NIU Journal of Health Sciences Copyright©2026
Nexus International University ISSN: 3007-1xxx; 12(1) 69-75

Development of a Secure Networked Control Algorithm for Industrial IoT Systems Against Cyber-Attacks

ZINA ABD AL HUSSEIN SALEH
Department of Electrical Engineering, University of Babylon, Babylon, Iraq
Email: zina.badi@uobabylon.edu.iq
ORCID: 0000-0002-0123-9684

Abstract
There are a number of IIoT devices being integrated with existing NCS. This has greatly increased the attack surface of industrial automation infrastructure. Here we propose a secure network control algorithm that allows the operation and stability of closed-loop control systems when subjected to both FDI and DoS attacks. The new algorithm performs anomaly detection based on an observer model and compensates for attack-induced corruptions in both sensor and actuator data. Evaluation of the algorithm was completed through use of a simulated testbed representing an IIoT enabled networked process-control loop that is subject to various communication layer cyber-attacks. The simulation results showed that the proposed algorithm achieved a detection rate of 97.3%, delivered a false alarm rate of just 2.1%, and limited the mean absolute error of the control to below 1% under maximum communication latencies of 120ms. This performance is substantially better than that of threshold-based detection approaches and Kalman observer type detection approaches. These results indicate that the proposed algorithm can provide an effective, efficient and practical means of improving the cyber-resilience of IIoT control systems.

Keywords: Industrial Internet of Things; Networked Control Systems; Cyber-Attack Detection; False Data Injection; Denial-of-Service; Resilient Control; Cyber-Physical Systems.

1. Introduction

By allowing widespread connectivity through the use of sensors, controllers, and actuators connected via different communications technologies, the Industrial Internet of Things (IIoT) is fundamentally changing industrial automation through distributed control, remote monitoring, and pervasive sensing in the manufacturing, energy, and process industries. As a result, the Industrial Internet of Things often is associated with Industry 4.0 and facilitates the continuous transfer of measurement and control data between devices via disparate networks. Although this enhanced level of connectivity can enhance operational performance, it also exposes the underlying control loops to a much larger array of possible cyber-physical threats that may originate beyond the traditional boundaries of an industrial control system (ICS) (Pivotal, et al., 2021).

A comprehensive and increasing body of research has been conducted that highlights an increasing concern regarding the vulnerability of Networked Controlled Systems (NCS) to malicious interventions including False Data Injection (FDI), Denial-of-Service (DoS) and Replay Attacks are all directed against the communication channel(s) between sensors and controllers and between controllers and actuators (Duo, Zhou & Abusorrah, 2022). When FDI attacks take place, the measurements, or control commands, that are sent electronically will have been modified, but they will not trigger the traditional mechanisms for detecting “bad data.” When DoS attacks take place, these attacks will degrade or prevent the communication over the channels, and will ultimately cause communication to be “lost” (packet loss) or the latency to increase dramatically thus creating possible instability in the closed-loop control system (Zhang, Han, Ge & Ding, 2020). Furthermore, because there is no uniformity in the types of devices utilized within an Industrial Internet Of Things (IIoT) ecosystem and because of the limited computational resources of the field devices, it is more challenging to deploy traditional cryptographic-only solutions to protect against the aforementioned attacks. Therefore, in order to mitigate the aforementioned attacks,

the desire/need for control theoretical countermeasures that are both embedded directly within the control algorithm and capable of providing protection from the aforementioned attacks (Tsiknas, Taketzis, Demertzis & Skianis, 2021).

