Analysis And Design of Secure Sampled-Data Control Subject to Denial-Of-Service Attacks

Mohammed Abdul Kareem[1], Mohammed Abbas Qureshi[2], Subramanian K.M [3]

[1]PG Scholar, Department of IT, Shadan College of Engineering and Technology, Hyderabad, Telangana, India-500086

[2]Associate Professor, Department of CSE, Shadan College of Engineering and Technology, Hyderabad, Telangana, India-500086

[3]Professor, Department of CSE, Shadan College of Engineering and Technology, Hyderabad, Telangana, India-500086

***Abstract*—The problem of secure control design against denial of service (DoS) attacks for cyber-physical systems (CPS) is the focus of this work. We consider a continuous-time linear system with sampled linear state feedback control and a convex quadratic performance measure. DoS attacks place restrictions on the CPS, where a hostile party may jam packets between the sensor and controller, thereby causing instability and a decline in system performance. We assume that energy constraints limit the attacker's ability to launch DoS attacks for a finite amount of time and frequency. We develop an effective method to determine an upper bound on the performance deterioration caused by the DoS assault, based on the linear matrix inequality approach. Additionally, we suggest redesigning the controller to reduce this performance drop. Lastly, a simulation example demonstrates how to construct a secure controller and calculate the performance deterioration under a bounded DoS attack. The results of the simulation demonstrate that the designed controller successfully defends the stability and performance of the feedback loop against threats.**

***Index Terms*—Denial-of-service attacks, secure control, linear quadratic cost, and performance degradation are all related to cyber-physical systems.**

I. INTRODUCTION

Computational, communication, and physical components are all included in cyber-physical systems. There are many advantages to this embodiment, such as improved mobility and interoperability. The tremendous progress that CPSs have made allows for a wider range of services and applications, such as smart homes, smart grids, supply chains, transportation, oil, and gas. On the other hand, because CPSs connect the physical and digital worlds, they are a prime target for attacks that aim to compromise their availability, confidentiality, and integrity. Malevolent actors often investigate CPS flaws and launch assaults that impair system functionality and can lead to an unstable feedback loop, such as in Supervisory Control and Data Acquisition Systems (SCADA). as well as power grids [3], [4]. Therefore, in order to facilitate the widespread adoption and deployment of CPSs, it is imperative to safeguard them against harmful activity. Cyber-attacks against CPSs fall into two primary groups [5]. First, denial-of-service (DoS) attacks are directed at stopping authorized network agents from interacting with one another. DoS attacks commonly target routing protocols and obstruct communication [6]. Deceptive attacks fall into the second type. In these assaults, the attacker seeks to alter the data or compromise specific cyber components by gaining the private key. Because they are unable to record physical behavior, security methods that solely rely on information technology security strategies are inadequate for securely managing CPSs. They ought to be enhanced by security control methods. Because these methods use attack models for control design, creating a secure controller is a significant task.

because of the unusual and erratic characteristics of assault models [9]. Researchers have recently focused a great deal of emphasis on the secure control design problem. A team of researchers achieved a robust control in the face of cyber-attacks by applying the game theoretic methods. Attack-tolerant control methods were demonstrated by a different group [14], [15]. In [16], [17], and [18], fault tolerant control was also used to construct robust control and estimation algorithms. Fault-tolerant control, however, falls short of providing secure control since attackers deliberately craft cyber-attacks to do harm to CPSs.Model predictive control strategies were employed by yet another set of researchers for the resilient control of CPSs [19], [20]. The majority of contemporary controllers are sampled-data based and implemented using discrete-time control methods as a result of advances in digital technology.

Sampled-data control, as opposed to continuous control, uses a sampler to discretize process measurements, which are then sent to the control node for the purpose of determining the control signal. In order to achieve maximum performance deterioration, scientists in this research direction investigated when to block the LQR controller's communication channel. A hybrid aperiodic sampling technique was examined in [23] to provide a stabilizing controller for networked systems vulnerable to stochastic false-data injection attacks. A CPS's performance under reset attacks was examined in [24]. An H∞ controller using the sampled-data technique is built in [25] for networked systems that are subjected to a mix of deception and DoS attacks. The total system was modelled as a feedback controller. To ensure the H∞ performance level of the resulting feedback loop, a criterion was constructed using the piecewise Lyapunov–Krasovsky functional. A robust control design challenge of an NCS under denial-of-service (DoS) assaults was presented in [26]. The feedback system was modeled as a non-uniformly sampled system by capturing the attack's timespan. Afterwards, a statefeeback controller was created to maintain closed loop stability. As far as the authors are aware, the stability analysis and control design challenge are the only aspects of the secure control of CPSs that have been addressed in previous research. There hasn't been much research done on the issue of determining how much a successful cyber-attack can impair a feedback loop's performance.

