electronics

Article

Resilient Integrated Control for AIOT Systems under DoS Attacks and Packet Loss [†]

Xiaoya Cao [1,2], Wenting Wang [3,4], Zhenya Chen [1,2,*], Xin Wang [1,2] and Ming Yang [1,2]

[1] Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan 250014, China; xiaoyacao1@gmail.com (X.C.); xinwang@qlu.edu.cn (X.W.); yangm@sdas.org (M.Y.)
[2] Shandong Provincial Key Laboratory of Computer Networks, Shandong Fundamental Research Center for Computer Science, Jinan 250014, China
[3] College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China; wangwenting@yjy.sd.sgcc.com.cn
[4] State Grid Shandong Electric Power Research Institute, Jinan 250003, China
[*] Correspondence: chenzhy@qlu.edu.cn

[†] This paper presents an extended version of our previous conference paper published in 2023 International Conference on Artificial Intelligence of Things and Systems (AIoTSys), Xi'an, China, 19–22 October 2023; pp. 18–21.

Abstract: This paper addresses bandwidth limitations resulting from Denial-of-Service (DoS) attacks on Artificial Intelligence of Things (AIOT) systems, with a specific focus on adverse network conditions. First, to mitigate the impact of DoS attacks on system bandwidth, a novel model predictive control combined with a dynamic time-varying quantization interval adjustment technique is designed for the encoder–decoder architecture of AIOT systems. Second, the network state is modeled to represent a Markov chain under suboptimal network conditions. Furthermore, to guarantee the stability of AIOT systems under random packet loss, a Kalman filter algorithm is applied to precisely estimate the system state. By leveraging the Lyapunov stability theory, the maximum tolerable probability of random packet loss is determined, thereby enhancing the system's resilient operation. Simulation results validate the effectiveness of the proposed method in dealing with DoS attacks and adverse network conditions.

Keywords: AIOT systems; DoS attacks; bandwidth limitation; packet loss; Lyapunov stability

check for updates

Citation: Cao, X.; Wang, W.; Chen, Z., Wang, X., Yang, M., Wu, C and Liu, R. Resilient Integrated Control for AIOT Systems under DoS Attacks and Packet Loss. *Electronics* **2024**, *13*, 1737. https://doi.org/10.3390/electronics13091737

Academic Editor: Franco Cicirelli

Received: 8 March 2024
Revised: 18 April 2024
Accepted: 19 April 2024
Published: 1 May 2024

1. Introduction

In recent years, the rapid convergence of Internet of Things (IoT) and Artificial Intelligence (AI) technologies has given rise to a promising and nascent technological domain recognized as AIOT [1,2]. AIOT amalgamates AI algorithms across the strata of perception, networking, and application layers, thus enabling intelligent cooperation in the realms of sensing, connectivity, computation, and control [3]. This innovation has catalyzed groundbreaking advancements and ushered in developmental prospects across multifarious domains, encompassing but not limited to intelligent healthcare, advanced manufacturing, and autonomous vehicular systems, among others [4]. In the course of this technological transformation, AIOT is anticipated to permeate diverse facets of society, imparting profound influences on human existence and a myriad of industries.

However, akin to other emerging technologies, the rapid advancement of AIOT systems has presented a myriad of distinctive challenges. These challenges mainly involve the inherent security vulnerabilities within AIOT systems and the continually evolving landscape of network threats. Due to the incorporation of complex functionalities related to perception, control, and execution, AIOT systems exhibit significant differences compared to traditional network systems. This complexity heightens the difficulty of ensuring security, particularly in the context of addressing security threats such as DoS attacks, making the issue increasingly prominent and urgent [5,6].

In the realm of AIOT, adversaries frequently deploy malicious network traffic to overwhelm systems, aiming to deplete system resources [7]. This deliberate resource consumption can lead to network bandwidth saturation, triggering service interruptions and even causing the entire system to collapse in extreme cases. In situations of poor network conditions, malicious actors may intentionally orchestrate network congestion, induce packet losses, and introduce transmission delays [8,9]. These behaviors profoundly disrupt the internal exchange of status data and transmission of control commands within the AIOT infrastructure. Due to the decreased availability of services and the presence of potential threats, system performance may severely degrade, or even collapse entirely.

In the face of continually evolving security threats in AIOT systems, researchers have devoted significant efforts to developing various defense mechanisms. In response to the issue of DoS attacks in AIOT, notable research contributions have been made. The author meticulously establishes thresholds for attack frequency and duration, utilizing state feedback control to uphold system stability [10]. Within this framework, the researcher introduces an elastic controller, employing model establishment and a hybrid system stability analysis approach. An adaptive gain-based control scheme is integrated to effectively mitigate the impact of DoS attacks [11]. Moreover, the study delves into a collaborative elastic control methodology, systematically addressing communication delays and countering the adverse effects of DoS attacks by introducing dynamic, time-varying sampling periods and enhanced communication mechanisms [12]. Additionally, the author adeptly mitigates the influence of periodic DoS attacks on the observability of Networked Control Systems (NCSs) by considering matrix eigenvalues and delineating sufficient conditions for DoS attacks [13]. In continuation, an edge-triggered distributed control framework is introduced, contributing to the overall maintenance of system stability. In the aforementioned design, the system attains asymptotic stability in the presence of disturbances and noise [14]. However, under DoS attacks and constrained network bandwidth, the signal deviation induced by quantization introduces inaccuracies in the prediction process, which are ignored by the aforementioned works.

The bandwidth limitation caused by DoS attacks on AIOT systems is evident, and when these systems encounter adverse network conditions such as network congestion, routing issues, or transmission errors, random packet loss phenomena will also arise accordingly.

To deal with the packet loss problem, the author explores network-based modeling and proportional-integral (PI) control for continuous-time direct-drive-wheel systems in wireless network environments, addressing challenges posed by stochastic packet dropouts in system design [15]. The concept of the “overall packet loss rate” is introduced, offering a comprehensive assessment of the combined impact of malicious attacks and inherent packet loss [16]. This enriches the comprehension of network security and performance dynamics. Additionally, the author investigated the event-triggered synchronization problem of master–slave neural networks. In doing so, they employed static output feedback and designed suitable output feedback controllers using the Lyapunov–Krasovskii functional method [17]. Subsequently, the author introduces an innovative dynamic quantization scheme and formulates a Lyapunov function type tailored for systems influenced by quantization and packet loss. This framework facilitates the in-depth analysis of gain performance [18]. Following this, the author presents a bounded real condition contingent on the upper limit of network-induced delays and the maximum consecutive malicious packet losses. This enables the simultaneous examination of their collective impact on system performance [19]. Furthermore, the author shifts focus to the stability of discrete-time networked control systems, placing specific emphasis on delays induced by the network and malicious packet loss, and establishes corresponding stability criteria [20]. While the aforementioned approaches offer valuable theoretical foundations, further validation and an adaptability investigation are required to address the challenges of real-time responsiveness in dealing with dynamic and unpredictable random data packet loss in AIOT systems.

