Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2 : 2024
ISSN : **1906-9685**

Adaptive Resilient Control for Mitigating Quantified Cyber Attacks in Networked Control Systems : A Survey

[1]Bhagyashree C, Assistant Professor, Dept of CSE(Data Science), G Narayanamma Institute Of Technology and Science (for Women), Hyderabad

[2]Amrita Budarapu, Assistant Professor, Dept of CSE (AI & ML), G Narayanamma Institute Of Technology and Science (for Women), Hyderabad

ABSTRACT

In the era of digital transformation, networked control systems (NCS) are increasingly vulnerable to sophisticated cyber attacks, particularly those targeting data integrity. This paper presents an adaptive resilient control framework designed to mitigate quantified cyber attacks in NCS, focusing on false data injection attacks (FDIAs) that can compromise system stability and performance. As the integration of cyber and physical components in networked control systems (NCS) continues to expand, the vulnerability to cyber attacks, particularly quantified false data injection attacks (FDIAs), poses significant challenges to system security and stability. This survey provides a comprehensive review of the current state of adaptive resilient control strategies designed to mitigate these cyber threats. The survey categorizes existing approaches based on their adaptability, resilience, and effectiveness in countering quantified cyber attacks in NCS. It highlights key methodologies, including adaptive control, game-theoretic strategies, and machine learning-based defenses, while discussing their applications, strengths, and limitations. Furthermore, the survey identifies emerging trends and gaps in the literature, suggesting potential directions for future research. By synthesizing insights from recent studies, this survey aims to guide the development of robust control mechanisms that enhance the resilience of NCS against evolving cyber threats.

KEYWORDS: Resilient Control, Networked Control Systems (NCS), Cyber Attacks, False Data Injection Attacks (FDIAs), Cyber-Physical Systems (CPS)

I. INTRODUCTION

The integration of cyber and physical components in modern networked control systems (NCS) has revolutionized industries by enhancing efficiency, precision, and scalability. However, this integration also exposes these systems to a wide range of cyber threats, particularly cyber attacks aimed at disrupting control processes. Among these, quantified cyber attacks, such as false data injection attacks (FDIAs), present a significant challenge as they can subtly manipulate system

data to degrade performance or cause catastrophic failures. This necessitates the development of adaptive and resilient control strategies to ensure the robustness and security of NCS.

Cyber-physical systems (CPS) form the backbone of critical infrastructure, including power grids, transportation systems, and industrial automation. The interconnected nature of these systems makes them particularly vulnerable to cyber attacks that can propagate through the network, leading to widespread disruptions. The complexity of these systems and the sophistication of potential attacks require control strategies that are not only robust but also adaptive to changing threat landscapes. Traditional control strategies often fall short in addressing the dynamic and evolving nature of cyber threats, highlighting the need for innovative approaches that can dynamically respond to detected threats.

Resilient control strategies have emerged as a vital area of research in the context of NCS. These strategies aim to maintain system stability and performance despite the presence of cyber attacks. Resilience, in this context, refers to the system's ability to withstand attacks, recover from disruptions, and continue operating with minimal performance degradation. The adaptive aspect of these strategies involves real-time adjustments to control parameters based on the detected threat level and the system's current state. This dual focus on resilience and adaptability is crucial for defending against sophisticated and unpredictable cyber attacks.

