ACTIVE SECURITY CONTROL APPROACH AGAINST DOS ATTACKS IN CYBER-PHYSICAL SYSTEMS

Hamza Ghulam Nabi

ABSTRACT

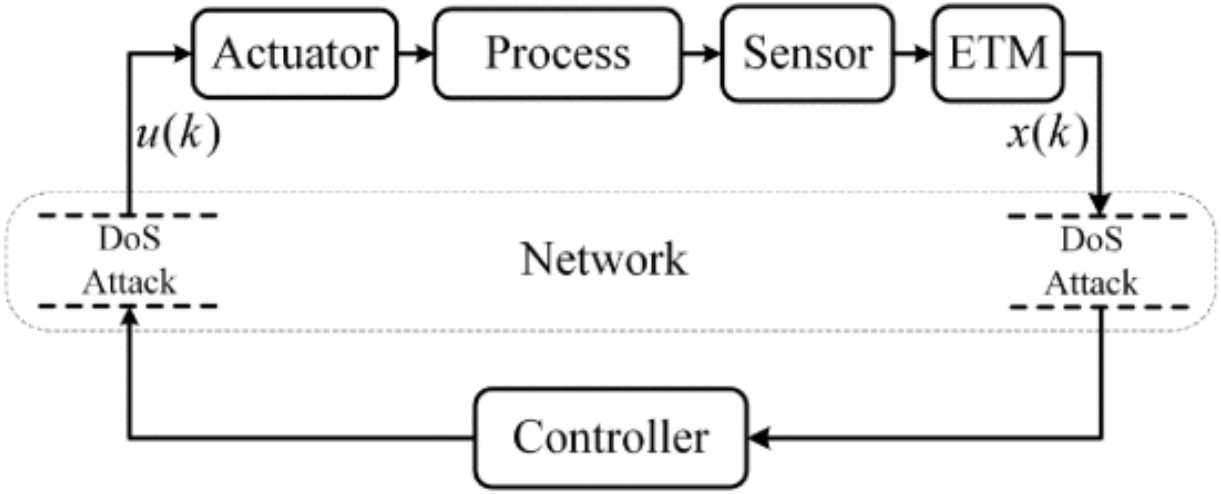
- An **active security control approach** is developed for cyber-physical systems (CPSs) under denial-of-service (DoS) attacks.
- DoS attacks are considered in both the sensor-to-controller (S–C) channel and the controller-to-actuator (C–A) channel.
- The number of maximum continuous DoS attacks is assumed to be bounded due to cost constraints.
- An active security control strategy is designed to defend against two-channel DoS attacks and update control inputs timely.
- A security controller that contains both current and future control inputs is designed. • The proposed active security control approach ensures asymptotic stability without losing control performance.
- Simulations and experiments are provided to demonstrate the effectiveness of the approach.

INTRODUCTION

- Cyber-physical systems (CPSs) are used in various engineering fields, but their use of communication networks makes them vulnerable to malicious attacks, such as denial-of-Service (DoS) attacks.
- DoS attacks are the most financially expensive security incidents and can cause environmental damage in critical industrial control processes.
- There are three approaches to the secure control problem for CPSs under DoS attacks: **stochastic system, game theory, and resilient control**.
- Existing approaches assume that DoS attacks occur only in the controller-to-actuator (C-A) channel or sensor-to-controller (SC) channel or both synchronously.
- The general scenario where DoS attacks exist in two channels asynchronously is more difficult to address.

INTRODUCTION (2)

- A novel security control approach is developed based on the event-triggered idea and predictive control theory to actively defend the DoS attacks and ensure that the addressed CPS under two-channel DoS attacks is asymptotically stable without losing the control performance.
- The approach consists of an active security control strategy that makes full use of the unattacked intervals and a security controller that contains both the current and future control inputs.



Schematic diagram of the CPS under the two-channel DoS attacks. ETM is the event-triggered mechanism.

INTRODUCTION (3)

❑Main Contribution

1. To actively defend the two-channel DoS attacks, an active security control strategy that makes full use of the unattacked intervals is designed to ensure that there are appropriate control inputs to be updated in each period. And the closed-loop system resulted by the active security control strategy is equivalent to the case without DoS attacks.