This paper aims to devise a pioneering control scheme to tackle the inaccuracies stemming from signal deviation induced by quantization during the prediction process, while also effectively managing the dynamic and unpredictable random data packet loss in AIOT systems. The contributions of our work can be summarized as follows:

- Firstly, we have introduced a model predictive control method based on uniform quantization within the encoder and decoder components. This method aims to alleviate bandwidth limitations during data transmission, especially in the presence of DoS attacks. The approach enhances the reliability of data transmission within AIOT systems.
- Secondly, to address the discrepancy between predicted values and actual values, this paper delves into the application of dynamic system design to enhance the security defenses of AIOT. This approach not only improves system robustness but also reinforces the system's resistance to interference.
- Finally, to tackle the challenge of random packet loss in adverse network conditions, this study employs a Markov chain model to characterize packet loss rates across diverse network scenarios. Additionally, it utilizes the Kalman filter algorithm technique for predicting system states, thereby mitigating the adverse effects of random packet loss. Through a rigorous analysis grounded in Lyapunov stability theory, this paper elucidates a quantitative relationship between random packet loss rates and overall system stability. This, in turn, provides a robust theoretical framework ensuring the sustained stability of system operations.

The paper's structure is outlined as follows: Section 3 introduces the research framework covering system description, predictive techniques, secure quantization, and dynamic system design. Section 4 rigorously validates and assesses the impact of quantization methodologies on system stability through comprehensive analyses and experiments. Section 5 involves experimental simulations, and Section 6 concludes the paper, summarizing findings and suggesting future research directions.

2. Problem Formulation

2.1. Research Questions

In the context of AIOT systems, the emergence of challenges related to network attacks and data packet losses poses new obstacles to the reliability and robustness of control systems. This paper aims to address the following questions:

- How is a resilient control strategy that mitigates DoS attacks and data packet losses designed?
- How are sensor data within the control system effectively encoded and decoded to accurately reflect system states and ensure control performance?
- How are predictive models and data loss scenarios utilized to adjust controllers, ensuring system stability and performance?

2.2. System Description

The state-space representation is as follows:

$$\dot{\eta}(t) = \tilde{A}\eta(t) + \tilde{B}u(t) \tag{1}$$

where $\tilde{A} = SAS^{-1}$, where $A \in \mathbb{R}^{n_x \times n_x}$ is a block diagonal matrix, $\tilde{B} = SB$, $\tilde{K} = KS^{-1}$, K represents the control gain matrix, and $S \in \mathbb{R}^{n_x \times n_x}$ is a transformation matrix. For clarity, we assume the system matrix has a single eigenvalue as follows:

$$\tilde{A} = \begin{bmatrix} D & I & & \\ & D & I & \\ & & \ddots & I \\ & & & D \end{bmatrix}^{n \times n} \tag{2}$$

$$D = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{3}$$

In addition, we define the initial values of $\hat{\eta}(t)$, $\hat{\eta}(0^-) = 0$. The synchronization of all signals in the encoding and decoding systems is achieved through identical structures, initial conditions, and acknowledgments. As depicted in Figure 1, the system comprises six fundamental components: the sensor, encoder, communication channel, decoder, controller, and actuator. The sensor plays a pivotal role in capturing the system's current state, while the encoder performs intricate tasks such as coordinate transformations, quantization, and predictive encoding. The resulting encoded digital signal is transmitted through a network channel susceptible to potential DoS attacks.

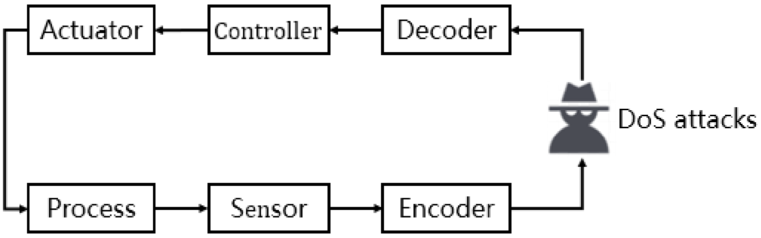

Figure 1. Control architecture of AIOT systems with DoS attacks.

Upon successful transmission, the decoder meticulously deciphers the received data and utilizes the capabilities of a predictive model to forecast the system's imminent state, adjusting the quantization intervals [21]. In the event of transmission failure, the decoder carefully distinguishes between data loss caused by the current network conditions and transmission failure caused by a DoS attack, employing different methods to predict the system's state based on specific circumstances. The decoder transmits these predictive state updates to the controller [22].

Drawing upon this predictive information, the controller formulates robust feedback control signals. These refined control signals are subsequently sent to the actuator, which assumes the ultimate responsibility for effecting changes in the system's state. Through this orchestrated process that incorporates prediction, adept handling of transmission failures, precise controller design, and discerning actuator operation, the system evolves into a steadfast control infrastructure proficient at mitigating the disruptive impact of network anomalies [23].

As the data acquired by the sensor, referred to as $\eta(t)$, inherently represents a model signal, it necessitates a coordinate transformation before it can be utilized as a data signal within our control system. Consequently, a coordinate transformation is implemented on the sensor-collected data, resulting in

$$\bar{\eta}(t) = S\eta(t) \tag{4}$$

S represents the state transition matrix.

The following (Figure 2) is the system framework diagram we have designed.

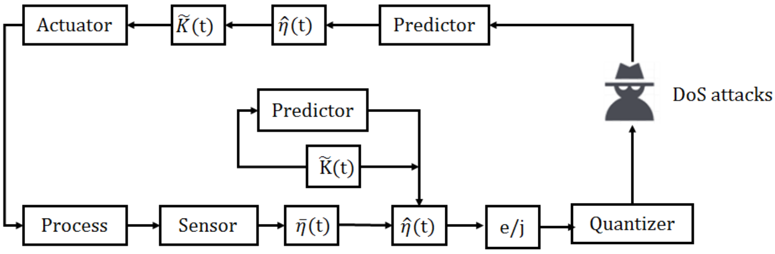

Figure 2. Control System

3. The Proposed Method

3.1. Model-Based Prediction of the Encoder and Decoder

Within our encoding system, depicted in Figure 3, a stable dynamic system with state $J(t)$, where $J(t) = [j_1(t), j_2(t), \cdots, j_{n_s}(t)]^{\mathrm{T}}$, enables the dynamic adjustment of $e(t)$ to minimize it as much as possible, ideally reducing it to 0, and predictive functionalities have been integrated into both the encoder and decoder. This integration enables the system to forecast the state vector for the subsequent time step, leveraging the quantized state data received at the current time point, denoted as t. The prediction of $\eta(t)$ at time t is denoted as $\hat{\eta}(t)$. The dynamics of this predictive system can be expressed using the following equation:

$$\begin{cases} \dot{\hat{\eta}}(t) = \widetilde{A}\hat{\eta}(t) + \widetilde{B}u(t), & t \neq t_s \\ \hat{\eta}(t) = \hat{\eta}(t^-) - \Delta(t^-), & t = t_s \\ u(t) = \widetilde{K}(t)\hat{\eta}(t) \end{cases} \tag{5}$$