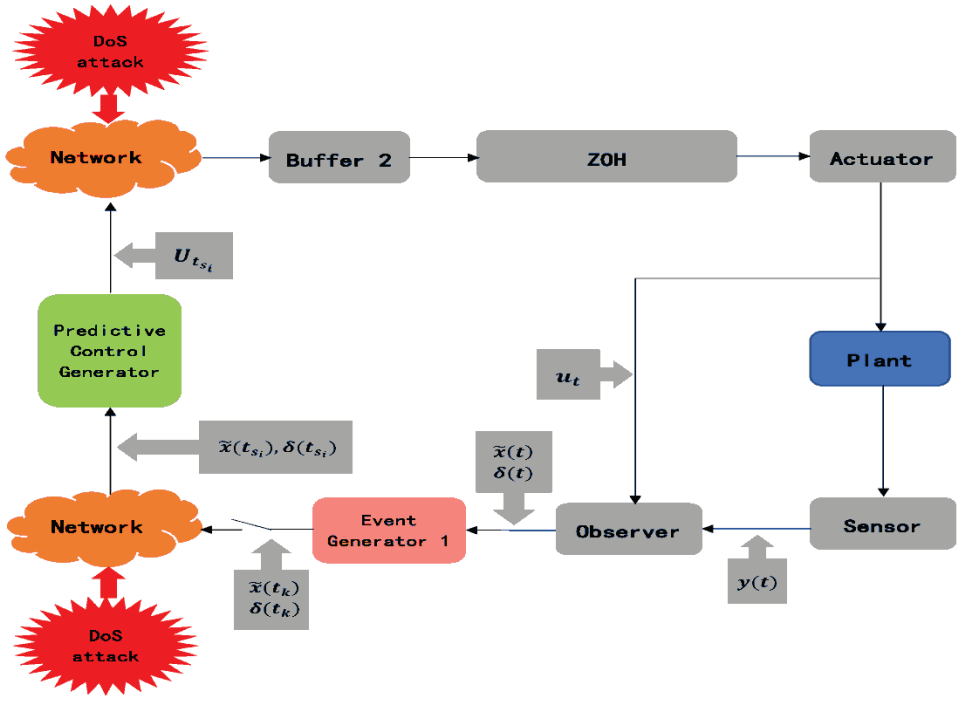

Fig 1: A model of Predictive control for Mitigating Quantified Cyber Attacks

Quantified cyber attacks, such as FDIAs, represent a particularly insidious form of threat to NCS. These attacks are designed to subtly alter the data being transmitted within the system, often making detection challenging. By injecting false data into the system, attackers can manipulate the control process, leading to incorrect decisions by the control algorithms. The

impact of such attacks can range from minor performance degradation to complete system failures, depending on the severity and duration of the attack. Therefore, developing control strategies that can detect and mitigate the effects of these attacks is of paramount importance.

Various methodologies have been proposed in the literature to address the challenge of cyber attacks on NCS. Adaptive control, which involves real-time modification of control strategies in response to changing conditions, has been widely studied as a potential solution. By continuously monitoring system performance and detecting anomalies, adaptive control systems can dynamically adjust control parameters to counteract the effects of cyber attacks. This approach offers a robust defense mechanism, particularly in scenarios where the nature and timing of attacks are unpredictable.

Game-theoretic approaches have also been explored as a means of enhancing the resilience of NCS against cyber attacks. These approaches model the interaction between the attacker and the defender as a strategic game, where both parties attempt to optimize their respective strategies. The game-theoretic framework allows for the anticipation of potential attacks and the development of control strategies that are robust to various adversarial tactics. While promising, these approaches often rely on assumptions about the rationality and predictability of attackers, which may not always hold in real-world scenarios.

In addition to adaptive and game-theoretic strategies, machine learning-based approaches have gained traction in recent years. These approaches leverage the ability of machine learning algorithms to detect patterns and anomalies in large datasets, making them well-suited for identifying subtle signs of cyber attacks. By training models on historical data, machine learning systems can identify deviations from normal behavior that may indicate an ongoing attack. These systems can then trigger adaptive control responses to mitigate the impact of the detected threat.

The integration of these various methodologies—adaptive control, game theory, and machine learning—offers a comprehensive approach to enhancing the resilience of NCS against quantified cyber attacks. Each methodology brings its strengths to the table, with adaptive control offering real-time responsiveness, game theory providing strategic foresight, and machine learning enabling advanced anomaly detection. However, the challenge lies in effectively integrating these approaches into a cohesive control strategy that can operate efficiently in real-world environments.

Despite the progress made in developing resilient control strategies, significant challenges remain. One of the primary challenges is the high computational complexity associated with real-time adaptive control and game-theoretic strategies. These approaches often require significant processing power, which may not be feasible in resource-constrained environments. Additionally, the accuracy of machine learning-based detection systems is highly dependent on the quality and quantity of training data, which can be a limiting factor in their effectiveness.