2. A security controller that contains both the current and future control inputs is designed by predictive control theory. Combined with the active security control strategy and the security controller, the active security control approach is developed in this article, which can ensure that the addressed CPS under two-channel DoS attacks is asymptotically stable without losing the control performance. Finally, both the simulations and experiments are given to demonstrate the effectiveness of the proposed methods.

PROBLEM FORMULATION

- The article considers a Cyber-Physical System (CPS) structure for power systems, smart grid infrastructures, and building automation systems.
- The system model (1) is widely adopted for describing system dynamics and is subject to actuator saturation problems.
- The article considers a **more general case** where DoS attacks can occur independently in the S-C and C-A channels, simultaneously or separately, with bounded maximum continuous DoS attacks in both channels.
- *Problem to be solved in this manner:* The article aims to develop an active security control strategy that makes full use of the unattacked intervals to ensure that the control inputs are updated timely and a security controller that contains both the current and future control inputs.

PROBLEM FORMULATION (2)

Remark 1

- The scenario considered in this article makes it more difficult to update the control signals successfully under the same attack frequency. For example, if the attack frequency is 50% in each channel and the DoS attacks in two channels are asynchronous, the control signals cannot be updated successfully at all time. To overcome this difficulty, an event-based security transmission policy will be designed to ensure that the measurement and control signals are successfully updated.

Remark 2

- The developed approach in this article only requires that the number of the maximum continuous DoS attacks is bounded, which is easily satisfied in practical applications. The resilient control approach requires the frequency and duration of DoS attacks to be known, while the developed approach only requires the number of the maximum continuous DoS attacks.

ACTIVE SECURITY CONTROL APPROACH

A. Event Based Security Transmission Policy

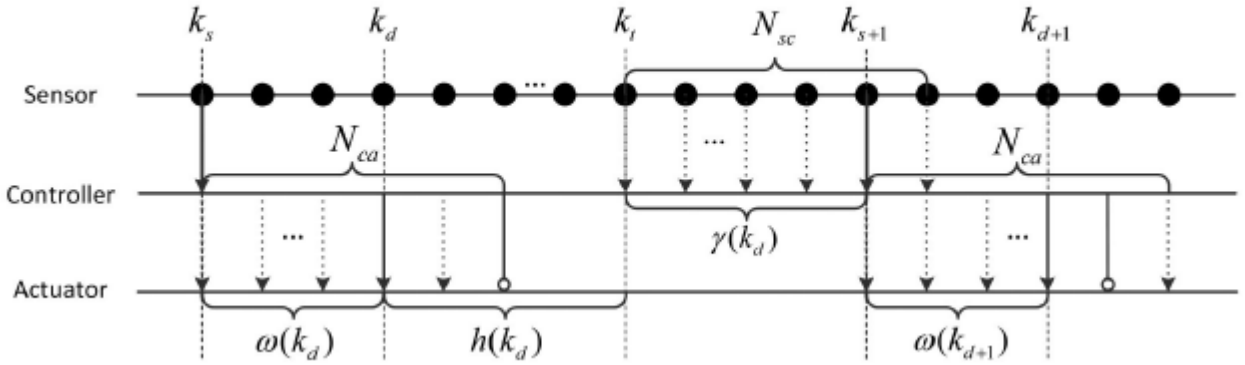
- A proposed event-based security transmission policy to defend against two-channel DoS attacks.
- The policy considers an event-triggered condition to determine the event-triggered time (kt).

$$k_t = \begin{cases} \min\{k \mid \|x(k) - x(k_d)\| > \varepsilon \|x(k)\|\}, & k < k_d + H \\ k_d + H, & k = k_d + H \end{cases} \quad (3)$$

- For a maximum continuous DoS attack scenario (Nsc), the sensor sends measurement signals to the controller Nsc+1 times continuously from kt to kt+Nsc.
- From time ks to ks+Nca, the controller sends control signals to the actuator Nca+1 times continuously to ensure the actuator successfully receives the signal at least once.