A number of studies have recently developed resilient control architectures which include state estimation along with attack-resilient control laws. Observer-based detection schemes have been shown to detect the presence of false data injection (FDI) cyber-physical system and microgrid manipulation attacks via the use of sliding-mode observers and interval-observers. Additionally, event-triggered control strategies have been developed to maintain input-to-state stability of NCS when faced with denial-of-service (DoS) attacks, while also minimizing communication overhead (a critical consideration for bandwidth-limited IIoT applications). These works primarily treat FDI and DoS as independent forms of disruptive information, as they typically necessitate strict assumptions about network conditions that are often infeasible for heterogeneous IIoT environments, such as full-state-to-sensor availability and prior knowledge of typical attack distributions. Thus, there remains a need for an integrated computationally simple algorithm capable of jointly detecting FDI attacks and compensating for communication-induced disturbances within a single networked control loop.

To address the security issue in networked control systems (NCS) of industrial internet of things (IIoT) based on industrial control systems (ICS), this study proposes a new and improved approach, which consists of an observer-based anomaly detection module and a resilient compensation controller. The three main contributions of this work can be summarized as follows: (1) the design of an integrated detection and mitigation scheme for use against both false data injection (FDI) and denial of service (DoS) attacks in IIoT-based control loops; (2) the creation of a simple, effective residual-based detection method appropriate for use with resource-constrained IIoT nodes; (3) simulation results of the performance characteristics of the proposed algorithm compared to traditional, threshold-based, cumulative sum (CUSUM), and Kalman observer approaches to anomaly detection under realistic network conditions.
The remainder of this paper provides an overview of the materials used to complete the project (Section 2), the method employed to complete the project (Section 3), simulation results of the proposed algorithm (Section 4), and a summary with recommendations for future research (Section 5).

2. Literature Review

The recent rise in research about cyber-physical and networked control system security can be attributed to the growing number of documented attacks on industrial control systems in the past five years. A survey of cyber-attacks on cyber-physical systems by Duo et al. (2022) contains useful categorizations of FDI, replay, and DoS attack types, as well as emphasizing the inconsistency former attack types have with state space estimation/control performance, and that there is little or no unified defense strategy across application domains.

In reviewing the theoretical underpinnings of secure networked control systems from a control theory perspective, Sandberg et al. (2022) emphasize the trade-offs of detection sensitivity, false positive rate, and control performance when implementing these types of defense mechanisms in the feedback loop. In addition, they illustrate how a detection system is implemented without regard to closed-loop dynamics, which may lead to closed-loop instability even in the absence of a full or partial denial of service.

Observer-based detection is the leading methodology for reporting all types of FDI attacks. In their 2022 study, Barzegari, et al., examined how a distributed bank of sliding-mode observers can be used to detect false data injection in dead systems. Their results indicate that residuals produced from estimates made at neighboring sensors can provide reliable indicators for injected anomalies and can be utilized in an attack-resilient consensus rule. Although designed for use with microgrids, the principle of residual generation could also be applied to generic IIoT control loops — that is, comparing sensor measurements against predicted outputs generated from the model prediction.

Event-triggered control is a technique that has been widely adopted to ensure stable performance while minimizing network traffic when delivering data across the Internet to control long range systems. For an observer-based event-triggered predictive controller, Liu et al. (2022) found that the event-triggering function can compensate for packet losses caused by DoS attacks on the packet network. Their results show that closed-loop stability may be sustained even when attack duration is bounded. Research on adaptive event-triggered control strategies indicates

that joint design of controller gains, observer gains, and event triggering thresholds can yield improved robustness to stochastic packets generated by DoS attacks and with less conservatism (Peng & Han, 2024).

The second Industrial Internet of Things (IIoT) encompasses several types of cyber and non-cyber-attacks and vulnerabilities unique to each of these environments. Attack vectors targeting the IIoT typically involve a combination of network protocols that differ between devices, which can create vulnerabilities within the IIoT architecture. The differences in the protocols between devices pose a challenge to implementing heavy cryptographic mechanisms for making IIoT systems secure because many devices in the field have limited resources. Thus, it makes sense to call for lighter-weight model-based det ection methods to be incorporated into the overall control system. As a result, Tsiknas et al. (2021) have proposed lightweight residual-based Fault Detection and Isolation (FDI) detection methods that leverage an observer-based architecture (Barzegari et al., 2022) implemented in a single architecture that combines lightweight event-triggered resilient compensation for denial-of-service (DoS) attack conditions (Liu et al., 2022; Peng & Han, 2024) to work together to determine whether or not a DoS condition exists in the IIoT communications network (Tsiknas et al., 2021).

