Formatted: Font: (Default) Calibri, 10 pt

Formatted: Normal, Right, Tab stops: 8.25 cm, Centered + 16.51 cm, Right

A False Data Injection Detection Using Sensor Based Control Protocol in Different Cases of Cyber Physical System.

~~A.Joshua~~A. Joshua Issac[1], Dr. ~~S.Shanmuga~~Shanmugam Priya[2]

[1]*Research Scholar, Department of Computer Science & Engineering, SRM Institute of Science & Technology, ~~Tiruchirapalli~~Tiruchirappalli.*

[2]*Associate Professor, Department of Computer Science & Engineering, SRM Institute of Science & Technology, ~~Tiruchirapalli~~Tiruchirappalli.*

***Abstract*—Safeguarding cyber-physical systems (CPSs) from cyberattacks is becoming ever more essential. False data injection assaults, which alter sensor readings and control signals, are one of the many dangers that could seriously impair CPS operation. This research presents a strong security strategy based on the idea of energy conversion to counter measured bogus data injection attacks. After that, an energy controller is created to dynamically control system energy in reaction to unidentified threats. The controller keeps the system stable and its dynamic performance intact by varying damping injection. Furthermore, the design of control systems is made simpler by the use of a disturbance attenuation technique, which removes the requirement to create an attack observer. By avoiding intricate mathematical processes, the suggested approach is also useful. An industrial CPS that manages a permanent magnet synchronous motor is used to verify its efficacy.**

I INTRODUCTION

Cyber-physical systems (CPSs) have been the target of increasingly frequent cyberattacks in recent years. The emergence of nonlinear control techniques for secure control is prompted by the considerable nonlinear features that these attacks frequently inject into CPSs. Numerous nonlinear techniques, including adaptive control, sliding mode control, and model predictive control, have been researched by researchers. Every technique, nevertheless, has disadvantages. Especially when non-parametric uncertainties are present, adaptive control can be intricate and susceptible to modeling errors. Backstepping techniques can result in dimensional expansion, while sliding mode control has chattering issues and is constrained by system order. Although powerful, model predictive control is computationally intensive, making real-time implementation problematic.

Due to the unpredictable, dynamic, and complex nature of cyber-attacks, high-gain controllers often struggle to effectively manage such threats. While adaptive secure controllers can counter denial-of-service (DoS) attacks and disturbances, tuning adaptive parameters remains a challenge. Similarly, backstepping controllers are generally suited only for second-order systems, limiting their scalability. Observer-based methods designed to stabilize attacked systems add complexity and design overhead. Model predictive control methods, which rely on solving constrained optimization problems, further increase computational burdens.

Most scientists and engineers agree that changes in different physical variables in dynamic systems correspond to changes in energy (absorption, conversion, and consumption). For instance, a change in the energy of the magnetic field is reflected in the change in the current passing through an inductor. As a result, controlling the system's energy allows for control over its physical quantity. The system's energy change characteristic is its passivity. Because of its strong physical interpretation and global convergence properties, passivity-based control [14]– [16] is intrinsically nonlinear. This nonlinear control approach offers a physical explanation for control behavior through an understandable physical idea [17], [18]. It uses the damping injection approach to increase the system's dynamic performance in addition to ensuring stability [19]– [21]. The high-gain feedback control law does not need to be solved by the passive-based control approach in contrast to other

Formatted: Font: (Default) Times New Roman

Formatted: Normal, Tab stops: 9.21 cm, Centered + 16.51 cm, Right nonlinear control techniques based on signal processing. Therefore, it is easier to implement in engineering because it is computationally simpler.

Passivity-based control compromises the stability of a cyber-physical system (CPS) under attack conditions. Malicious modifications to sensor readings or control inputs, either by raising or decreasing them, can intentionally upset the system's energy balance, leading to instability, especially during bogus data injection attacks. Two primary strategies are typically used to strengthen system stability: (1) using observers to identify and mitigate the impact of attacks, and (2) using disturbance attenuation techniques to reduce the impact of attacks on the system. Traditional disturbance watchers, however, may become useless due to the unpredictability of such attacks, especially when confronted with new attackers [11], [15]. Furthermore, creating specialized attack observers raises the control system's complexity and expense. This research suggests a technique that combines disturbance attenuation control and Hamiltonian system theory in order to get beyond these restrictions. To improve the overall control performance, a robust controller is built using the port-controlled Hamiltonian with dissipation (PCHD) model by implementing the passivity-based interconnection and damping assignment framework.