ACTIVE SECURITY CONTROL APPROACH (2)

- The worst-case scenario is when the actuator doesn't receive control inputs for N-1 periods due to the two-channel DoS attacks.
- The event-based security transmission policy ensures successful updating of measurement and control signals, which is crucial for closed-loop feedback control under two-channel DoS attacks.



Timing diagram of the CPSs with the active security control strategy. *The → indicates that the data is sent successfully, the indicates that the data is sent failed, and the represents the active packet loss.*

ACTIVE SECURITY CONTROL APPROACH (3)

- Summary

1. At time *kd*, the sensor executes event-triggered condition (3) to determine the event-triggered time *kt*.
2. From the time *kt* to *kt* + *Nsc*, the sensor sends the measurement signal to the controller *Nsc* + 1 times continuously.
3. When the controller receive the measurement signal at time *ks*+1, from time *ks*+1 to *ks*+1 + *Nca*, the controller calculates the control signals and sends it to the actuator.

ACTIVE SECURITY CONTROL APPROACH (3)

B. Security Controller Structure

- The article proposes an active security control approach for cyber-physical systems (CPSs) to defend against denial-of-service (DoS) attacks.
- The existing methods implement a sample-and-hold control strategy or zero-input control strategy, but the proposed approach uses a security controller that contains both current and future control inputs.
- The controller calculates NC control inputs at time kd and sends them to the actuator using one data packet, which helps to update the control signal timely.

ACTIVE SECURITY CONTROL APPROACH (4)

- The active security control strategy uses a state feedback controller that predicts the state at a future time kd + i.

$$u(k_d+i) = Kx(k_d+i\,|k_d) \\ = K(A+BK)^i x(k_d), i=0,1,\ldots,N_C-1 \quad (4)$$

- The proposed approach is summarized in **Algorithm 1**, which shows that the consumption of network resources will not increase if all the control signals in Uω(kd)(kd) can be packed into one data packet.
- The proposed approach does not require an acknowledge signal back to the sensor via the network to confirm the success of the transmission.
- Theorem 1 states that if the number of control inputs NC in Uω(kd)(kd) is not less than N, the active security control strategy in Algorithm 1 can defend against DoS attacks.

ACTIVE SECURITY CONTROL APPROACH (5)

Algorithm 1

- Step 1: When the actuator receives the control sequence $U\omega(kd)(kd)$ at time kd, the actuator executes the control inputs $u\omega(kd)(kd), \ldots, u\omega(kd)(kd + i), \ldots, u\omega(kd)(kd + NC - 1)$ successively, while the sensor executes event-triggered condition (3) to determine the event-triggered time kt.
- Step 2: At time kt, the sensor sends the state vector to the controller Nsc + 1 times continuously from kt to kt + Nsc.
- Step 3: After the controller receives the state x(ks+1) at time ks+1, the controller constructs the control sequence $U\omega(kd+1)(kd+1)$ based on the $x(ks+1 + \omega(kd+1)|ks+1)$ and then sends it to the actuator Nca + 1 times continuously from ks+1 to ks+1 + Nca. When the actuator receives the control sequence $U\omega(kd+1)(kd+1)$, let kd → kd+1 and ks → ks+1.
- Return to the Step 1.

ACTIVE SECURITY CONTROL APPROACH (6)

Theorem 1

- If the number of control inputs NC in Uω(kd)(kd) is not less than N, i. e. , NC ≥ N, the active security control strategy in Algorithm 1 can guarantee that the control inputs are updated timely in each period under the two-channel DoS attacks, where N = H + Nsc + Nca.

STABILITY ANALYSIS AND CONTROLLER DESIGN

- The article presents a method for designing a stable controller for Cyber-Physical Systems (CPSs).
- The predictive control theory is used to design the controller, which should ensure that the control inputs are updated in each period and satisfy the desired asymptotically stability criteria while also satisfying the input constraint.
- The article discusses the objective function and the control invariant ellipsoid of the system. The Lyapunov function is also considered to ensure the system is asymptotically stable.
- The article also discusses the use of the Schur complement lemma to convert inequality, and the predictive control idea is used to introduce an additional term to reduce online computation and improve control performance.
- Finally, the closed-loop system is presented, and the equation for $z(kd+1)$ is defined.