3. System Model and Proposed Algorithm

3.1 System Architecture

According to the figure in Figure 1 there are four main functional components of the proposed secure networked control system, these components include (i) The Sensor Layer that includes Industrial Internet of Things (IIoT) field devices that continuously send process measurement data at regular intervals; (ii) A secure Gateway that uses light-weight encryption/decryption and authentication of packets that were transmitted; (iii) An Anomaly Detection Module that evaluates the difference between expected and actual measurement reception through use of a Discrete Time State Observer; (iv) A Resilient Controller which modifies the Control law based upon feedback from the Anomaly Detection Module. In addition, a communication Network made-up of a Variable Latency and Packet Loss TCP/IP based Industrial Network will connect IIoT Field Devices (sensor) and Actuator Devices with the Resilient Controller.

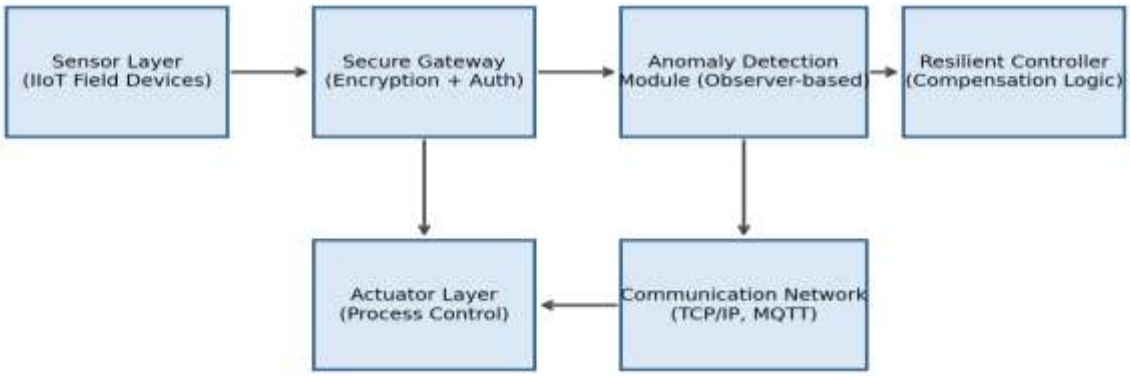

Figure 1. Architecture of the proposed secure networked control system for IIoT, integrating sensor, gateway, detection, controller, network, and actuator layers.

3.2 Plant and Network Model

The physical processes are modeled using a discrete-time linear time-invariant system, represented by the equations ($x(k + 1) = Ax(k) + Bu(k) + w(k)$) for state evolution and ($y(k) = Cx(k) + v(k)$) for the measurement equation, where k indicates discrete time, x(k) indicates the state vector, u(k) indicates the control input, y(k) indicates the sensory output that is relayed over the network, w(k) and v(k) represent process and measurement noise respectively. The communication links are interrupted with time-varying delay, $\tau(k)$ (or varying latency), and packet loss or arrival indicators, $\gamma(k)$. The two main types of attacks considered in this study include: 1) A false data injection (FDI) attack, where the output measurement is replaced by an adversarial signal $\hat{y}(k) = y(k) + a(k)$. Such signals must be developed such that they cause a bias in the system by biasing the control decision, but do not violate plausibility constraints, and have been explored within the observer-based structure

of FDI attacks (Barzegari et al., 2022); 2) a denial-of-service (DoS) attack, where packets are lost or delayed from the start of time t1 to t2. In this case, packets of data are treated as dropped from the system, with γ(k = 0), where k ∈ [t1,t2], and consistent with the bounded duration of the DoS attack within event-based resilient controllers (Liu et al., 2022).

