $i = 1, \ldots, N$ and $\sum_{i=1}^{N} \tilde{u}_i^a(0) = 0$, then all estimate $\hat{u}_i^a(t),\ i = 1, \ldots, N$ converges exponentially to u_i^a and all of the agents $x_i(t),\ i = 1, \ldots, N$ exponentially converge to the average consensus $x^* = \frac{1}{N} \sum_{i=1}^{N} x_i(0)$.

Proof: Using (1), (3), and (5), we have $\dot{x}_i(t) = \sum_{j=1}^{N} a_{ij}$ $(x_j(t) - x_i(t)) - \tilde{u}_i^a(t)$. We define the augmented vectors $x(t) := [x_1(t)\ x_2(t)\ \ldots\ x_N(t)]^\top$, $u^c(t) := [u_1^c(t)\ u_2^c(t)\ \ldots$ $u_N^c(t)]^\top$, $\hat{u}^a(t) := [\hat{u}_1^a(t)\ \hat{u}_2^a(t)\ \ldots\ \hat{u}_N^a(t)]^\top$, $u^a := [u_1^a\ u_2^a$ $\ldots\ u_N^a]^\top$ (noting that $u_i^a,\ i = 1, \ldots, N$ are constant), and $\tilde{u}^a(t) := \hat{u}^a(t) - u^a$. One can rewrite the resulting closed loop dynamics of the agent and proposed compensator as

$$\dot{x}(t) = -Lx(t) - \tilde{u}^a(t), \tag{7}$$

$$\dot{\hat{u}}^a(t) = \Gamma L x(t). \tag{8}$$

where $\Gamma = \text{diag}(\gamma_1, \ldots, \gamma_N)$ and L is Laplacian matrix of the network whose elements are given by [16]

$$L_{ij} = \begin{cases} \sum_{k=1, k\neq i}^{N} a_{ik}, & i = j \\ -a_{ij}, & i \neq j \end{cases} \tag{9}$$

Proof of part (a): Since the graph is connected and undirected, the Laplacian matrix L is symmetric positive semi-definite with only one zero eigenvalue [20, 14]. We introduce the following Lyapunov function

$$\mathcal{L}(t) = \frac{1}{2}x(t)^\top Lx(t) + \frac{1}{2}\tilde{u}^a(t)^\top \Gamma^{-1}\tilde{u}^a(t) \qquad (10)$$

Employing (7)-(8) and (10), one can obtain

$$\dot{\mathcal{L}}(t) = -x(t)^\top L^\top Lx(t) = -|Lx(t)|^2 \leq 0 \qquad (11)$$

Since $\mathcal{L}(t)$ is lower bounded (i.e. $\mathcal{L}(t) \geq 0$) and non-increasing (i.e. $\dot{\mathcal{L}}(t) \leq 0$), $\mathcal{L}(t)$ converges to a limit. One can also verify that $\ddot{\mathcal{L}}(t)$ is bounded implying that $\dot{\mathcal{L}}(t)$ is uniformly continuous. Hence, using Barbalat's lemma [21], we conclude that $\dot{\mathcal{L}} = Lx(t) \to 0$. Since the graph is connected, L has only a single zero eigenvalue whose associated right eigenvector is given by $\alpha\mathbf{1}$ for some α [20, 14]. This implies that $x(t) \to \alpha\mathbf{1}$ which means that all of the agents reach the consensus value α (but this does not necessarily imply that α is constant).

Since $\mathcal{L}(t)$ is non-increasing, we have $\mathcal{L}(t) \leq \mathcal{L}(0)$. Let us employ the Cholesky decomposition $L = M^\top M$ for some $M \in \mathbb{R}^{n\times n}$ with the same rank as L [22]. Using (10) and noting that the minimum singular value of $\Gamma^{-1} = \text{diag}(\gamma_1, \ldots, \gamma_N)^{-1}$ is $\max_i(\gamma_i)^{-1}$, we have $\frac{1}{2}|Mx(t)|^2 + \frac{1}{2}(\max_i(\gamma_i))^{-1}|\tilde{u}^a(t)|^2 \leq \mathcal{L}(t) \leq \mathcal{L}(0)$. This implies that $Mx(t)$ (and consequently $Lx(t)$) and $\tilde{u}^a(t)$ are bounded for all $t \geq 0$. Using (7)-(8), one can verify that