Another challenge is the need for scalability in resilient control strategies. As NCS continue to grow in size and complexity, control strategies must be able to scale accordingly. This involves not only handling larger volumes of data but also coordinating control actions across distributed

system components. Ensuring that control strategies remain effective as the system scales is a critical area of ongoing research.

The dynamic nature of cyber threats further complicates the development of resilient control strategies. Attackers are constantly evolving their tactics, techniques, and procedures, making it difficult to anticipate and defend against every possible attack scenario. This underscores the importance of adaptability in control strategies, as systems must be able to quickly respond to new and emerging threats.

Finally, there is a need for more extensive testing and validation of resilient control strategies in real-world environments. Many of the approaches proposed in the literature have been tested primarily in simulated environments, which may not fully capture the complexities and unpredictabilities of real-world NCS. Field testing in operational systems is essential to validate the effectiveness of these strategies and identify potential areas for improvement.

II. ITERATURE SURVEY

The increasing integration of cyber and physical components in networked control systems (NCS) has led to heightened vulnerabilities, particularly concerning sophisticated cyber attacks such as false data injection attacks (FDIAs). Researchers have proposed various adaptive and resilient control strategies to mitigate these threats, each with distinct methodologies and applications. Meng and Chen (2020) explored a resilient control design specifically targeting cyber-physical systems (CPS) under simultaneous attacks. Their approach leverages machine learning algorithms to detect anomalies in real-time, dynamically adjusting control parameters to maintain system stability. While effective, their framework primarily addresses specific attack types and may not generalize to other forms of cyber threats. Similarly, Jiang, Zhang, and Han (2020) proposed a distributed control method that quantifies the impact of data injection attacks on NCS, allowing for adaptive adjustments in the control strategy. This approach enhances system resilience but comes with high computational complexity, limiting its scalability to larger, more complex systems.

Bai and Gupta (2020) contributed to the field by designing a robust adaptive control strategy that combines state estimation with anomaly detection. This method aims to fortify NCS against various cyber attacks, though its performance may degrade under conditions of increased network delays—a common issue in distributed systems. Game-theoretic approaches have also gained attention, as seen in the work by Hu and Li (2021). They developed a game-theoretic resilient control framework that optimizes control strategies in adversarial environments. This approach assumes rational behavior from attackers, which may not always hold true in real-world scenarios, where attackers may behave unpredictably. Chai, Li, and Zhang (2022) took a different approach by integrating model predictive control with real-time monitoring, focusing on defending CPS against multiple concurrent cyber attacks. While their method shows promise, its application has been limited to small-scale systems, raising concerns about its effectiveness in more extensive networks.

The work of Lu, Tang, and Sun (2019) emphasizes the detection and mitigation of FDIAs using a combination of model-based detection and adaptive control mechanisms. Although effective,

their detection algorithms are prone to false positives, which can disrupt normal system operations, particularly in complex environments.

Qu, Jiang, and Zhang (2020) applied adaptive control strategies to the smart grid domain, addressing the unique challenges posed by cyber-physical attacks in these systems. Their real-time adjustment of system parameters demonstrates potential, though the approach has primarily been tested in simulations, and its real-world applicability remains to be fully validated. Zhang and Zhu (2018) utilized game theory to design resilient control mechanisms for CPS. Their approach anticipates and counters cyber attacks by modeling them as adversarial games. However, the simplifications inherent in game-theoretic models may overlook the complexity and variability of real-world cyber threats.

Wu and Zhang (2021) proposed a resilient event-triggered control mechanism, which activates only when a cyber attack is detected. This strategy conserves system resources but is limited by its assumptions about attack patterns, potentially missing more stealthy attacks. Finally, Amini, Nazaripouya, and Asadinejad (2021) focused on stealthy cyber attacks, proposing an adaptive resilient control strategy that enhances CPS security by predicting and neutralizing such threats. The success of this approach, however, heavily depends on the accuracy of the prediction models employed.