Two primary advances to the protection of CPSs against fake data injection attacks are made by this study overall:

1) An energy conversion-based defense framework is suggested; 2) a robust controller based on passivity from the port-controlled Hamiltonian model is created to stabilize the attacked CPSs using the L2 gain disturbance attenuation technology.

The rest of this essay is structured as follows: We outline our energy conversion-based defense strategy in Section II. We then design a robust controller based on passivity in Section III. Experiments are presented in Section IV. Lastly, the paper is concluded in Section V.

Notations: R, R^n, and R^{m*n} denotes a real space, n-dimensional real space, and m×n real matrices, respectively. $\|.\|$denotes the 1-norm of a vector or matrix, l_m represents an m- order unit matrix. ~~diag~~dig(x_1, ~~……~~, x_m) shows a diagonal matrix. The transpose of a vector or matrix A denotes A^T.

II FRAMEWORK FOR DEFENSE USING ENERGY CONVERSION

This section outlines a defense framework from an energy conversion standpoint. System transformation is the foundation of the framework.

A. Conversion of System Models for Energy Control

$$\begin{cases} \dot{x} = f(x) = g(x)u \\ \quad y = h(x) \end{cases}$$

Where $x \in R^n$, $u \in R^n$, and $y \in R^n$ are representing a system state vector, control input vector, sensor output vector, $f(x) \in R^n$ and $h(x) \in R^n$ are function vectors, and $g(x) \in R^{n\times n}$ denotes a function matrix.

The majority of current research uses a defense architecture based on system (1) and approaches secure control from the standpoint of signal processing. This essay, however, develops a defense architecture from an energy conversion standpoint. System (1) is converted into the following port-controlled Hamiltonian with passivity (PCHD) form for energy control:

$$\begin{cases} \dot{x} = [J(x) - R(x)]\dfrac{\partial H(x)}{\partial x} g(x)u + \Delta e \\ \qquad y = g^T(x)\dfrac{\partial H(x)}{\partial x} \end{cases}$$

Here H(x): $R^n \to R_+$ is the Hamiltonian function of the system. Symmetric positive semidefinite dissipative matrix $R(x)=R^T(x) \geq 0$ reflects the damping characteristics of the system. Anti-symmetric structure matrix $J(x) = -J^T(x)$ reflects the interconnection structure inside the system.$\Delta e \in R^n$ is the conversion error.

B. The Attacks' Description

Denial-of-service attacks, replay attacks, bogus data injection attacks, zero-dynamic assaults, and covert attacks are examples of common attacks. False data injection attacks are easy to execute and have the ability to randomly wipe out a system. As a result, a large body of literature examining security control concerns under fake data injection attacks exists, as in The literature's models of fake data injection attacks are typically complex due to the fact that intelligent attackers typically work alongside system models. In order for the attackers to gain the system model, they must use system identification techniques [40]–[42]. This procedure is extremely intricate, which restricts

Formatted: Font: (Default) Calibri, 10 pt

Formatted: Normal, Right, Tab stops: 8.25 cm, Centered + 16.51 cm, Right

Formatted: Font: (Default) Times New Roman

Formatted: Normal, Tab stops: 9.21 cm, Centered + 16.51 cm, Right

how these attack models can be used. however, how clever the attack models are, the malicious alteration of control orders and/or sensor outputs reflects their final impact on the system.

As a result, the use of these intricate false data injection attack models is not covered in this article. It discovers a novel method for fake data injection attacks that credits the malicious increase or reduction in control instructions and/or sensor outputs for the attack's systemic effects. For enhancing or reducing control commands and/or sensor outputs, this novel method of exploiting is straightforward to create and execute. In the end, it may intentionally undermine the system. The following are the exploit strategies displayed:

$$\begin{cases} a_u = \Lambda_a \sigma u \\ a_y = \Lambda_y \varphi y \end{cases}$$

Here the attack injection vector to actuators denotes$a_u \in R^n$, $\Lambda_a \in R^{n\times n} = \mathrm{diag}\{\varsigma_1, \dots \dots, \varsigma_n\}$ is a diagonal matrix, and σ is a constant. $\varsigma_i$denotes a random variable and the value shows 0 or 1. If ς_i=1, then the ith actuator is attacked, or it will 0 means no attack in ith actuator. An attacker can choose any actuator to target in this manner. and the attack also $a_y \in R^n$ injection vector to sensors, $\Lambda_y \in R^{n\times n}$=diag{$K_1$….,$K_n$} is a diagonal matrix, and constant is a φ. random variable K_i with a value either of 1 or 0. If, Ki=1 then the ith sensor is attacked, or else no attack to the ith sensor. This way gives an attacker the freedom to select any sensor to target.