$$L\dot{x}(t) = -LLx(t) - L\tilde{u}^a(t), \qquad (12)$$

$$L\ddot{x}(t) = (L^2 - L\Gamma)Lx(t) + L^2u^a(t). \qquad (13)$$

Since $Lx(t)$ and $\tilde{u}^a(t)$ are bounded, (13) implies that $L\ddot{x}(t)$ is bounded for all $t \geq 0$. This yields that $L\dot{x}(t)$ is uniformly continuous. Moreover, we showed that $Lx(t) \to 0$. Hence, invoking Barbalat's lemma implies that $L\dot{x}(t) \to 0$. Using (12) yields that $L\tilde{u}^a(t) \to 0$ which means that $\tilde{u}^a(t) \to \beta\mathbf{1}$ for some $\beta \in \mathbb{R}$. Using (7) and noting $Lx(t) \to 0$, we also have $\dot{x}(t) \to -\beta\mathbf{1}$. It only remains to show that β is constant and to compute its value. Multiplying the sides of (8) by Γ^{-1} we have $\Gamma^{-1}\dot{\tilde{u}}^a(t) = Lx(t)$. Summing up the elements of the resulting vectors and denoting the elements of the Laplacian matrix by L_{ij} we have $\sum_{i=1}^N \gamma_i^{-1}\dot{\tilde{u}}_i^a(t) = \sum_{i=1}^N\sum_{j=1}^N L_{ij}x_j(t)$. We recall that $\sum_{i=1}^N\sum_{j=1}^N L_{ij}x_j(t) = \sum_{i=1}^N\sum_{j=1}^N a_{ij}(x_j(t) - x_i(t)) = 0$ since the graph is undirected [20, 14]. Hence we have $\sum_{i=1}^N \gamma_i^{-1}\dot{\tilde{u}}_i^a(t) = 0$ which means that the value of $\sum_{i=1}^N \gamma_i^{-1}\tilde{u}_i^a(t)$ is invariant implying that $\sum_{i=1}^N \gamma_i^{-1}\tilde{u}_i^a(t) = \sum_{i=1}^N \gamma_i^{-1}\tilde{u}_i^a(0)$ for all $t \geq 0$. Since $\tilde{u}_i^a(t) \to \beta$ we have $\sum_{i=1}^N \gamma_i^{-1}\beta = \beta\sum_{i=1}^N \gamma_i^{-1} = \sum_{i=1}^N \gamma_i^{-1}\tilde{u}_i^a(0)$ which implies that $\beta = \frac{\sum_{i=1}^N \gamma_i^{-1}\tilde{u}_i^a(0)}{\sum_{i=1}^N \gamma_i^{-1}}$. Defining $\mathring{x}^* = -\beta$ completes the proof of part (a).

Proof of part (b): summing up the elements of the sides of (7), setting $\gamma_i = \gamma$, and $\sum_{i=1}^N \tilde{u}_i^a(0) = 0$ and invoking part (a) we conclude that $\mathring{x}^* = 0$ and $\hat{u}_i^a(\infty) = u_i^a$. This proves the convergence of $\hat{u}_i^a(t)$ to u_i^a. We have $\sum_{i=1}^N \dot{x}_i(t) = -\sum_{i=1}^N L_{ij}x_j(t) - \sum_{i=1}^N \tilde{u}^a(t) = 0$ since $\sum_{i=1}^N L_{ij}x_j(t) = 0$ due to the undirected graph topology and $\sum_{i=1}^N \tilde{u}^a(t) = \sum_{i=1}^N \tilde{u}^a(0) = 0$ due to the assumption of Theorem. Hence we have $\sum_{i=1}^N \dot{x}_i(t) = 0$ or equivalently $\sum_{i=1}^N x_i(t) = \sum_{i=1}^N x_i(0)$ for all $t \geq 0$. Recalling $x_i(t) \to \alpha$ from the proof of part (a), we have $N\alpha = \sum_{i=1}^N x_i(0)$ and the consensus value α is computed as $\alpha = \frac{1}{N}\sum_{i=1}^N x_i(0)$. Since the closed loop system (7)-(8) is LTI, asymptotic convergence of $x_i(t)$ and $\hat{u}_i^a(t)$ is equivalent to the exponential convergence of those signals. This completes the proof. ■

According to the proof of Theorem 1, the value of $\sum_{i=1}^N \gamma_i^{-1}\hat{u}_i^a(t)$ is constant for all $t \geq 0$ (i.e. it is invariant). This property is similar to the invariance of the average value of the node states in the normal average consensus scheme when there is no input attack [14].