During network transmission, DoS attacks may result in signal interruptions, followed by deteriorating network conditions, potentially leading to packet loss [24,25]. To address this issue, predictors in both the encoder and decoder infer missing signals based on previously received data. In our decoding system, as depicted in Figure 4, it distinguishes between bandwidth constraints caused by DoS attacks and packet loss due to poor network conditions. For failures caused by bandwidth limitations, the decoder relies on previous state data to predict signals. For packet loss due to poor network conditions, the Kalman filter algorithm is utilized to predict the system's state. Subsequently, the controller utilizes these predicted signals to mitigate the impact of DoS attacks on control performance and maintain system stability.

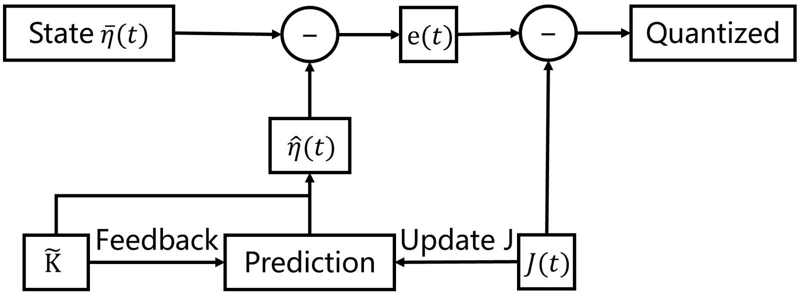

Figure 3. Model-based prediction of the encoder.

Furthermore, the predictor closely collaborates with the encoding and decoding systems to facilitate signal synchronization between endpoints, thus preventing confusion. Through the utilization of prediction mechanisms, the overall system's resilience against DoS attacks is enhanced, thereby promoting stability even under more frequent and prolonged DoS attack conditions [26,27].

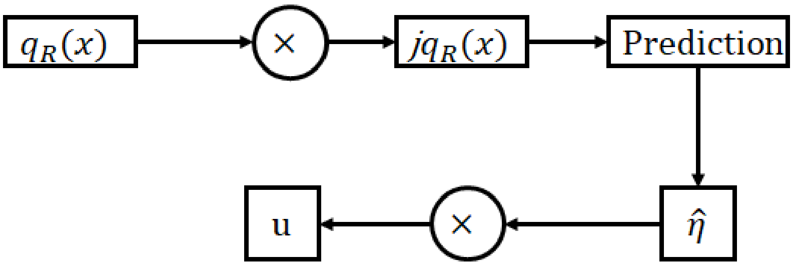

Figure 4. Model-based prediction of the decoder.

When t diverges from the successful transmission time t_s, it signifies a scenario where the system encounters a DoS attack, disrupting the transmission process [28,29]. Consequently, the decoder faces challenges in fully reconstructing the original state transmitted by the encoder. In such instances, the decoder approximates the signal at the current time using the predicted signal from the previous time step.

3.2. Secure Quantization under DoS Attacks

Uniform quantization plays a critical role in data transmission by reducing the volume of signal data requiring transmission, thereby adapting to network bandwidth constraints and significantly enhancing transmission efficiency [30–33]. Moreover, the deliberate design enables quantization to bolster resilience against DoS attacks by facilitating signal reconstruction and maintaining stability during transmission [34–36]. This study implements adaptive quantization ranges based on the system state vector to minimize quantization errors and improve transmission accuracy. The dynamic adjustment of quantization ranges helps mitigate overflow issues and potential signal distortion. Overall, with proper design, uniform quantization can surmount bandwidth limitations and bolster system robustness against DoS attacks.

First, the prediction error is defined as $e(t) = \hat{\eta}(t) - \bar{\eta}(t)$. We apply uniform quantization to the prediction error, transforming $x(e/j)$ into discrete binary data (0,1). Referring to Equation (1), we can express e(t) as $e(t) = e(t^-) - j(t^-)q\mathcal{R}(\frac{e(t^-)}{j(t^-)})$. This leads to the impulsive system:

$$\begin{cases} \dot{e}(t) = \widetilde{A}e(t), \quad t_s < t < t_{s+1} \\ e(t_s) = \begin{bmatrix} e_1(t_s) - j_1(t_s)q_R\left(\frac{e_2(t_s)}{j_1(t_s)}\right) \\ \vdots \\ e_n(t_s) - j_n(t_s)q_R\left(\frac{e_2(t_s)}{j_n(t_s)}\right) \end{bmatrix} \end{cases} \tag{6}$$

where t_s is the update instant and

$$q_R(x) := \begin{cases} \frac{\lfloor 2^{R-1}x \rfloor + 0.5}{2^{R-1}}, & \text{if} - 1 \leq x < 1 \\ 1 - \frac{0.5}{2^{R-1}} & \text{if } x = 1 \end{cases} \tag{7}$$

R is a design parameter.

The quantization of the prediction error, as described, enables effective signal transmission even in scenarios of restricted network bandwidth, including instances with DoS attacks. By keeping the quantization error within a predefined threshold, the encoding and decoding processes accurately represent the original signal. This ensures the integrity and precision of information, thereby facilitating efficient transmission.

3.3. Dynamic Time-Varying Quantization Interval Adjustment Technique

Dynamically adjusting the quantization range allows for the constraint of prediction errors within specific bounds to minimize their impact [37]. This method not only facilitates reliable signal reconstruction but also bolsters system resilience against interference, even amidst transmission disruptions caused by DoS attacks. Furthermore, it ensures synchronization between encoding and decoding endpoints while selectively transmitting quantized error data to alleviate bandwidth demands.

To swiftly adapt to environmental changes and promptly adjust the quantization range to minimize prediction errors, our research has revealed that designing a stable dynamic system with state $J(t)$, where $J(t) = [j_1(t), j_2(t), \cdots, j_{n_s}(t)]^{\mathrm{T}}$, enables the dynamic adjustment of $e(t)$ to minimize it as much as possible, ideally reducing it to 0.