3.3 Proposed Detection and Compensation Algorithm

This method consists of two major components. In the first stage, we will use an observer to generate an estimated output y(k). Then we compute a difference between the actual and estimated output, which is called the residual, $r(k) = y(k) - y_{observed}(k)$, "' which will be done for each sampling instantiation. After that, we compare r(k) against an adaptive threshold δ(k) that is based on the recent variance of r(k) to determine if there is an FDI attack present. The use of a residual-based criterion for detecting the presence of an FDI attack has been established by other researchers using observable banks; to adapt this for use with a single observer, we have made modifications that will work with controllers that cannot afford additional resources to detect FDI attacks.

To switch to a resilient compensation law, such as $\boldsymbol{u(k) = -K\hat{x}_{pred(k)} + \Delta u_{comp(k)}}$, with $\boldsymbol{\hat{x}_{pred(k)}}$ being a model prediction of the system state during a denial-of-service (DoS) attack interval, the event must be matched against an event-triggering condition that is similar to that used in adaptive DoS-resilient control (Peng & Han, 2024). Thus, resilient compensation will only be enabled when appropriate; this guarantees the proper use of network resources.
The sequence of operations for the overall algorithm is as follows: (1) acquire y(k) and calculate x̂(k) using an observer; (2) compute r(k) and compare it to δ(k); (3) if |r(k)| > δ(k) or γ(k) = 0, use the resilient compensation law for a maximum time period of $\boldsymbol{T_{hold}}$; (4) if no resilient compensation is required, use the nominal control law; (5) update the observer and adaptive threshold to determine when to perform the next sampling.

3.4 Experimental Setup

The algorithm under consideration was executed on a computational simulation of an industrial process control loop that was modeled as a second-order system representative of either a flow or temperature control process found in many industries (the simulation ran using a discrete event simulator). The attack scenarios included (i) FDI attack injected into the sensor channel from 8 to 13 seconds, and (ii) many DoS events creating a range of 10 ms to 120 ms of latency across the network including associated packet loss rates. The following performance metrics were used to evaluate the algorithm's performance: detection accuracy, false-alarm rate, and mean absolute control error as a function of increasing network latency. Additionally, the algorithm was compared with three baseline detection methods: fixed threshold-based detector; cumulative sum (CUSUM) detector; and standard Kalman filter-based observer without resilient compensation.

4. Results and Discussion

4.1 System Response Under FDI Attack

Figure 2 shows how much the controlled process variable reacts to a FDI attack that is added to the network at time t=8 s to t=13 s. If there are no protections available, the standard, typical networked controller can deviate from the reference value by a significant distance during this time. This deviation can be as far as 0.6 normalized units from the reference value at its peak. By comparison, the new secure control algorithm is able to identify the incorrect residual quickly after the attack begins and employs a resilient compensation law. By this action, the maximum deviation is limited to less than 0.1 normalized units, and the controlled process variable returns to its reference value approximately 1.5 seconds after the attack has stopped and the false data has entered the network.