Assumption 2: Real-time access to system (2) control commands and sensor outputs is possible to an attacker.

III DESIGN OF PASSIVITY-BASED ROBUST CONTROLLER

A passivity-based robust controller offers a promising solution by leveraging the physical principle of energy dissipation to ensure system stability and resilience. Particularly in cyber-physical systems (CPSs) like the control of Interior Permanent Magnet Synchronous Motors (IPMSMs), passivity-based control methods provide a structured and physically meaningful way to resist both dynamic uncertainties and cyber-attacks. Passivity-based control (PBC) involves designing controllers that shape the energy function of the system and inject damping, ensuring that the closed-loop system remains passive and hence, stable.

A passivity-based robust controller consists of the following components:

1. Energy Shaping: Modifies the system's energy function (Hamiltonian) to achieve desired equilibrium.
2. Damping Injection: Adds virtual dissipation to enhance convergence and robustness.
3. Feedback Interconnection: Ensures that controller and system are both passive, guaranteeing stability via passivity theorem.
4. Robustness Design: The controller is designed to tolerate:Parametric uncertainties,Disturbances (e.g., load changes, torque ripple), Cyber-attacks like false data injection (FDI) or replay attacks

~~4.~~

1. Modeling the System

Start with the nonlinear dynamic model of the IPMSM in d-q coordinates:

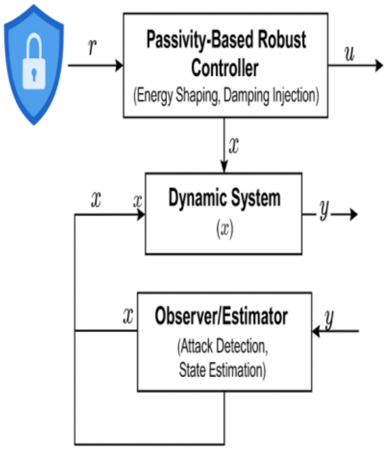
r
Passivity-Based Robust Controller
(Energy Shaping, Damping Injection)
u
x
x
x
Dynamic System
(x)
y
x
Observer/Estimator
(Attack Detection, State Estimation)
y

Diagram:1 for Passivity- based robust controller

$v_d = Ri_d + \frac{d\psi_d}{dt} + -\omega\psi_q$

$v_q = Ri_q + \frac{d\psi_q}{dt} + -\omega\psi_d$

$Te = \frac{3}{2} p(\psi d^i q - \psi q^i d)$

$J\frac{d\omega}{dt} = T_e - T_L - B_\omega$

Where:

Formatted: Font: (Default) Calibri, 10 pt

Formatted: Normal, Right, Tab stops: 8.25 cm, Centered + 16.51 cm, Right

Formatted: No bullets or numbering

Formatted: Left

Formatted: Font: (Default) Times New Roman

Formatted: Normal, Tab stops: 9.21 cm, Centered + 16.51 cm, Right

v_d, v_q denotes the voltages of the controller i_d, i_q denotes the currents of it, ψ_d, ψ_q denotes flux linkages and rotor speed assign a ω respectively. T_e and T_L shows electromagnetic torque, load torque respectively

2. Define Storage Function (Energy Function)

The total energy in the system is:

$H(x)=\frac{1}{2} L_d {i^2}_d + \frac{1}{2} L_q {i^2}_q + \frac{1}{2} J\omega 2$

This serves as the Lyapunov candidate for stability analysis.

3. Design Control Law

Construct control inputs v_d, v_q such that the energy derivative $\dot{H}(x)$ is negative semi-definite:

$\dot{H}(x)=-R{i^2}_d - R{i^2}_q - B\omega^2 +$ External Inputs

To ensure robustness and passivity, introduce damping injection terms and compensate for disturbances via feedback linearization or sliding mode terms.