STABILITY ANALYSIS AND CONTROLLER DESIGN

Algorithm 2

Offline design:

- Step 1: Solve the LMIs (21) and (25) offline, and obtain the feedback control law K.
- Step 2: For this control law K, solve the following optimization problem to maximize the volume of Exz.

$$\min_{Q_z} \log\det(TQ_zT^{\mathrm{T}})^{-1}$$
$$\text{s.t.} \quad (35) \text{ and } (36) \qquad (38)$$

Online synthesis:

- At time kd, the controller solves the following online optimization problem to obtain the f(kd).

$$\min_{f(k_d)} f^{\mathrm{T}}(k_d)f(k_d)$$
$$\text{s.t.} \quad z^{\mathrm{T}}(k_d)Q_z^{-1}z(k_d) \leq 1 \qquad (39)$$

- Then, the controller calculates the control inputs (26) and further constructs the control sequence $U\omega(kd)(kd)$.

STABILITY ANALYSIS AND CONTROLLER DESIGN

Theorem 2

By applying Algorithm 2 and the active security control strategy in Algorithm 1, the closed-loop system (12) under the two channel DoS attacks is asymptotically stable without losing the control performance, and the control inputs satisfy the constraints (2).

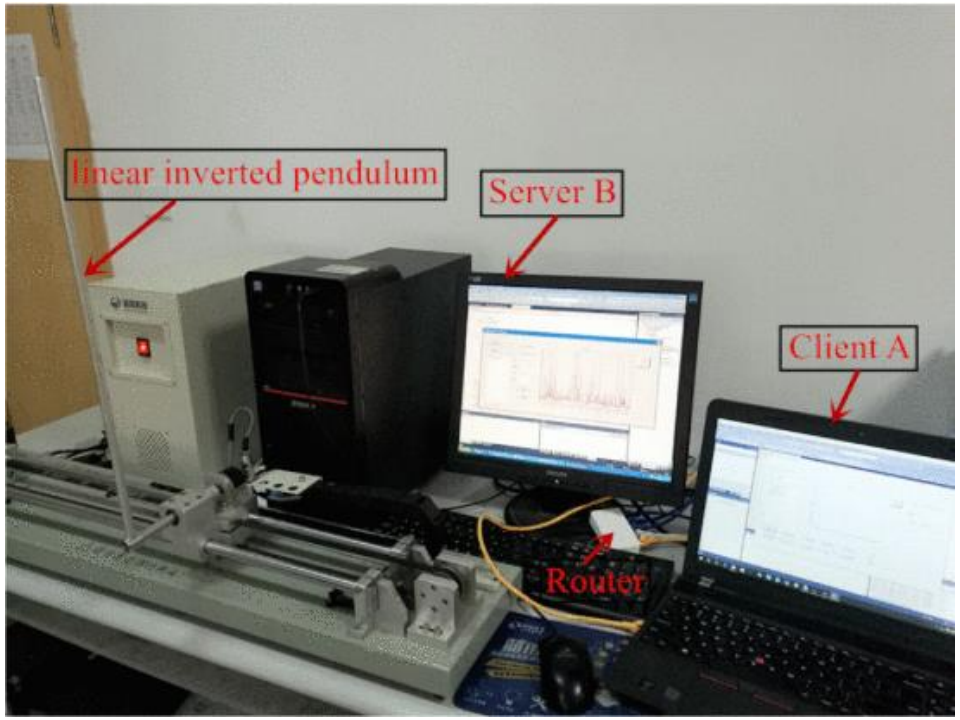
SIMULATION

- The effectiveness of proposed methods is shown through simulations and experiments of a networked inverted pendulum control system.
- The system uses data packets transmitted over communication networks using UDP.
- The system's state-space model is obtained using the Newton-Euler method.
- The control input is subjected to a constraint of -18m/s2 ≤ u ≤ 18m/s2.
- The proposed active security control approach can guarantee the asymptotically stability of the system without losing control performance.
- The control inputs satisfy the constraint (42).