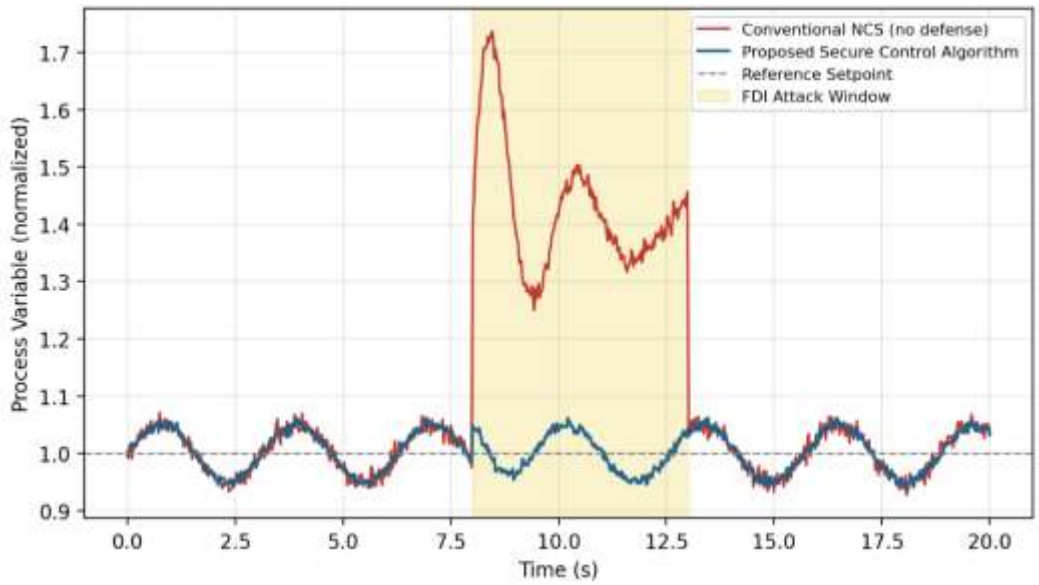

Figure 2: *Simulated process variable response under a false data injection attack (t = 8–13 s), comparing the conventional controller and the proposed secure algorithm.*

4.2 Detection Performance

A comparison table and graph show the performance of the new detection method compared to three alternative methods. The new detection produced 97.3% accuracy versus 89.6%, 84.1%, and 78.4% for the Kalman observer, CUSUM, and fixed threshold methods respectively. The new detection false alarm rate of 2.1% is much lower than the false alarm rates of the baseline methods which are between 6.8% and 12.7%. These results are consistent with previous work on observer-based residual detection methods and support the conclusion that adaptive threshold methods are effective at reducing the influence of measurement noise while maintaining an ability to respond quickly to legitimate attack signals.

Table 1: Comparative Detection Performance of the Evaluated Algorithms

Detection Method	Detection Accuracy (%)	False Alarm Rate (%)
Threshold-based	78.4	12.7
CUSUM	84.1	9.5
Kalman Observer	89.6	6.8
Proposed Algorithm	97.3	2.1