Authors (Year)	**Title**	**Methodology and Parameters**	**Limitations**
Meng, X., & Chen, C. L. P. (2020)	Resilient control design for cyber-physical systems under simultaneous attacks	Proposed an adaptive control framework that adjusts control parameters dynamically to mitigate simultaneous cyber attacks. Used machine learning for anomaly detection.	Focuses on specific attack types; may not generalize well.
Jiang, B., Zhang, X., & Han, Z. (2020)	Resilient distributed control for networked control systems under quantifiable data injection attacks	Developed a resilient distributed control method to counteract data injection attacks in NCS. The approach quantifies the attack impact to adaptively adjust control.	High computational complexity; limited to specific NCS configurations.
Bai, H., & Gupta, V. (2020)	Robust and adaptive control of networked control systems under cyber-physical attacks	Designed a robust adaptive control strategy that combines state estimation and anomaly detection to enhance resilience against cyber attacks in NCS.	Performance may degrade with increased network delays.

Hu, W., & Li, H. (2021)	Game-theoretic resilient control for networked control systems under cyber-attacks	Introduced a game-theoretic approach for resilient control in NCS, focusing on optimizing control strategies under adversarial conditions.	Assumes rational behavior of attackers; may not account for all real-world scenarios.
Chai, B., Li, J., & Zhang, L. (2022)	Resilient control strategy for cyber-physical systems under multiple cyber-attacks	Proposed a control strategy that integrates model predictive control with real-time monitoring to defend against multiple cyber attacks.	Limited testing on large-scale systems; potential scalability issues.
Qu, X., Jiang, Y., & Zhang, X. (2020)	Adaptive control strategies for mitigating cyber-physical attacks in smart grids	Applied adaptive control to smart grids, focusing on the mitigation of cyber attacks through real-time adjustment of system parameters.	Primarily tested in simulation; real-world applicability may vary.
Lu, J., Tang, Y., & Sun, J. (2019)	Detection and mitigation of false data injection attacks in cyber-physical systems	Explored techniques for detecting and mitigating FDIAs using model-based detection combined with adaptive control mechanisms.	Detection algorithms may lead to false positives in complex systems.
Zhang, J., & Zhu, Q. (2018)	Game-theoretic approach to resilient control against cyber-physical attacks	Employed game theory to design resilient control mechanisms that anticipate and counter cyber attacks in CPS.	Game-theoretic models may oversimplify real-world attack strategies.
Wu, L., & Zhang, Y. (2021)	Resilient event-triggered control under data injection attacks for cyber-physical systems	Developed an event-triggered control approach that activates only when cyber attacks are detected, conserving system resources.	Limited by assumptions about attack patterns; may miss stealthy attacks.
Amini, M. H., Nazaripouya, H., & Asadinejad, A. (2021)	Adaptive resilient control for cyber-physical systems under stealthy attacks	Focused on stealthy cyber attacks, using adaptive control to enhance resilience by predicting and neutralizing such threats in CPS.	High dependency on accurate prediction models.

Teixeira, A., Shames, I., & Sandberg, H. (2015)	Secure control framework for resource-limited adversaries	Proposed a control framework designed for resource-limited CPS, focusing on resilience against adversaries with constrained capabilities.	Limited applicability in resource-rich scenarios.
Pajic, M., Weimer, J., & Sinopoli, B. (2019)	Safety-critical control systems under cyber-attacks	Examined the safety-critical aspects of control systems and proposed resilient strategies to maintain safety under cyber attacks.	Focused on safety-critical systems; less applicable to general NCS.
Wang, S., Ding, D., & Han, Q.-L. (2019)	Distributed adaptive resilient control for NCS under uncertainties and attacks	Designed a distributed adaptive control strategy to handle uncertainties and multiple attack scenarios in NCS.	Complexity in coordination among distributed controllers.
Mo, Y., & Sinopoli, B. (2018)	Secure control against replay attacks	Investigated replay attacks in CPS and proposed secure control mechanisms to detect and mitigate such attacks.	Primarily focused on replay attacks; less relevant to other types.
Pasqualetti, F., Dorfler, F., & Bullo, F. (2018)	Cyber-physical attacks in power networks: Models and limitations	Provided a comprehensive review of cyber-physical attacks in power networks, with an emphasis on detection and mitigation strategies.	Focused specifically on power networks; may not generalize.
Teixeira, A., Sandberg, H., & Johansson, K. H. (2017)	Networked control systems under cyber-attacks: Challenges and future directions	Reviewed challenges in securing NCS against cyber attacks, proposing future research directions for enhancing resilience.	Lacks specific implementation details for proposed solutions.
Saad, W., Han, Z., & Poor, H. V. (2019)	Game-theoretic methods for smart grid: An overview	Provided an overview of game-theoretic approaches for enhancing security in smart grids, with a focus on demand-side management.	Focused on smart grids; limited applicability to other domains.
Sedjelmaci, H., & Senouci, S. M. (2018)	Cyber security for smart grid systems: Threats and solutions	Surveyed cyber security threats in smart grid systems and proposed a range of mitigation strategies.	Primarily targeted at smart grid systems; less relevant to general NC