1.1 OBJECTIVE

Enhancing network security is the aim of this research. In order to accomplish this, we suggested the authorization and access control mechanism, which allows or prohibits access based on the capabilities and scope of the client's access. Our study's primary goal is to safeguard system resources from harm brought on by unauthorised access, intrusions, and harmful attacks.

1.2 SCOPE OF THE PROJECT

We introduced a concept of computer network security that primarily relies on security technology.

There are four different kinds of computer network concerns in the project.

Our network security shields it from intruders. In order to defend against the networks, we have incorporated four different kinds of attacks.

2. EXISTING SYSTEM

- ➢ Because of energy constraints, we assume that the attacker can launch DoS attacks only occasionally and for a limited amount of time. We develop an effective method to determine an upper bound on the performance deterioration caused by the DoS assault, based on the linear matrix inequality approach.
- ➢ Because they are unable to record physical behavior, security methods that solely rely on information technology security strategies are inadequate for securely managing CPSs. They ought to be enhanced by security control methods.

2.1 PROPOSED SYSTEM

- ➢ We also suggest redesigning the controller in order to reduce this decrease in performance. Lastly, a simulation example demonstrates how to construct a secure controller and calculate the performance deterioration under a bounded DoS attack.
- ➢ The results of the simulation demonstrate that the designed controller successfully defends the stability and performance of the feedback loop.
- ➢ To defend against a computer network, we have demonstrated four different sorts of attacks.

2.1.2 PROPOSED SYSTEM ADVANTAGE

- ➢ Identify unapproved users.
- ➢ Boosts privacy and security while offering flexibility.

3. GOAL OF PROJECT

This paper's objective is to solve this issue. We take into consideration a sampled-data state feedback control with a linear quadratic performance criterion and a linear time-invariant plant.

We first design a numerical approach to evaluate the performance degradation in the event of a finite-energy DoS assault in the feedback loop, assuming that the loop is already stable. Next, in order to minimise the performance deterioration caused by the DoS attack, we develop a controller design technique. The benefit of the suggested method is then demonstrated using an example of a pendulum on a cart system.

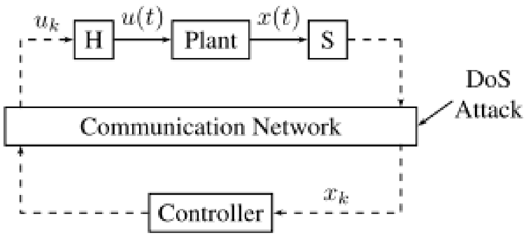


FIGURE 1. A cyber-physical system under denial-of-service attacks

It is important to note that the approach presented here can be extended to more complex classes of systems and other performance criteria, like H∞ performance, even though the procedures for performance analysis and control design are It is important to note that the approach presented here can be extended to more complex classes of systems and other performance criteria, like H∞ performance, even though the procedures for performance analysis and control design are developed for linear time-invariant systems and linear quadratic control. In this regard, it is anticipated that the findings in this work will spur additional investigation into how feedback loop performance degrades under various cyber-attacks.

4. METHODOLOGIES

1. User Interface Design

We create the project's windows in this module. All users can securely log in using these windows. Users can only connect to the server by providing their login and password in order to establish a connection. The user can log in straight to the server if they have previously left; otherwise, they must register their information, including their email address, password, and username. In order to maintain the upload and download rates, the server will create an account for each user. The user ID will be set to name. Typically, logging in allows access to a certain page.

2. Admin

He will be the administrator and have complete control over everything in this first module of the project. The admin may log in to this module. The administrator can upload data.Client data can be accessed by the admin. An administrator's data may be kept in the database. The administrator can see the client's requests. The administrator can produce a key.