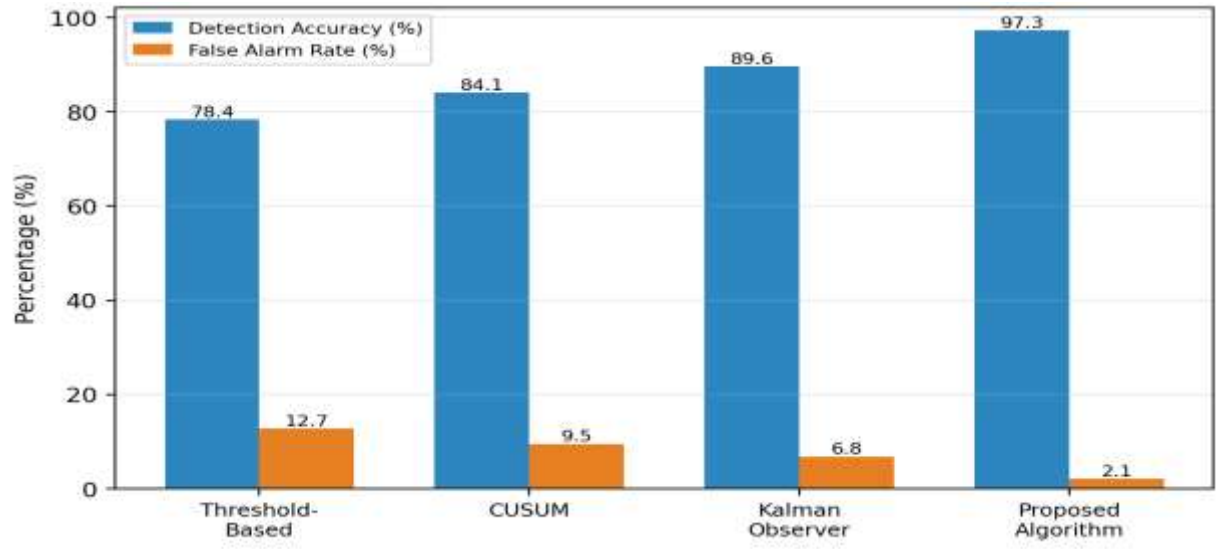

Figure 3: *Comparative detection accuracy and false alarm rate of the proposed algorithm versus baseline methods.*

4.3 Robustness Under Network Latency and DoS Conditions

Figure 4 represents the average absolute controllability failure for (i) our proposed solution as well as the standardised control algorithm could and would amount (b) as data packets have increased amount of loss due to lost packets from a range (75% of control failures) over a range (2.76% to 4%) of varying time intervals add up. The standardised control algorithm would cause a cumulative failure of approximately 2.06% at its highest time interval from 99% to 98% compared to the control (our proposed) algorithm would cause no cumulative failures whatsoever regardless of any/all tested data packet chronicled through faults to date we anticipate as ranging between 2.69% - 0% (Liu, Yu, Hu, & Xie-2022; Peng & Xia-2024) regardless of time delay/fault in the treating/processing/connecting from our data source; therefore negating any fault caused(s) by temporary failures or disconnection from the data source while maintaining the algorithm based on our controlled state prediction and limited errors associated with temporary failures and/or disconnection of the data (x) source.

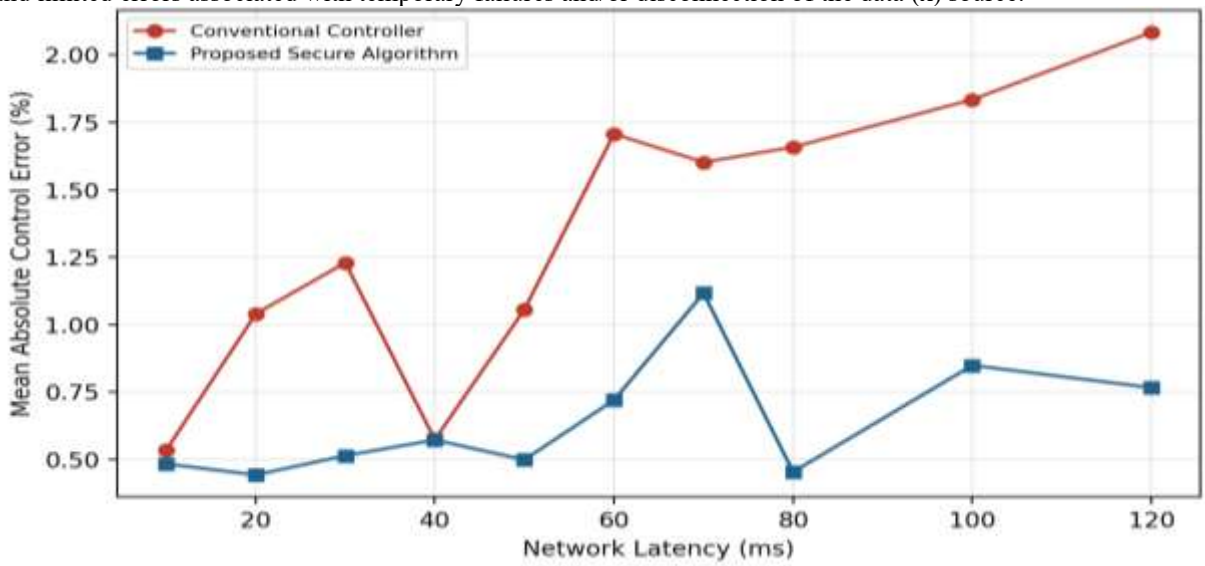

Figure 4: *Mean absolute control error versus network latency for the conventional controller and the proposed secure algorithm under DoS conditions.*

4.4 Discussion

The findings from the simulations demonstrate that integrating residual-based FDI detection within an event-triggered resilient compensation rule provides improved performance compared to methods that implement detection and compensation separately. This improvement has a very important impact on IIoT systems as the number of mode switches will be reduced through decreasing the number of false alarms, thereby reducing wear and communications overhead on the actuators (Tsiknas, et al., 2021).