Even amidst DoS attacks and bandwidth limitations, the decoder's predictive capabilities ensure the reliable reconstruction of the original system state within the AIOT framework. Precise management of the prediction error, symbolized as $e(t)$, is of utmost importance, necessitating meticulous control to minimize its impact. The correlation between $e(t)$ and the adaptive quantization range, represented as $j(t)$, is pivotal in achieving accurate state estimation despite potential distortions. This resilient transmission approach, rooted in signal prediction and quantization, is instrumental in safeguarding the performance integrity of the AIOT system in the face of DoS attacks. The relationship between $e(t)$ and $j(t)$ is

$$|\frac{e(t)}{j(t)}| \leq 1 \tag{8}$$

The following is the dynamic stable system that we designed

$$\begin{cases} J(t) & = \mathrm{e}^{c(t-t_s)} U(t-t_s) \otimes \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} J(t_s), t_s < t < t_s + 1 \\ J(t_s) & = 2^{-R} p^{n \times n} J(t_s^-), t = t_s \\ J(t_0) & \geq |e(t_0)|, t = t_0 \end{cases} \tag{9}$$

where

$$U_{(t-t_s)} = \begin{bmatrix} 1 & t-t_s & \dots & \dots & \dots & \frac{(t-t_s)^{n-1}}{(n-t_s)!} & \\ & & 1 & t-t_s & \dots & \frac{(t-t_s)^{n-2}}{(n-2)!} & \\ & & \vdots & \vdots & & & \\ & & & \vdots & \vdots & & \\ & & & & & t-t_s & \\ & & & & & & 1 \end{bmatrix} \tag{10}$$

3.4. Random Packet Loss in Adverse Network Conditions

When transmitting data through a channel vulnerable to DoS attacks, we encounter bandwidth limitations. In adverse network conditions, this challenge extends to random packet loss. From an academic perspective, this presents a dual challenge, involving restricted data transmission capacity and the unpredictable loss of data packets [38–40]. The limited capacity and unpredictable delivery of data packets pose complex challenges for state estimation [41–44]. To ensure reliable state tracking over such unreliable networks, robust techniques are essential to overcome the obstacles posed by constrained bandwidth and random packet losses. In this paper, we employ a Markov chain model to simulate the dynamic transitions of network conditions over time. The primary benefit of utilizing this model lies in its capacity to capture distinct network states, each exerting a substantial impact on packet loss rates. When packet loss occurs, we leverage a Kalman filter algorithm to predict the next state by considering both the previous state estimate and the current measurement. Subsequently, the filter adjusts the estimate based on the reliability of the measurement, thereby enabling the Kalman filter algorithm to provide reasonable system state estimations even in scenarios involving packet loss. Additionally, we construct Lyapunov functions to comprehensively analyze the system's stability.

The integrated application of the Markov chain model and Kalman filter algorithm enables more precise tracking of the system state, facilitating effective adaptation to unstable network environments. This combination yields a robust and reliable control system, essential for preserving data integrity and system stability amidst packet loss challenges and complexities of real-world networks. By constructing appropriate Lyapunov functions, we can analyze the dynamics of complex systems, guiding them towards stable and optimal equilibrium points.

The constructed Lyapunov function is represented as follows:

$$\mathrm{N}_{\eta} = \eta_{(t)}{}^{T}\mathrm{P}\eta_{(t)} \tag{11}$$

Calculating the first derivative of the Lyapunov function, one has

$$\dot{\mathrm{N}}_{\eta} = \eta^{T}(P\tilde{A} + \tilde{A}^{T}P)\eta + 2\eta^{T}P\tilde{B}u_{k}(t) \tag{12}$$

where

$$u_{k}(t) = \tilde{K}\hat{\eta}(t) \tag{13}$$

The Kalman filter algorithm is used to predict the system state to adjust the control input, as follows:

$$\dot{\hat{\eta}} = \tilde{A}\hat{\eta} + \tilde{B}u_{k}(t) \tag{14}$$

Then, the State Estimate is updated using the Kalman filter algorithm:

$$\hat{\eta}(t|t) = \hat{\eta}(t|t-1) + I(t)\cdot[C(t) - H(t)\cdot\hat{\eta}(t|t-1)] \tag{15}$$

where $\hat{\eta}(t|t)$ represents the updated state estimate at time t, $\hat{\eta}(t|t-1)$ represents the predicted state estimate at time t, $I(t)$ denotes the Kalman gain at time t, $C(t)$ signifies the measurement at time t, and $H(t)$ denotes the measurement matrix at time t.

Substituting the packet loss probability and solving for the expectation of the Lyapunov function,

$$E[\dot{N}] = (1-p)\dot{N}_{1} + p\dot{N}_{0} \tag{16}$$

To maintain system stability, it is necessary to guarantee $E[\dot{N}] \leq 0$. Therefore, we have explored the relationship between packet loss rate(p) and system stability to enhance system resilience.

4. Stability Analysis

4.1. Verification of Dynamic System Stability

In our approach, the quantization interval $J(t)$ for state measurements is adaptively adjusted over time to reduce quantization errors. Reducing $J(t)$ improves the accuracy of state quantization. Our analysis proves that $J(t)$ converges to zero under the adaptation mechanism, achieving precise quantization of system states. This helps realize accurate state estimation even when facing DoS attacks that are limited in frequency and duration. In summary, the adaptive quantization method can enhance resilience against DoS attacks by optimizing the tradeoff between quantization precision and bandwidth requirements.

Theorem 1. *In the given (9), when R is sufficiently large and c is positive, as t_s approaches infinity, the value of $J(t_s)$ tends to approach 0.*

Through iteration, we can obtain the following:

$$\begin{aligned} J(t_S) &= 2^{-R}(I^{n\times n})\mathrm{e}^{c(t_s-t_{s-1})}U_{(t-t_s)} \otimes \begin{bmatrix}1 & 1\\1 & 1\end{bmatrix} J(t_{s-1}) \\ &= (2^{-R})^{s}(I^{n\times n})e^{c(t_s-t_0)}(\prod_{k=1}^{s}U(t_k-t_{k-1})) \otimes \begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}^{s} J(t_0) \end{aligned} \tag{17}$$

Assumption 1. *There exists an A_s such that the value of J at any given moment can be represented using the value of J at time $t = 0$.*

$$J(t_s) = A_s J(t_0) \tag{18}$$

Therefore,

$$\begin{aligned} A_s &:= (2^{-R})^s I^{n\times n} e^{c(t_s - t_0)} (\prod_{k=1}^{s} U(t_k - t_{k-1})) \otimes \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}^s \\ B_s &:= (2^{-R})^s I^{n\times n} e^{c(t_s - t_0)} (\prod_{k=1}^{s} U(t_k - t_{k-1})) \\ C_s &:= \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}^s \end{aligned} \tag{19}$$

By calculation, we obtain the eigenvalues of B_s and C_s:

$$\lambda(B_s) = \frac{e^{c(t_s - t_0)}}{(2^R)^s}, \quad \lambda(C_s) = 0, 2^s \tag{20}$$

The eigenvalues of A_s

$$\lambda(A_s) = \lambda(B_s)\lambda(C_s) = 0, \frac{e^{c(t_s - t_0)}}{(2^{R-1})^s} \tag{21}$$

Therefore, if R is sufficiently large (with c being positive), as $s \to \infty$, $\lambda(A_s)$ approaches 0, which means $A_s \to 0$ as $s \to \infty$. If R is sufficiently large, as $s \to \infty$, $J(t_s) \to 0$.