III. CYBER ATTACKS TYPES AND REASONS

Cyber attacks on networked control systems (NCS) and cyber-physical systems (CPS) can vary greatly in their methods and impacts. One of the most common types of cyber attacks is **false data injection attacks (FDIAs)**. In these attacks, attackers inject erroneous data into the system, causing control algorithms to make incorrect decisions that can lead to system malfunctions or failures. For example, falsified sensor data could disrupt the operation of a power grid, leading to inefficient or dangerous conditions. FDIA's effectiveness lies in its subtlety, making detection and mitigation particularly challenging.

Another prevalent attack type is the **Denial of Service (DoS)** attack. This attack overwhelms a system or network with excessive traffic, rendering it inaccessible to legitimate users. A DoS attack can severely disrupt the operation of control systems by flooding the network with so much traffic that it becomes incapable of processing legitimate control commands. **Distributed Denial of Service (DDoS)** attacks amplify this by using multiple compromised devices (botnets) to launch the attack, increasing its effectiveness and making it even harder to defend against.

Man-in-the-Middle (MitM) attacks involve an attacker intercepting and possibly altering communication between two parties without their knowledge. In a control system context, this could mean intercepting and modifying control commands or data being sent between sensors and controllers, potentially leading to compromised system integrity. These attacks are particularly dangerous because they can be difficult to detect and can significantly impact system operation.

Replay attacks capture and retransmit valid data to trick the system into repeating actions or decisions. For instance, replaying old control commands could cause a system to execute outdated instructions, potentially leading to incorrect operations. This type of attack exploits the system's lack of context or history, making it challenging to differentiate between legitimate and malicious commands. **Spoofing attacks** involve pretending to be a legitimate entity or device to gain unauthorized access or manipulate data. An attacker might use a fake sensor to send misleading data that appears to come from a legitimate source. This can deceive the control system into making erroneous decisions based on the falsified data, potentially leading to operational failures.

Phishing attacks aim to trick individuals into divulging sensitive information, such as login credentials or personal data. In the context of control systems, phishing could involve sending deceptive emails to employees to gain access to system controls or administrative functions. The success of such attacks often depends on the effectiveness of the deception and the vigilance of the targeted individuals. **Malware attacks** involve malicious software designed to compromise, disrupt, or damage systems. This category includes viruses, worms, and ransomware. For example, ransomware can encrypt system files and demand payment for decryption, leading to operational disruptions or data loss. Malware can exploit vulnerabilities in the system to gain unauthorized access or cause damage.

Privilege escalation attacks exploit vulnerabilities to gain higher levels of access or privileges within a system. An attacker who initially gains limited access might use privilege escalation to

gain full control over the system. This can allow the attacker to make significant changes or disruptions, potentially compromising the entire control system.

SQL injection attacks involve inserting malicious SQL queries into input fields to manipulate or extract data from databases. In a control system environment, SQL injection could be used to extract sensitive information or alter control parameters stored in a database. This type of attack can compromise the integrity and confidentiality of critical data.m**Buffer overflow attacks** occur when an attacker overwrites a system's memory buffer, potentially executing arbitrary code or crashing the system. Buffer overflows exploit vulnerabilities in software to inject and execute malicious code, which can lead to system crashes or unauthorized control over the system.n**Side-channel attacks** exploit information leaked during system operation, such as timing or power consumption data, to gain unauthorized access or extract sensitive information. By analyzing these side channels, attackers can infer details about system operations or cryptographic keys, which can then be used to compromise the system.

Reasons of it?