3. Server

This project's second module is this one. The host server needs to log in to this module. Keys can be updated on the host server. Port information may be available on the server. Client queries are received by the host server. The host server may be home to unapproved clients. A key that is stored in the database can be modified by the server.

4. User

This project's third module is this one. The client must first register in this module before logging in. The user will upload data. The client can obtain the important answers. The client has the ability to download and search the data.

5. CLASSIFICATIONSOF ALGORITHMS

5.1 PROPOSED ALGORITHM

➢ Distributed Denial –of-Service Attack

In order to take control of the system and send spam and fictitious requests to other devices and servers, hackers infect computers with malicious software. When a DDoS assault occurs, the hundreds or thousands of fake traffic requests that are sent to the target server cause an overload. The server is being attacked from several angles; therefore it can be challenging to identify every address.

Another reason a server finds it difficult to survive a DDoS attack is that it may not be possible to distinguish between real and fraudulent traffic.

1. IP Snooping Attacks

An IP address can be protected by IP snooping attacks. The web application's IP address cannot be changed.

2. Port Attacks

The method used to find open ports and services on hosts within a network is called port scanning. Hackers can also use it to target victims, while security engineers can occasionally use it to scan machines for weaknesses. It can be used to track ports after sending connection requests to the intended machines. Network scanners do not physically damage computers; instead, they mimic human users' requests when they access websites or use programmer like Telnet and Remote Desktop Protocol (RDP) to connect to other computers. Sending ICMP echo-request packets with particular flags set in the packet headers to identify the kind of message being transmitted allows you to execute a port scan: Type 0 indicates that no response is expected from the answering host, but Type 8 indicates that the request is an echo-reply packet with the source IP address as the responding host.

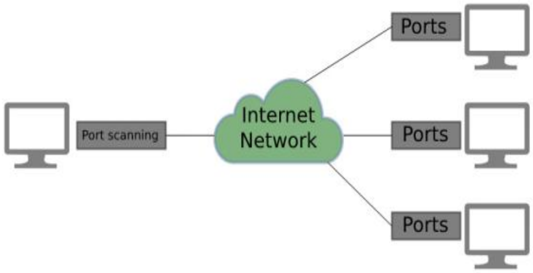


FIG 5.1 PROPOSED ALGORITHM

3. PC Snooping

The computer system. Every Internet-connected Personal Computer (PC) is a potential target for network security.

4. User’s Security

We can put in place security measures to prevent and address problems with data protection, such as protecting unauthorized users.

5.2 EXISTING ALGORITHM

- NETWORK COMMUNICATION AND DoS ATTACK

Sensors, controllers, and actuators are connected via a communication network. Allow network communication phenomena like packet dropout and delays to not happen in a real-time network. On the other hand, we presume that the communication network has been compromised by an attacker. It is possible for the attacker to prevent the sensor and controller from communicating. Assuming the attacker is stealthy and has limited energy, we can say that the attack's frequency and duration are limited

6. ARCHITECTURE OF MODEL

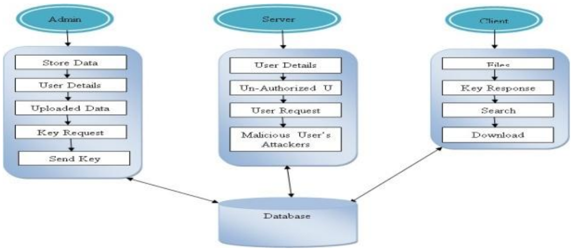


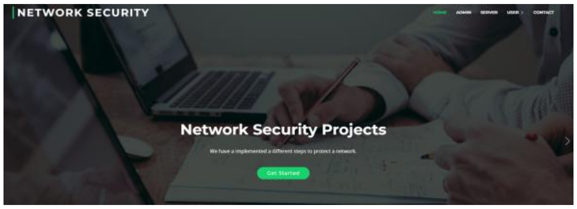
FIG 7 ARCHITECTURE MODEL

EXPLANATION

The project administrator can log in and control this. Database uploads are possible for the admin. All of the client data from the user data will be available to the administrator. Administrators will also have data saved in the database. The administrator may also get a request from a user. Admin will possess a different key. A host server login is possible. The user networks' keys can be updated by the host server. The data contains port information for the host server. The data contains port information for the host server. From the data, the host server can receive client requests.