4.2. Confirmation of Secure Quantization in the Presence of DoS Attacks

Theorem 2. *Given the dynamics of $e(t)$ and $J(t)$ as defined in equations (6) and (9), respectively, at any time instant t within the non-negative real numbers $(t \in \mathbb{R}_+)$, it holds that $|e(t)|$ is constrained by $J(t)$.*

Proof. First, let's determine the solution for $e(t)$ within the time interval $t_s < t < t_{s+1}$:

$$e(t) = e^{c(t-t_s)} U_{(t-t_s)} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} e(t_s) \tag{22}$$

By evaluating the magnitudes of all individual components of $e(t)$,
$| e(t) |= [| e_1(t) |, | e_2(t) |, ..., | e_n(t) |]^{\mathrm{T}}$, one has

$$|\mathrm{e}(t)| \leq \mathrm{e}^{c(t-t_s)} U(t - t_s) \otimes \left[\begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \right] |\mathrm{e}(t_s)| \tag{23}$$

Next, for $t_0 \leq t < t_1$, by examining $|e|$ and J, we obtain

$$| e(t) | \leq J(t) \tag{24}$$

Initially, we defined $| e(t_0) | \leq J(t_0)$, resulting in

$$| e(t) | \leq J(t), z_0 \leq t < t_1 \tag{25}$$

Then

$$| e(t_1^-) | \leq J(t_1^-) \tag{26}$$

Recalling (2) the properties of the function, we find

$$| e(t) - j(t) q_R \left(\frac{e(t)}{j(t)} \right) | \leq \frac{j(t)}{2^R}, \text{ if } | \frac{e(t)}{j(t)} | \leq 1 \tag{27}$$

Since $\mid e\left(t_1^-\right) \mid \leq J\left(t_1^-\right)$ (element − wise), we obtain

$$\mid e(t_1^-) - j(t_1^-)q_R\left(\frac{e(t_1^-)}{j(t_1^-)}\right) \mid \leq \frac{j(t_1^-)}{2^R} \tag{28}$$

Reviewing the update of $J(t)$,

$$J(t_S) = 2^{-R}I^{n\times n}J(t_S^-) \tag{29}$$

We can conclude that

$$\mid e(t_1) \mid = \mid e(t_1^-) - j(t_1^-)q_R\left(\frac{e(t_1^-)}{j(t_1^-)}\right) \mid \leq \frac{j(t_1^-)}{2^R} = j(t_1) \tag{30}$$

By generalizing the above results, one has

$$\mid e(t) \mid \leq J(t) \tag{31}$$

According to Theorem 1, it is known that J can approach 0 under certain conditions. Since $\mid e(t) \mid \leq J(t)$, the prediction error can, under certain conditions, approach 0. □

4.3. Verification of the Resilience between the Maximum Random Packet Loss Rate and System Stability

Theorem 3. *In Equation (16), where $E[\dot{N}] = (1-p)\dot{N}_1 + p\dot{N}_0$, to maintain system stability, it is necessary that $E[\dot{N}] \leq 0$.*

In general, network degradation can lead to random packet loss. To mathematically analyze the effects of such losses, we employ a Markov chain model to simulate the dynamic evolution of network conditions over time. In instances of random packet loss, we utilize an estimation scheme based on the Kalman filter algorithm to optimize the prediction of the system's state trajectory, thereby mitigating the impact of measurement losses. This method enables a comprehensive understanding of the dynamics involved in network behavior and provides a means to enhance system robustness against unpredictable events such as random packet loss.

Specifically, we prove that, below a critical loss threshold, the Kalman filter algorithm facilitates resilient state estimation to guarantee closed-loop stability. Consequently, when the packet loss rate induced by adverse network conditions is restricted below this quantified stability threshold, the stability of the feedback control system can be ensured mathematically.

When the network state is favorable, the system experiences no random packet loss, and we obtain

$$u_k(t) = \tilde{K}\eta(t) \tag{32}$$

$$\dot{\mathrm{N}}_1 = \eta^T(P\tilde{A} + \tilde{A}^TP)\eta + 2\eta^TP\tilde{B}K\eta \tag{33}$$

When the network state is poor, and the system experiences random packet loss, we find

$$u_k(t) = \tilde{K}\hat{\eta}(t) \tag{34}$$

$$\dot{\mathrm{N}}_0 = \hat{\eta}^T(P\tilde{A} + \tilde{A}^TP)\hat{\eta} + 2\hat{\eta}^TP\tilde{B}u_K \tag{35}$$

We need to ensure that $E[\dot{N}] \leq 0$; therefore,

$$p \leq \dot{N}_1/(\dot{N}_1 - \dot{N}_0) \tag{36}$$

By substituting Equations (33) and (35) into Inequality (36),

$$(1-p)(\eta^T(P\tilde{A} + \tilde{A}^TP)\eta + 2\eta^TP\tilde{B}\tilde{K}\eta) + p(\hat{\eta}^T(P\tilde{A} + \tilde{A}^TP)\hat{\eta} + 2\hat{\eta}^TP\tilde{B}u_K) \leq 0 \tag{37}$$

The analysis presented enables the establishment of a suitable threshold for the random packet loss rate, thereby ensuring the stability of the networked control system amidst DoS attacks. Our integrated framework, which merges Markov modeling and the Kalman filter algorithm, offers robust methodologies for quantifying resilience against packet losses and deriving stability conditions essential for designing secure control systems.