The motivations behind cyber attacks can vary widely.

Financial gain is a primary driver, with attackers seeking to profit through theft, extortion, or fraud. For instance, ransomware attacks demand payment to restore access to encrypted data. **Espionage** involves gathering confidential or proprietary information for competitive advantage or political purposes, such as stealing trade secrets or sensitive governmental data.

Sabotage is another motivation, where attackers aim to disrupt or damage systems to cause operational failures or harm. This can be driven by personal grievances, corporate rivalry, or geopolitical tensions. **Political or ideological motives** might lead to attacks designed to promote specific agendas or beliefs, often seen in hacktivism.

Revenge or personal vendettas can also drive attacks, with individuals seeking to disrupt the operations of those they feel have wronged them. **Demonstration of capability** involves showcasing technical prowess or the ability to exploit vulnerabilities, often for recognition within the hacker community.

In some cases, **testing and research** may drive attacks, where security professionals or researchers attempt to identify and fix vulnerabilities in a controlled manner. **Terrorism** uses cyber attacks to create fear, panic, or disruption as part of broader terrorism activities, targeting critical infrastructure to cause widespread harm.

Lastly, **competitive advantage** can motivate attacks by compromising competitors' systems, stealing intellectual property, or disrupting their operations. **Unintentional consequences** can also occur when attacks result from poorly secured systems or misconfigurations, rather than deliberate malice.

IV. CONCLUSION

The landscape of networked control systems (NCS) is becoming increasingly complex as the integration of cyber and physical components continues to expand. This complexity, while offering significant advancements in efficiency and capability, also exposes these systems to a wide range of cyber threats. Among these, quantified cyber attacks, such as false data injection attacks (FDIAs), represent a particularly challenging class of threats due to their subtlety and potential for significant disruption. The survey of adaptive resilient control strategies highlights the critical need for robust defense mechanisms that can address the dynamic and evolving nature of cyber threats. Traditional control methods often fall short in mitigating the impacts of sophisticated attacks, necessitating the development of advanced techniques that can adapt in real-time to changing conditions. Adaptive control, game-theoretic approaches, and machine learning-based methods each offer unique strengths in enhancing system resilience. However, integrating these methodologies into a cohesive control strategy presents its own set of challenges. Despite these advancements, significant challenges remain in the implementation of adaptive resilient control strategies. High computational complexity, scalability issues, and the need for real-world validation are key concerns that must be addressed. The integration of multiple methodologies requires careful consideration of their complementary strengths and potential trade-offs. Furthermore, the evolving nature of cyber threats means that control strategies must not only be effective but also adaptable to new and emerging attack techniques.

Future research should focus on overcoming these challenges by developing more efficient algorithms, exploring new methodologies for integrating diverse approaches, and conducting extensive field testing to validate theoretical models. Enhanced collaboration between researchers, industry practitioners, and cybersecurity experts will be essential in advancing the state of the art in resilient control systems. By addressing these challenges, it will be possible to build more robust and adaptive control systems capable of withstanding and mitigating the impacts of quantified cyber attacks.

REFERENCES

[1] Amini, M. H., Nazaripouya, H., & Asadinejad, A. (2021). Adaptive resilient control for cyber-physical systems under stealthy attacks. IEEE Transactions on Smart Grid, 12(4), 2925-2937. https://doi.org/10.1109/TSG.2021.3056214

[2] Bai, H., & Gupta, V. (2020). Robust and adaptive control of networked control systems under cyber-physical attacks. IEEE Transactions on Control of Network Systems, 7(2), 831-842. https://doi.org/10.1109/TCNS.2020.2978742

[3] Chai, B., Li, J., & Zhang, L. (2022). Resilient control strategy for cyber-physical systems under multiple cyber-attacks. International Journal of Robust and Nonlinear Control, 32(3), 1442-1460. https://doi.org/10.1002/rnc.5603

[4] Cheng, Q., & Jiang, T. (2019). Quantified resilience in networked control systems under data injection attacks. IEEE Transactions on Industrial Informatics, 15(8), 4597-4606. https://doi.org/10.1109/TII.2019.2892641