Part (a) of Theorem 1 ensures that, without any knowledge of the input attack, the network reaches a consensus, though this consensus is not necessarily the average consensus. According to part (b), if moreover the initial conditions of the attack estimates $\hat{u}_i^a$ are chosen such that $\sum_{i=1}^N \tilde{u}_i^a(0) = 0$, the trajectory of the estimated attack signal converges to the actual attack value and that implies that the agents reach the average consensus. A particular case where the condition $\sum_{i=1}^N \tilde{u}_i^a(0) = 0$ is satisfied is when attacks do not exist ($u_i^a(t) = 0,\ i = 1, \ldots, N$) and the initial estimates of attacks are also considered as zero ($\hat{u}_i^a(0) = 0,\ i = 1, \ldots, N$). This initialization of the compensator ensures that the network converges to the average consensus at least in nominal condition when there is no attack. This shows that the compensator (5)-(6) maintains the convergence properties of the original consensus law (2) in attack free condition. Another particular case is where the agents know the average value of the attack signals and they choose that average value as the initial condition $\hat{u}_i^a(0)$.

3. SIMULATIONS

In this section, we present numerical simulations to demonstrate performance of the proposed attack compensation scheme (5)-(6) versus the pure consensus law (2) (without attack compensation). In order to simplify presentation of the results, we consider the simple network demonstrated in Fig. 1. The initial condition of agent states are given as $x_1(0) = 1,\ x_2(0) = -0.75,\ x_3(0) = -0.25$ and we choose the gains as $\gamma_1 = \gamma_2 = \gamma_3 = 1$.

3.1. Constant attack signals

Assume that the input attacks of $u_1^a(t) = 0.5$, $u_2^a(t) = -2$, and $u_3^a(t) = 1.5$ are exerted to the system at time $t = 10$ (s) (the attack signals are zero for $t < 10$ (s)). The initial condition of the dynamics (6) is chosen as zero. This ensures

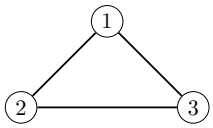

Fig. 1. The network topology.

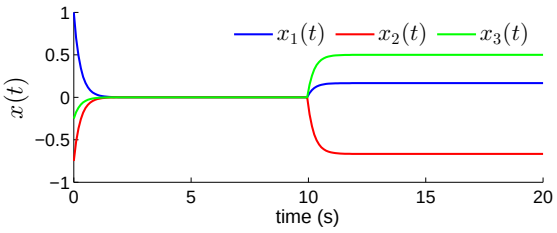

Fig. 2. Performance of the pure consensus law (2) in presence of a constant attack starting at $t = 10$ (s).

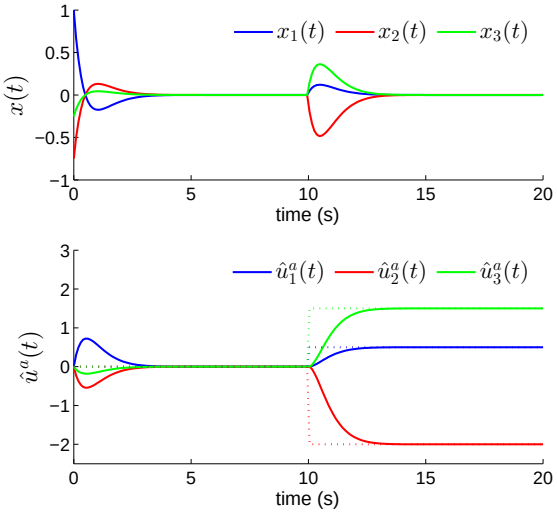

Fig. 3. Performance of the proposed compensator (5)-(6) in presence of a constant attack starting at $t = 10$ (s). Dashed lines in the bottom figure show the attack signals.

that the condition $\sum_{i=1}^{3} \tilde{u}_i^a(0) = 0$ holds. Fig. 2 and Fig. 3 illustrate the trajectories of agents when the pure consensus law (2) is used compared to when the proposed compensator (5)-(6) is employed. For $t < 10$ (s) where there is no input attack, both compensators perform such that the agent trajectories converges toward the average consensus value which is zero in this simulation. However, when attacks occur at time $t = 10$ (s), they completely destroy the consensus of the network with the pure consensus law (2) (Fig. 2), while the proposed compensator in this paper compensates for the attacks such that the whole networked system states converge back to the consensus value after a short transient time (Fig. 3). Trajectories of the estimates of attack signals have also been illustrated by Fig. 3 showing the convergence of those