An unauthorised client may access the data on the host server. Customers must log in and have a register. Customers will receive files.The database will provide a crucial response to clients. All the info will be searched by clients. All of the network security data will be downloaded by clients.

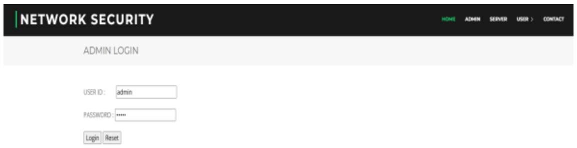
7. RESULTS



Network Security Projects

We have a implemented a different steps to protect a network.

FIG 7.2.1 INDEX PAGE



ADMIN LOGIN

USER ID : admin

PASSWORD : •••••

FIG 7.2.2 ADMIN LOGIN

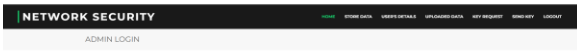
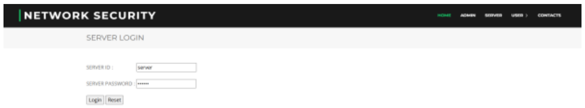


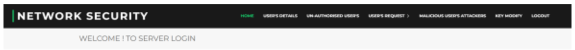
FIG 7.2.3 ADMIN HOMEPAGE



SERVER ID : server

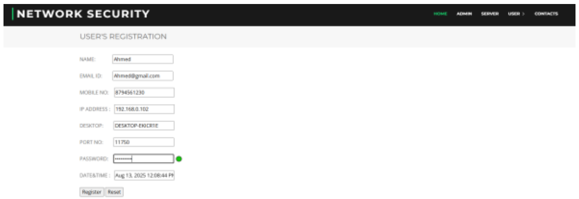
SERVER PASSWORD : ••••••

FIG 7.2.4 SERVER LOGIN



WELCOME ! TO SERVER LOGIN

FIG 7.2.5 SERVER HOMEPAGE



NAME: Ahmed

EMAIL ID: Ahmed@gmail.com

MOBILE NO: 8794561230

IP ADDRESS : 192.168.0.102

DESKTOP: DESKTOP-EKICR1E

PORT NO: 11750

PASSWORD: •••••••••

DATE&TIME : Aug 13, 2025 12:08:44 PM

FIG 7.2.6 USER REGISTRATION

8. FUTURE ENHANCEMENT

Hybrid systems are among the more intricate CPS models to which the suggested approach might be applied. Other kinds of control systems, such H∞ control, can also be taken into account.

9.CONCLUSION

We have introduced a methodical approach to assess the performance deterioration of cyber-physical systems, which are simulated by linear time-invariant plants and are vulnerable to deceptive denial-of-service assaults. The process takes the shape of a semi-definite programmer, which may be effectively solved with the aid of contemporary solvers. Additionally, we demonstrated how to create a safe controller that reduces the amount of performance degradation brought on by a denial-of-service attack. The usefulness of the proposed technique was proved using a simulated example of the benchmark inverted pendulum system.

REFERENCES

[1] A. Rahman, G. Mustafa, A. Q. Khan, M. Abid, and M. H. Durad, ‘‘Launch of denial-of-service attacks on the modbus/TCP protocol and development of its protection mechanisms,’’ Int. J. Crit. Infrastruct. Protection, vol. 39, Dec. 2022, Art. no. 100568.

[2] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, ‘‘Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks,’’ Appl. Soft Comput., vol. 71, pp. 66–77, Oct. 2018.

[3] C. Pu, P. Wu, and Y. Xia, ‘‘Vulnerability assessment of power grids against link-based attacks,’’ IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 67, no. 10, pp. 2209–2213, Oct. 2020.

[4] S. Lai, B. Chen, T. Li, and L. Yu, ‘‘Packet-based state feedback control under DoS attacks in cyber-physical systems,’’ IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 66, no. 8, pp. 1421–1425, Aug. 2019.

[5] Z.-H. Pang, L.-Z. Fan, H. Guo, Y. Shi, R. Chai, J. Sun, and G.-P. Liu, ‘‘Security of networked control systems subject to deception attacks: A survey,’’ Int. J. Syst. Sci., vol. 53, no. 16, pp. 3577–3598, Dec. 2022.