Example robust control law:

$v_d = Ri_d - \omega L_q i_q + {u^*}_d$, $v_q = Ri_q - \omega L_d i_d + {u^*}_q$,

Where ${u^*}_d$, ${u^*}_q$ is designed to:

To track current references and reject disturbances also Maintain passivity

4. Add Cyber Attack Detection and Rejection

Introduce an observer or estimator for current and position, such as an Extended State Observer (ESO) or Kalman Filter, which:

- Compares actual vs. estimated states
- Flags anomalies (e.g., in FDIA)
- Switches to fallback control mode or adjusts feedback gain

Advantages of Passivity-Based Robust Control

- Guaranteed Stability under modeling errors
- Energy-Aware Design aligns with physical system properties
- Modular and Scalable for multi-agent CPS
- Resilience to Cyber Attacks through passive redundancy and energy monitoring

Challenges and Research Directions

- Designing PBC under real-time computation limits
- Extending to distributed systems with communication delays
- Integrating AI-based intrusion detection with passivity theory
- Hardware-in-the-loop (HIL) validation for critical applications (e.g., EVs, drones)

Table: Ten Cases of Attacks on Control Input (aui) and Sensor Output (ayi)

Case	Attack Type	Affected Channel	Description	Possible Impact
1	Constant Bias Injection	a_{u1}	Injects a fixed offset to control input in loop 1	Causes steady-state error or speed/torque shift
2	Random Noise Injection	a_y^2	Adds Gaussian noise to sensor output in loop 2	Degrades observer performance; false alarms
3	Replay Attack	a_{y1}	Reuses past valid output data in loop 1	Hides real-time system behavior from controller
4	Signal Scaling Attack	a_{u2}	Multiplies control input by a gain factor in loop 2	Over- or under-actuation, leading to instability
5	Delay Injection	a_{y1}	Introduces time delay in sensor signal	Destabilizes fast-response systems

Formatted: Font: (Default) Calibri, 10 pt

Formatted: Normal, Right, Tab stops: 8.25 cm, Centered + 16.51 cm, Right

Formatted: Left

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

Formatted: Indent: Left: 0 cm

Formatted Table

Formatted: Font: (Default) Times New Roman

Formatted: Normal, Tab stops: 9.21 cm, Centered + 16.51 cm, Right

6	Zero-Dynamics Attack	a_{u1}, au_2	Exploits internal model zeros to silently manipulate inputs	Produces output deviations without triggering alarms
7	Denial-of-Service (DoS)	a_y^2	Blocks transmission of sensor signals intermittently	Controller operates on outdated or missing information
8	False Data Injection (FDI)	a_{u2}	Alters control commands to deviate system behavior	Drifts system states to unsafe or inefficient regions
9	Saturation Spoofing	a_{u1}, ay_1	Forces values to actuator/sensor limits	Creates controller errors or protection shutdowns
10	Coordinated Multi-Channel Attack	au1, ay2a_{u1}, a_{y2}au1, ay2	Simultaneously corrupts control and output channels	Bypasses redundancy and observer detection mechanisms

REFERENCE:

[1] H. Gao et al., "Security Control of Cyber-Physical Systems with Applications to IPMSM Drives," IEEE Transactions on Industrial Informatics, 2021.

[2] Y. Mo, T. H.-J. Kim, et al., "Cyber-hysical Security of a Smart Grid Infrastructure," Proc. IEEE, 2012.

[3] R. Teixeira et al., "Secure Control systems: A Quantitative Risk Management Approach," Springer, 2015.

[4] S. Zuo et al., "Robust Observer-Based Control of IPMSM Under Cyber Attack," IEEE Access, 2023.

[5] O. Puñal et al., "Machine Learning–Based Jamming Detection for IEEE 802.11: Design and Experimental Evaluation", in Proc. 14th IEEE WoWMoM, Jun 2014.

[6] "Mitigation of jamming attacks in wireless networks", IEEE Conf. Pub. (2024).

[7] A. Benslimane et al., "Analysis of Jamming Effects on IEEE 802.11 Wireless Networks", in IEEE ICC 2011.

[8] G. Puleo et al., "Performance of IEEE 802.11 under Jamming", Mobile Networks and Applications, 2013.