4.4. Verification of Overall Closed-Loop System Stability under DoS Attacks

Theorem 4. *In the given (1), when the eigenvalues of the matrix $(\tilde{A} + \tilde{B}\tilde{K})$ are negative and when the error term $e(t)$ approaches zero, the system remains stable.*

The linear state-space system is as follows:

$$\dot{\bar{\eta}}(t) = \tilde{A}\bar{\eta}(t) + \tilde{B}u(t) \tag{38}$$

The following is the control input of the system:

$$u_k(t) = \tilde{K}\hat{\eta}(t) \tag{39}$$

Below is the prediction error associated with the system's state vector:

$$e(t) = \hat{\eta}(t) - \bar{\eta}(t) \tag{40}$$

Therefore, we obtain

$$\dot{\bar{\eta}}(t) = (\tilde{A} + \tilde{B}\tilde{K})\bar{\eta}(t) + \tilde{B}\tilde{K}e(t) \tag{41}$$

Thus, the conditions to ensure system stability in the presence of a DoS attack are that the eigenvalues of the matrix $(\tilde{A} + \tilde{B}\tilde{K})$ are negative and the error term $e(t)$ needs to approach zero.

5. Numerical Simulation

Simulation studies were conducted in Python 3.7. We selected Windows 10 as the operating system, to ensure compatibility with the simulation tools. The computer hardware comprises two physical CPU cores and four logical CPU cores, ensuring efficient execution of the simulation experiments. By initializing the system states to the values of 1 and -1, our proposed controller design was implemented to regulate the state dynamics, to asymptotically drive the AIOT system to the desired equilibrium point. The effectiveness of the controller in guiding the states toward stability from the specified non-zero initial conditions is empirically validated through closed-loop control simulations.

Firstly, we considered an open-loop and unstable system with the following matrix representation:

$$A = \tilde{A}(t) = \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix}, B = \tilde{B}(t) = \begin{bmatrix} 2.3 & 0 \\ 0 & 2.3 \end{bmatrix} \tag{42}$$

The state feedback matrix was defined as

$$\tilde{K}(t) = \begin{bmatrix} -3.2 & -2.65 \\ -2.65 & -3.7 \end{bmatrix} \tag{43}$$

In simulation with a 0.1 s transmission interval, we assessed the controller's performance in the presence of DoS attacks and adverse network conditions. Randomized attacks occurred within a 20 s timeframe, totaling 15.52 s. The quantization parameter was set to R = 2. The results demonstrate that our adaptive quantization and control framework ensures the system's resilience against DoS attacks and maintains stability in the face of random packet losses. Mathematical analysis indicates that prediction errors converge to zero, quantization intervals adapt to counteract packet drops, and the Kalman filter algorithm produces optimal estimates for accurate state tracking. Simulations under various network conditions further confirm the robustness guarantees.

5.1. Empirical Validation of Prediction Error Convergence Dynamics

After the initial transient phase, the prediction error exhibits an exponential decay trend (Figure 5). Eventually, the prediction error converges to zero. This validates the theoretical analysis that, under the adaptive quantization mechanism, prediction errors monotonically decrease over time, achieving zero steady-state error as estimation accuracy continuously improves. This further confirms that the designed control framework can effectively alleviate the impact of DoS attacks on AIOT systems. The experimentally verified results are supported by rigorous stability analysis, endorsing the resilience of the proposed integrated cyber-physical approach against random packet losses.

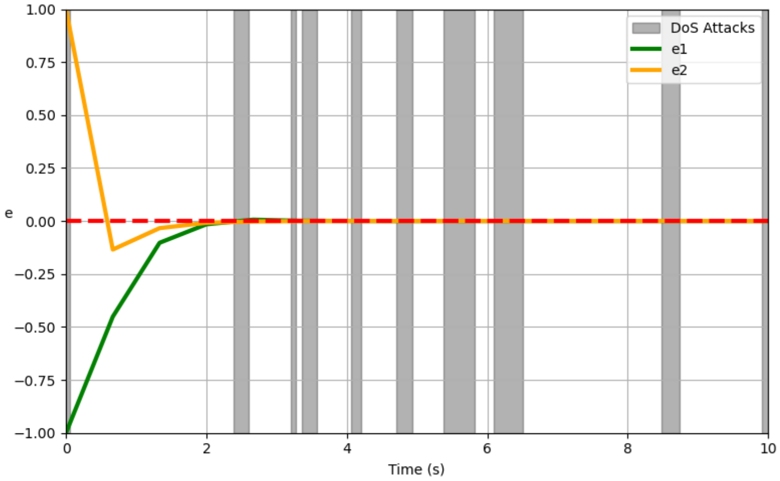

Figure 5. Prediction error.

5.2. Simulation-Based Quantization Interval Convergence Analysis

The simulation results demonstrate that the quantization interval $J(t)$ exhibits an exponential decaying trend under the influence of the adaptive tuning algorithm, eventually converging to zero. This corroborates our theoretical analysis that $J(t)$ decreases monotonically to zero over time (Figure 6). The empirical evidence validates the conclusion that the convergence of $J(t)$ minimizes quantization errors to achieve high-precision state quantification. As $J(t)$ approaches zero, the vanishingly small quantization intervals effectively eliminate quantization distortions, accomplishing accurate quantization.

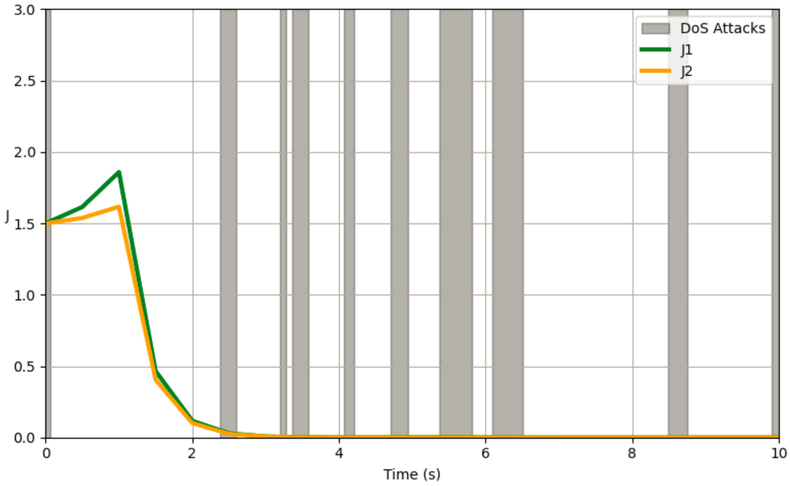

Figure 6. Quantization interval.

5.3. Investigation into Kalman Filter Algorithm Performance for State Estimation

Through simulating the temporal evolution of the system state and introducing multidimensional measurement noise, the Kalman filter algorithm iteratively estimates and corrects the system state at each time step through prediction and update steps. Ultimately, the performance of the Kalman filter algorithm in a multidimensional scenario is rigorously evaluated by computing the root mean square error between the filtered and true states. The plotted graphs elucidate the true state, noisy measurements, and the dynamic evolution of the Kalman-filtered state over time, underscoring the filter's precise estimation of the system state and its resilience against noise (see Figure 7). Consequently, the Kalman filter algorithm framework provides effective and robust means for ensuring stability and enhancing the performance of network control systems.