[6] X. Wang and G. Yang, ‘‘Cooperative attack strategy design via H/H∞ scheme for linear cyber-physical systems,’’ Int. J. Robust Nonlinear Control, vol. 30, no. 1, pp. 33–50, Jan. 2020.

[7] H. Sun, Y. Cui, L. Hou, and K. Shi, ‘‘Adaptive finite-time control for cyber-physical systems with injection and deception attacks,’’ Appl. Math. Comput., vol. 430, Oct. 2022, Art. no. 127316.

[8] N. He, K. Ma, and H. Li, ‘‘Resilient predictive control strategy of cyber–physical systems against FDI attack,’’ IET Control Theory Appl., vol. 16, no. 11, pp. 1098–1109, Jul. 2022.

[9] M. S. Mahmoud and Y. Xia, Cloud Control Systems: Analysis, Design and Estimation. New York, NY, USA: Academic, 2020.

[10] J. Sun, P. Li, and C. Wang, ‘‘Optimise transient control against DoS attacks on ESS by input

convex neural networks in a game,'' Sustain. Energy, Grids Netw., vol. 28, Dec. 2021, Art. no. 100535.

[11] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, ''Resilient control of networked control system under DoS attacks: A unified game approach,'' IEEE Trans. Ind. Informat., vol. 12, no. 5, pp. 1786–1794, Oct. 2016.

[12] R. Meira-Góes, E. Kang, R. H. Kwong, and S. Lafortune, ''Synthesis of sensor deception attacks at the supervisory layer of cyber–physical systems,'' Automatica, vol. 121, Nov. 2020, Art. no. 109172.

[13] L. Xue, B. Ma, J. Liu, and Y. Yu, ''Jamming attack against remote state estimation over multiple wireless channels: A reinforcement learning based game theoretical approach,'' ISA Trans., vol. 130, pp. 1–9, Nov. 2022.

[14] S. Bezzaoucha Rebaï, H. Voos, and M. Darouach, ''Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems,'' Eur. J. Control, vol. 47, pp. 30–36, May 2019.

[15] J.-W. Zhu, Y.-P. Yang, W.-A. Zhang, L. Yu, and X. Wang, ''Cooperative attack tolerant tracking control for multi-agent system with a resilient switching scheme,'' Neurocomputing, vol. 409, pp. 372–380, Oct. 2020. nonlinear networked control system with actuator failures and DoS jamming attacks,'' J. Franklin Inst., vol. 357, no. 14, pp. 9288–9307, Sep. 2020.

[16] M.-Y. Su and W.-W. Che, ''Fault-tolerant control for model-free networked control systems under DoS attacks,'' J. Franklin Inst., vol. 358, no. 17, pp. 9023–9033, Nov. 2021.

[17] Q. Sun, K. Zhang, and Y. Shi, ''Resilient model predictive control of cyber–physical systems under DoS attacks,'' IEEE Trans. Ind. Informat., vol. 16, no. 7, pp. 4920–4927, Jul. 2020.

[18] B. Zhang and Y. Song, ''Asynchronous constrained resilient robust model predictive control for Markovian jump systems,'' IEEE Trans. Ind. Informat., vol. 16, no. 11, pp. 7025–7034, Nov. 2020.

[19] J. Skaf and S. Boyd, ''Analysis and synthesis of state-feedback controllers with timing jitter,'' IEEE Trans. Autom. Control, vol. 54, no. 3, pp. 652–657, Mar. 2009.

[20] J. Zhou, J. Shang, Y. Li, and T. Chen, ''Optimal DoS attack against LQR control channels,'' IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 68, no. 4, pp. 1348–1352, Apr. 2021. [23] K. Bansal and P. Mukhija, ''Aperiodic sampled-data control of distributed networked control systems under stochastic cyber-attacks,'' IEEE/CAA J. Autom. Sinica, vol. 7, no. 4, pp. 1064–1073, Jul. 2020.

[21] Y. Ni, Z. Guo, Y. Mo, and L. Shi, ''On the performance analysis of reset attack in cyber-physical systems,'' IEEE Trans. Autom. Control, vol. 65, no. 1, pp. 419–425, Jan. 2020.

[22] P. Zeng, F. Deng, X. Gao, and X. Liu, ''Sampled-data resilient H∞ control for networked stochastic systems subject to multiple attacks,'' Appl. Math. Comput., vol. 405, Sep. 2021, Art. no. 126265.