[9] E. Garcia-Villegas et al., "A Novel Cheater and Jammer Detection Scheme for IEEE 802.11-based WLANs", Computer Networks, 2015.

[10] R. Ortega, A. van der Schaft, I. Mareels, B. Maschke "Energy Shaping Revisited: A Unified Approach for the Control of Mechanical Systems" (IEEE Transactions on Automatic Control)

[11] B. Cui, Z. Han, J. Li, and J. Mu, "Research on pmsm speed control system based on improved reaching law," in Proc. 3rd Int. Conf. Circuits, System and Simulation, 2019

[12] A. Levant, "Sliding order and sliding accuracy in sliding mode control," Int. Journal of Control, vol.58, no.6

[13] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," IEEE Trans. Cybernetics, vol.48, no.12

[14] A. Rosich, H. Voos, Y. Li, and M. Darouach, "A model predictive approach for cyber-attack detection and mitigation in control systems," in Proc. 52nd IEEE Conf. Decision and Control, Dec. 2013, pp. 6621–6626.

[15] T.-Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber-hysical systems: A self-generated approach," Automatica, vol.120, no.1, pp.109–117, 2020.

[16] A. Barboni, H. Rezaee, F. Boem, and T. Parisini, "Detection of covert cyber-attacks in interconnected systems: A distributed model-

Formatted: Font: (Default) Calibri, 10 pt

Formatted: Normal, Right, Tab stops: 8.25 cm, Centered + 16.51 cm, Right

Formatted: Centered

Formatted: Indent: Left: 0 cm

Formatted: Font color: Auto

Formatted: Font: (Default) Times New Roman

Formatted: Normal, Tab stops: 9.21 cm, Centered + 16.51 cm, Right

based approach," IEEE Trans. Automatic Control, vol.65, no. 9, pp. 3728~~–3741~~–3741, May 2020

[17] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," IEEE Trans. Automatic ~~Control,vol.~~Control, vol.63, no.6, pp. 1648–1663, Jun.2018.

[18] E. Kim, "A fuzzy disturbance observer and its application to control," IEEE Trans. Fuzzy Systems, vol.10, no.1, pp.77–84, Mar. 2002.

[19] A. Macchelli and C. Melchiorri, "Control by interconnection and energy shaping of the timoshenko beam," Mathematical and Computer Modelling of Dynamical Systems, vol.10, pp.231–251, Sep. 2004.

[20] Z. Pang, R. Yang, G. Liu, and J. Zhang, "Design and detection of false data injection attacks against output tracking control systems," in Proc. 36th Chinese Control Conf., 2017, pp. 7996–8001.

[21] T. Sun, J. Wang, and X. Chen, "Maximum torque per ampere (mtpa) control for interior permanent magnet synchronous machine drives based on virtual signal injection," IEEE Trans. Power Electronics, vol.30, no.9, pp.5036–5045, 2015.

[22] S. Potluri, C. Diedrich, and G. K. R. Sangala, "Identifying false data injection attacks in industrial control systems using artificial neural networks," in Proc. 22nd IEEE Int. Conf. Emerging Technologies and Factory Automation, 2017, pp. 1–8.

[23] G. Espinosa-Prez, H. Siguerdidjane, and A. Dria-Cerezo, "On the passivity-based power control of a doubly-fed induction machine," Int. Journal of Electrical Power & Energy Systems, vol.45, no.1, pp.303–312, Feb. 2013

[24] M. Khanchoul, M. Hilairet, and D. Normand-Cyrot, "A passivity-based controller under low sampling for speed control of pmsm," Control Engineering Practice, vol.26, no.9, pp.20–27, 2014.

[25] J. Hu, J. Wang, and Q. Tang, "A new cuk converter with high stepdown ratio and its control," Applied Mechanics and Materials, vol.571–572, no.12, pp.1053–1058, Jun. 2014.

Formatted: Font: (Default) Calibri, 10 pt

Formatted: Normal, Right, Tab stops: 8.25 cm, Centered + 16.51 cm, Right

Formatted: Font color: Auto

Formatted: Font color: Auto

Formatted: Font color: Auto

Formatted: Font: (Default) Times New Roman

Formatted: Normal, Tab stops: 9.21 cm, Centered + 16.51 cm, Right