$$-18\,\mathrm{m/s^2} \leq u \leq 18\,\mathrm{m/s^2} \qquad (42)$$

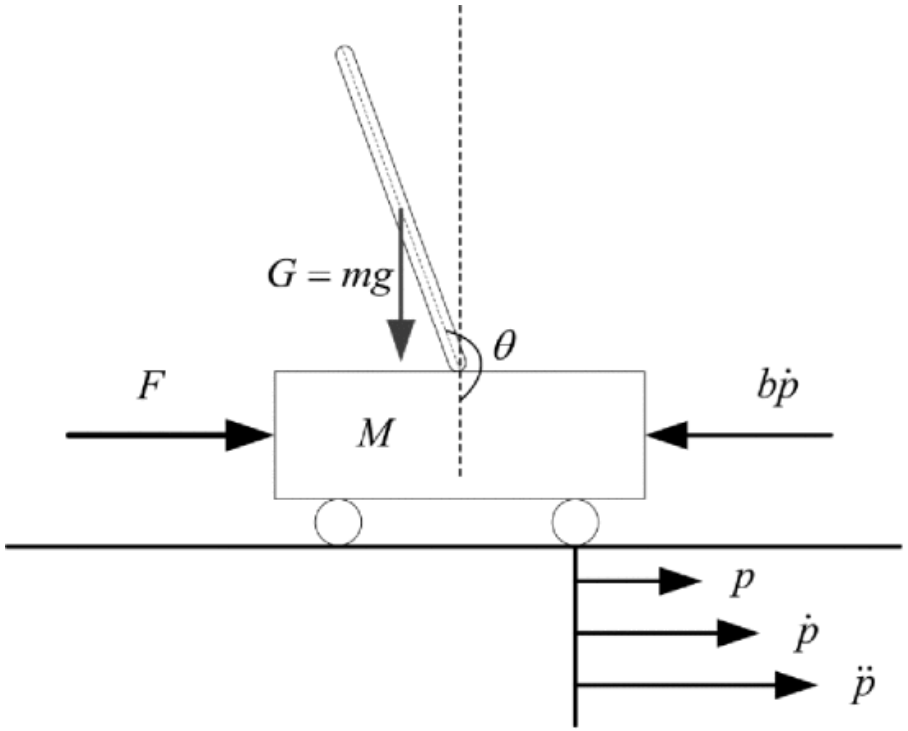
SIMULATION (2)

- The active security control strategy can ensure that the control inputs are updated timely in each period.
- The active security control approach can achieve the same control performance as no DoS attacks.



SIMULATION (3)

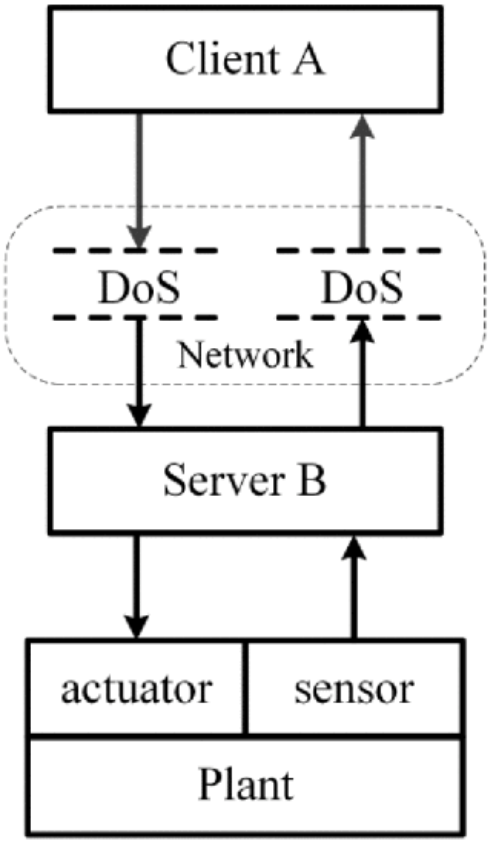
- An inverted pendulum system is a classic example used in control theory and engineering. It is a simple mechanical system consisting of a pendulum mounted on a cart that can move along a horizontal surface.
- The pendulum is unstable in the upright position, and the objective of the control system is to keep the pendulum balanced in this position using feedback control.
- This system is commonly used to illustrate the principles of control engineering, and it has many applications in areas such as robotics, transportation, and aerospace.