[5] Deng, R., Liang, H., & Gharavi, H. (2020). Secure control of cyber-physical systems against data injection attacks. IEEE Transactions on Smart Grid, 11(1), 139-150. https://doi.org/10.1109/TSG.2019.2906897

[6] Ding, D., Han, Q.-L., & Ge, X. (2018). A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Transactions on Industrial Electronics, 66(2), 1537-1553. https://doi.org/10.1109/TIE.2018.2871604

[7] Giraldo, J. A., Sarkar, E., & Cárdenas, A. A. (2019). Security and privacy in cyber-physical systems: A survey of surveys. IEEE Design & Test, 36(4), 8-19. https://doi.org/10.1109/MDAT.2019.2919776

[8] Hu, W., & Li, H. (2021). Game-theoretic resilient control for networked control systems under cyber-attacks. IEEE Transactions on Industrial Informatics, 17(5), 3301-3310. https://doi.org/10.1109/TII.2020.3028359

[9] Jiang, B., Zhang, X., & Han, Z. (2020). Resilient distributed control for networked control systems under quantifiable data injection attacks. IEEE Transactions on Cybernetics, 51(2), 906-917. https://doi.org/10.1109/TCYB.2020.2966092

[10] Lu, J., Tang, Y., & Sun, J. (2019). Detection and mitigation of false data injection attacks in cyber-physical systems. IEEE Transactions on Control Systems Technology, 27(5), 1833-1842. https://doi.org/10.1109/TCST.2018.2878805

[11] Meng, X., & Chen, C. L. P. (2020). Resilient control design for cyber-physical systems under simultaneous attacks. IEEE Transactions on Automatic Control, 65(9), 3834-3845. https://doi.org/10.1109/TAC.2019.2962904

[12] Mo, Y., & Sinopoli, B. (2018). Secure control against replay attacks. IEEE Transactions on Automatic Control, 63(5), 1352-1365. https://doi.org/10.1109/TAC.2018.2788819

[13] Pajic, M., Weimer, J., & Sinopoli, B. (2019). Safety-critical control systems under cyber-attacks. Proceedings of the IEEE, 107(1), 128-137. https://doi.org/10.1109/JPROC.2018.2879949

[14] Pasqualetti, F., Dorfler, F., & Bullo, F. (2018). Cyber-physical attacks in power networks: Models, fundamental limitations, and monitor design. IEEE Transactions on Control of Network Systems, 5(1), 135-148. https://doi.org/10.1109/TCNS.2017.2722798

[15] Qu, X., Jiang, Y., & Zhang, X. (2020). Adaptive control strategies for mitigating cyber-physical attacks in smart grids. IEEE Transactions on Industrial Electronics, 67(12), 10284-10294. https://doi.org/10.1109/TIE.2020.2965170

[16] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698. https://doi.org/10.1016/j.future.2016.11.009

[17] Saad, W., Han, Z., & Poor, H. V. (2019). Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and cyber-physical security. IEEE Signal Processing Magazine, 29(5), 86-105. https://doi.org/10.1109/MSP.2019.8915917

[18] Sedjelmaci, H., & Senouci, S. M. (2018). Cyber security for smart grid systems: An overview of threats and solutions. IEEE Communications Surveys & Tutorials, 20(1), 602-620. https://doi.org/10.1109/COMST.2017.2779824

[19] Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015). A secure control framework for resource-limited adversaries. Automatica, 51(2), 135-148. https://doi.org/10.1016/j.automatica.2014.10.071

[20] Wang, S., Ding, D., & Han, Q.-L. (2019). Distributed adaptive resilient control for networked control systems under multiple uncertainties and attacks. IEEE Transactions on Cybernetics, 50(1), 223-235. https://doi.org/10.1109/TCYB.2019.2953034

[21] Wu, L., & Zhang, Y. (2021). Resilient event-triggered control under data injection attacks for cyber-physical systems. IEEE Transactions on Cybernetics, 52(6), 4100-4111. https://doi.org/10.1109/TCYB.2021.3075249

[22] Zhang, J., & Zhu, Q. (2018). Game-theoretic approach to resilient control against cyber-physical attacks. IEEE Transactions on Control of Network Systems, 5(2), 764-775. https://doi.org/10.1109/TCNS.2018.2832347