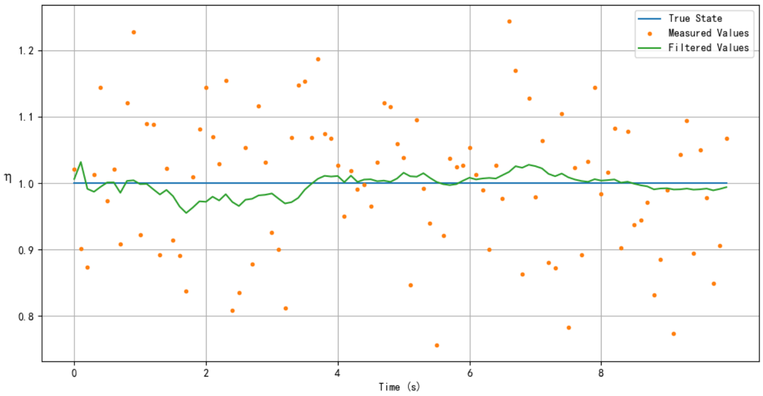

Figure 7. The state predicted by the Kalman filter.

5.4. Modeling and Evaluation of Random Packet Losses under DoS Attacks

In the simulation experiments, the initial random packet loss rate is configured as 1, representing an extreme case of total data unavailability. As the adaptive control and estimation mechanism iterates, the loss rate gradually decreases and eventually stabilizes around 0.3115 (Figure 8). This demonstrates that the closed-loop system can maintain stability under such a packet loss rate. This stable loss rate numerically validates our theoretically derived stability condition that the system retains stability given packet loss rates below 0.3115.

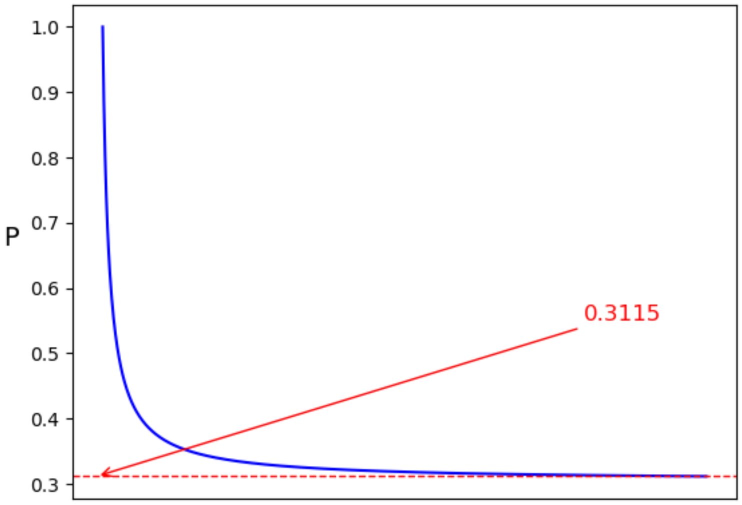

Figure 8. Random packet loss rate.

5.5. Characterization of Closed-Loop State Trajectories under DoS Attacks

As depicted by the system state response, following the initial transient phase, the state vector gradually converges to the theoretically predicted equilibrium under the control input (Figure 9). This validates the efficacy of the designed controller. Despite the substantial simulated random packet losses mimicking denial-of-service attacks, the system state remains stable. This suggests that the proposed network control framework can effectively endure the impact of denial-of-service attacks and random packet losses in adverse network conditions, thereby ensuring the stability and regular operation of the system.

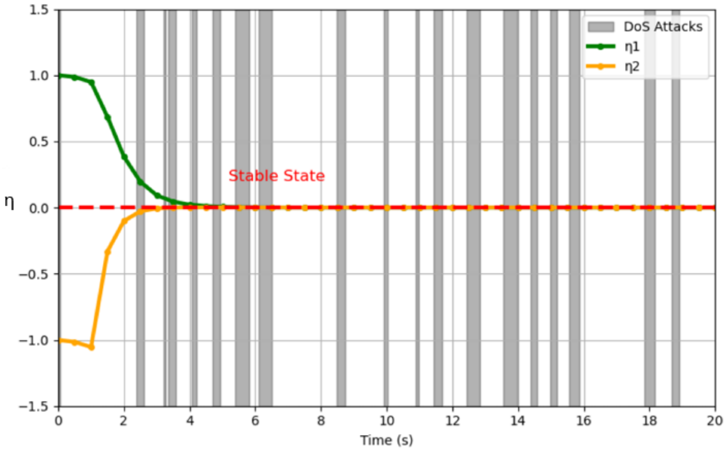

Figure 9. System state.

6. Conclusions

This paper addresses the challenges stemming from unpredictable packet losses and persistent DoS attacks within AIOT systems. We employ uniform quantization in the encoding–decoding framework, effectively mitigating bandwidth constraints induced by DoS attacks. The utilization of sophisticated Markov chain models and Kalman filter techniques bolsters the system's resilience against random packet losses. Through detailed stability analysis grounded in Lyapunov theory, the intricate relationship between system stability and packet loss rates is impeccably elucidated. Simulation results demonstrate that the proposed approach can ensure the security and reliability of AIOT systems, particularly when facing complex network conditions. For future research, exploring advanced techniques such as machine learning algorithms for adaptive mitigation, investigating alternative encoding–decoding frameworks, and developing real-time detection mechanisms could enhance the security and reliability of AIOT systems.

Author Contributions: Writing—original draft preparation, X.C.; project administration, W.W.; writing—review and editing, Z.C.; supervision, X.W. and M.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Shandong Provincial Innovation Capability Improvement Project for Small and Medium-sized Scientific and Technological Enterprises under Grant 2023TSGC0108, in part by the Taishan Scholars Program under Grant tsqn202211203, in part by the Shandong Provincial Higher Education Youth Innovation Team Development Project under Grant 2022KJ290, and in part by the "20 New Universities" Project of Jinan City under Grant 202228077. The Pilot Project for Integrated Innovation of Science, Education and Industry of Qilu University of Technology (Shandong Academy of Sciences) under Grant 2022JBZ01-01 is also acknowledged.

Data Availability Statement: This paper did not utilize any datasets, nor did it generate any new data.