Inverted pendulum system.

SIMULATION (3)

- **Client A:** This is the client side of the control system, where the control algorithm is implemented. It sends control signals to the server for processing.
- **Network:** This is the communication network that connects the client and server. It enables the transmission of control signals and feedback signals between the two devices.
- **Server B:** This is the server side of the control system, where the control signals are received, processed, and sent to the plant. It also receives feedback signals from the plant and sends them back to the client.
- **Plant:** This represents the physical system being controlled, which is the inverted pendulum in this case. It consists of an actuator and sensor. The actuator receives control signals from the server and applies them to the pendulum, while the sensor measures the state of the pendulum and sends feedback signals back to the server. The server then uses the feedback signals to adjust the control signals and maintain the stability of the system.



Structure diagram of the networked inverted pendulum control system.

EXPERIMENTS

Case 1

- Same parameters and network environment as in simulations.
- Active security control approach proposed in this article applied in experiments.
- Experiment results shown in Figs. 8 and 9.
- Fig. 8 shows networked inverted pendulum control system is stable and control inputs satisfy constraint (42).
- Fig. 9 shows feedback control timing diagram of first 50 periods under two-channel DoS attacks in experiment.

EXPERIMENTS (2)

- Control sequence $U\omega(kd)(kd)$ containing both current and future control inputs updated 10 times successfully during first 50 periods.
- Control inputs $u\omega(kd)(kd)$, $u\omega(kd)(kd + 1)$, ..., $u\omega(kd)(kd + j - 1)$ implemented successively in case of $kd+1 = kd + j$, ($j \in \{1, 2, ..., 9\}$).
- Active security control strategy ensures appropriate control inputs are updated in each period under two-channel DoS attacks in real system.
- Figs. 8 and 9 show active security control approach proposed in this article is effective in real system.

EXPERIMENTS (3)

Comparative Experiments

- This section presents a comparative experiment to verify the effectiveness of the active security control approach proposed in the article.
- The comparative experiment considers a "sample-and-hold control" strategy where the controller calculates a single control input and sends it to the actuator.
- The experiment results show that the sample-and-hold control strategy reduces control performance, leading to unstable behavior of the inverted pendulum.
- The active security control approach proposed in the article is found to be superior to the sample-and-hold control strategy in terms of stability and control performance.

CONCLUSION

- An active security control approach has been proposed for CPSs under the two-channel DoS attacks.
- The active security control strategy in Algorithm 1 has been developed to defend against the two-channel DoS attacks.
- The proposed approach ensures that appropriate control inputs are updated in each period to ensure control performance.
- Theorems 1 and 2 guarantee that the active security control approach is equivalent to the case without DoS attacks and ensures asymptotic stability without losing control performance.

CONCLUSION (2)

- Simulations and experiments were conducted to show the effectiveness of the proposed active security control approach.
- Future works include designing the active security control method for nonlinear CPSs with noise and active countermeasures against deception attacks.

OPINION

- The paper proposes an active security control approach to defend against Denial of Service (DoS) attacks in Cyber-Physical Systems (CPSs) with an inverted pendulum control system as a case study. The proposed approach uses a security controller to generate appropriate control inputs that can be updated in each period to ensure the stability of the control system. The paper provides theoretical proofs and simulation and experimental results to show the effectiveness of the proposed approach in ensuring control performance while defending against DoS attacks.
- Overall, the paper appears to present a well-structured and well-researched approach to address an important security concern in CPSs. The authors provide a comprehensive discussion of related work, and the proposed approach is supported by solid theoretical proofs and experimental results.