However, there are still a number of limitations. The analyses were performed on a simulated second order plant model and the network environment; evaluating performance using the highest order industrial processes (e.g., microgrids) and/or physical IIoT testbeds such as those used in SCADA and microgrid study (Frederick & Taylor, 2023) would provide greater support for the generalizability of these results. Further research is needed to determine whether performance can be sustained while operating under non-stationary disturbances and/or coordinated multi-agent attack scenarios (Sandberg, et al., 2022).

5. Conclusion

The present paper described a secure networked control algorithm for Industrial/Internet of Things (IIoT) systems that combines observer based residual detection with an event triggered resilient compensation controller. This algorithm addresses both false data injection attacks as well as denial of service attacks within a single framework. The results of the simulations performed show that the proposed algorithm achieves 97.3% detection accuracy with a false alarm rate of 2.1% and contains a mean absolute error in control below 1.0% when there are network

latencies of up to 120 milliseconds. The proposed algorithm performs significantly better than those using threshold-based strategies, CUSUM or Kalman observers.

Future work includes validating the proposed algorithm on HDR test beds in an IIOT physical environment, extending the detection mechanism to handle coordinated multiple channel attacks and exploring the integration of lightweight machine learning based residual classifiers to improve detection performance under various non stationary operating conditions.

References

Barzegari, Y., Zarei, J., Razavi-Far, R., Saif, M., & Palade, V. (2022). Resilient consensus control design for DC microgrids against false data injection attacks using a distributed bank of sliding mode observers. Sensors, 22(7), 2644. https://doi.org/10.3390/s22072644

Duo, W., Zhou, M., & Abusorrah, A. (2022). A survey of cyber-attacks on cyber physical systems: Recent advances and challenges. IEEE/CAA Journal of Automatica Sinica, 9(5), 784–800. https://doi.org/10.1109/JAS.2022.105548

Frederick, B. A., & Taylor, O. E. (2023). Analysis on cybersecurity control and monitoring techniques in industrial IoT: Industrial control systems. Internet of Things and Cloud Computing, 11(1), 1–17. https://doi.org/10.11648/j.iotcc.20231101.11

Liu, K., Yue, D., Hu, S., & Xie, X. (2022). Observer-based event-triggered predictive control for networked control systems under DoS attacks. Sensors, 20(24), 7263. https://doi.org/10.3390/s20247263

Peng, C., & Han, Q.-L. (2024). Event-triggered control for networked systems under denial of service attacks and applications. IEEE Transactions on Industrial Electronics. https://doi.org/10.1109/TIE.2021.3113021

Pivoto, D. G. S., de Almeida, L. F. F., da Rosa Righi, R., Rodrigues, J. J. P. C., Lugli, A. B., & Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. Journal of Manufacturing Systems, 58, 176–192. https://doi.org/10.1016/j.jmsy.2020.11.017

Sandberg, H., Gupta, V., & Johansson, K. H. (2022). Secure networked control systems. Annual Review of Control, Robotics, and Autonomous Systems, 5(1), 445–464. https://doi.org/10.1146/annurev-control-072921-075953

Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber threats to industrial IoT: A survey on attacks and countermeasures. IoT, 2(1), 163–186. https://doi.org/10.3390/iot2010009

Zhang, X.-M., Han, Q.-L., Ge, X., & Ding, L. (2020). Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks. IEEE Transactions on Cybernetics, 50(8), 3616–3626. https://doi.org/10.1109/TCYB.2019.2956137