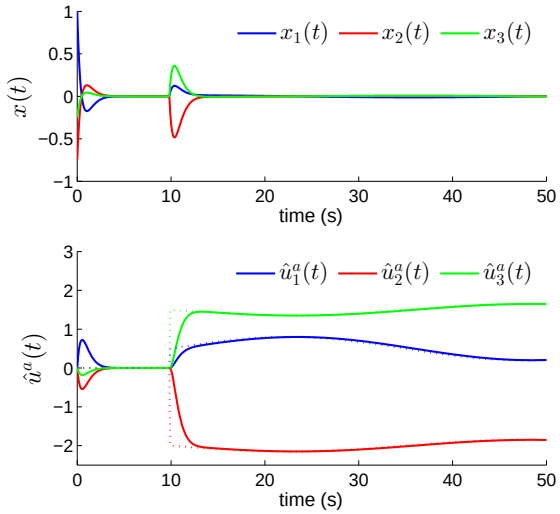

Fig. 4. Performance of the proposed compensator (5)-(6) in presence of time-varying attacks starting at $t = 10$ (s). Dashed lines in the bottom figure show the attack signals.

signals to the true values of the attack signals.

3.2. Time-varying attack signals

Although Theorem 1 is only valid when the attack signals are constant, here we demonstrate that the proposed adaptive compensator (5)-(6) performs well even if the attack signals slowly vary with time. We consider the time-varying attack signals $u_1^a(t) = 0.5 + 0.3\sin(\omega t)$, $u_2^a(t) = -2 - 0.15\sin(\omega t)$ $u_3^a(t) = 1.5 - 0.15\sin(\omega t)$ with $\omega = \frac{2\pi}{50}$ and we initiate the estimates $\hat{u}_i^a$, $i = 1, 2, 3$ to zero. Notice that we still have $\sum_{i=1}^{3} u_i^a(t) = 0$ for all $t \geq 0$. Fig. 4 demonstrates that the proposed attack compensator (5)-(6) yields the states trajectories to converge to a very close neighborhood of the average consensus value (after a short transient time) even in the presence of time-varying attacks. Fig. 4 also shows that the estimate of attack signals provided by (6) track the actual time-varying attack signals very well.

4. CONCLUSION

We present a novel attack compensation scheme for a network of systems connected through a distributed consensus law. We propose adaptive corrections such that the network maintains its desired convergence behavior in presence of attack signals. We present simulation studies demonstrating the performance of the proposed approach in presence of both constant and time-varying attacks. This paper shows that even for consensus networks under constant attacks, the decentralized approach naturally causes theoretical complications that are not easy to handle without employing rigorous tools from adaptive and nonlinear systems theory. This contribution provides strong mathematical basis and paves the way to tackle more complicated scenarios in future.

5. REFERENCES

[1] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, 2011.

[2] T. Rid, "Cyber war will not take place," *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5–32, 2012.

[3] S. Gorman, "Electricity grid in us penetrated by spies," *The Wall Street Journal*, vol. 8, 2009.

[4] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, Feb 2015.

[5] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[6] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014.

[7] Y. iu, 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, pp. 13, 2011.

[8] R. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 82–92, 2015.

[9] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *IEEE Annual Allerton Conf. Communication, Control, and Computing*, 2012, pp. 1806–1813.

[10] M. Zamani, U. Helmke, and B. D. O. Anderson, "Zeros of networked systems with time-invariant interconnections,," *Automatica*, pp. 97–105, 2015.

[11] 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, 2012.

[12] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc Annual Allerton Conference on Communication, Control, and Computing*, 2009, pp. 911–918.

[13] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Workshop on Secure Control Systems*, 2010, pp. 1–6.

[14] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1520–1533, 2004.

[15] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions Automatic Control*, vol. 48, no. 6, pp. 988–1001, 2003.

[16] C. D. Godsil and G. Royle, *Algebraic graph theory*, vol. 207, Springer, 2001.

[17] André Teixeira, Daniel Pérez, Henrik Sandberg, and Karl Henrik Johansson, "Attack models and scenarios for networked control systems," in *Proc of the 1st international conference on High Confidence Networked Systems*. ACM, 2012, pp. 55–64.

[18] S. Sastry and M. Bodson, *Adaptive control: stability, convergence and robustness*, Courier Corporation, 2011.

[19] P. A. Ioannou and J. Sun, *Robust adaptive control*, Courier Corporation, 2012.

[20] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative control of multi-agent systems: optimal and adaptive design approaches*, Springer, 2013.

[21] H. K. Khalil and J. W Grizzle, *Nonlinear systems*, vol. 3, Prentice hall New Jersey, 1996.

[22] A. R. Horn and C. R. Johnson, *Matrix analysis*, Cambridge university press, 2012.