Acknowledgments: With the help of Xuguo Jiao, Chuantao Wu, and Ruixin Liu, our work was successfully completed. Jiao works at the School of Information and Control Engineering, Qingdao University of Technology. He provided valuable revision suggestions for the abstract, background, conclusion, and overall structure of the manuscript, which enhanced the presentation and coherence of our research. Wu and Liu work at Shandong Zhongzhi Electronics CO, LTD. Wu conducted an in-depth analysis of system stability under denial of service (DoS) attacks, which enhanced to the theoretical and empirical foundation of our research. Liu organized and analyzed literatures on DoS attacks and random packet loss, which enriched the contents and refined the academic depth. We are deeply appreciative of their contributions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Adli, H.K.; Remli, M.A.; Wan Salihin Wong, K.N.S.; Ismail, N.A.; González-Briones, A.; Corchado, J.M.; Mohamad, M.S. Recent Advancements and Challenges of AIoT Application in Smart Agriculture: A Review. *Sensors* **2023**, *23*, 3752. [CrossRef] [PubMed]
2. Nozari, H.; Szmelter-Jarosz, A.; Ghahremani-Nahr, J. Analysis of the challenges of artificial intelligence of things (AIoT) for the smart supply chain (case study: FMCG industries). *Sensors* **2022**, *22*, 2931. [CrossRef] [PubMed]
3. Hou, K.M.; Diao, X.; Shi, H.; Ding, H.; Zhou, H.; de Vaulx, C. Trends and Challenges in AIoT/IIoT/IoT Implementation. *Sensors* **2023**, *23*, 5074. [CrossRef]
4. Shi, Z.; Yao, W.; Li, Z.; Zeng, L.; Zhao, Y.; Zhang, R.; Tang, Y.; Wen, J. Artificial intelligence techniques for stability analysis and control in smart grids: Methodologies, applications, challenges, and future directions. *Appl. Energy* **2020**, *278*, 115733. [CrossRef]
5. Wang, X.; Ding, D.; Ge, X.; Dong, H. Neural-Network-Based Control with Dynamic Event-Triggered Mechanisms under DoS Attacks and Applications in Load Frequency Control. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2022**, *69*, 5312–5324. [CrossRef]
6. Eliyan, L.F.; Di Pietro, R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Gener. Comput. Syst.* **2021**, *122*, 149–171. [CrossRef]
7. Sun, X.; Gu, Z.; Yue, D.; Xie, X. Event-triggered H∞ filtering for cyber–physical systems against DoS attacks. *IEEE Trans. Syst. Man, Cybern. Syst.* **2022**, *53*, 2705–2715.
8. Baglietto, M.; Battistelli, G.; Tesi, P. Packet loss detection in networked control systems. *Int. J. Robust Nonlinear Control* **2020**, *30*, 6073–6090. [CrossRef]
9. Li, J.Y.; Wang, Z.; Lu, R.; Xu, Y. A component-based coding–decoding approach to set-membership filtering for time-varying systems under constrained bit rate. *Automatica* **2023**, *152*, 110874. [CrossRef]
10. Zhang, X.M.; Han, Q.L.; Ge, X.; Ding, L. Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks. *IEEE Trans. Cybern.* **2019**, *50*, 3616–3626. [CrossRef]
11. Liu, X.K.; Wen, C.; Xu, Q.; Wang, Y.W. Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks. *IEEE Trans. Smart Grid* **2021**, *12*, 3742–3754. [CrossRef]
12. Deng, C.; Guo, F.; Wen, C.; Yue, D.; Wang, Y. Distributed resilient secondary control for DC microgrids against heterogeneous communication delays and DoS attacks. *IEEE Trans. Ind. Electron.*, **2022**, *69*, 11560–11568. [CrossRef]
13. Liu, C.; Du, D.; Zhang, C.; Peng, C.; Fei, M. Observability Analysis of Networked Control Systems Under DoS Attacks. In Proceedings of the IECON 2023—49th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 16–19 October 2023; pp. 1–6. [CrossRef]
14. Ge, P.; Chen, B.; Teng, F. Cyber-Resilient Self-Triggered Distributed Control of Networked Microgrids Against Multi-Layer DoS Attacks. *IEEE Trans. Smart Grid* **2023**, *14*, 3114–3124. [CrossRef]
15. Zhang, D.; Han, Q.L.; Zhang, X.M. Network-based modeling and proportional–integral control for direct-drive-wheel systems in wireless network environments. *IEEE Trans. Cybern.* **2019**, *50*, 2462–2474. [CrossRef] [PubMed]
16. Zhao, C.; Cai, L.; Cheng, P. Stability analysis of vehicle platooning with limited communication range and random packet losses. *IEEE Internet Things J.* **2020**, *8*, 262–277. [CrossRef]
17. Kazemy, A.; Lam, J.; Zhang, X.M. Event-triggered output feedback synchronization of master-slave neural networks under deception attacks. *IEEE Trans. Neural Netw. Learn. Syst.* **2020**, *33*, 952–961. [CrossRef] [PubMed]
18. Wu, C.; Zhao, X.; Xia, W.; Liu, J.; Başar, T. L2-gain analysis for dynamic event-triggered networked control systems with packet losses and quantization. *Automatica* **2021**, *129*, 109587. [CrossRef]
19. Zhang, X.M.; Han, Q.L.; Ge, X. A novel approach to H∞ performance analysis of discrete-time networked systems subject to network-induced delays and malicious packet dropouts. *Automatica* **2022**, *136*, 110010. [CrossRef]
20. Zhou, M.Y.; Chen, W.H.; Zhang, C.K.; Hou, Y.X.; Xie, K.Y. Stability Analysis of Discrete Networked Systems with Network Induced Delay and Malicious Packet Dropout Based on a Matrix Transformation Method. In Proceedings of the 2023 42nd Chinese Control Conference (CCC), Tianjin, China, 24–26 July 2023; pp. 210–214. [CrossRef]
21. Pan, Y.; Wu, Y.; Lam, H.K. Security-based fuzzy control for nonlinear networked control systems with DoS attacks via a resilient event-triggered scheme. *IEEE Trans. Fuzzy Syst.* **2022**, *30*, 4359–4368. [CrossRef]
22. de Bézenac, E.; Rangapuram, S.S.; Benidis, K.; Bohlke-Schneider, M.; Kurle, R.; Stella, L.; Hasson, H.; Gallinari, P.; Januschowski, T. Normalizing Kalman filters for multivariate time series analysis. *Adv. Neural Inf. Process. Syst.* **2020**, *33*, 2995–3007.

23. Hu, S.; Yue, D.; Cheng, Z.; Tian, E.; Xie, X.; Chen, X. Co-design of dynamic event-triggered communication scheme and resilient observer-based control under aperiodic DoS attacks. *IEEE Trans. Cybern.* **2020**, *51*, 4591–4601. [CrossRef] [PubMed]
24. Chen, P.; Liu, S.; Chen, B.; Yu, L. Multi-agent reinforcement learning for decentralized resilient secondary control of energy storage systems against DoS attacks. *IEEE Trans. Smart Grid* **2022**, *13*, 1739–1750. [CrossRef]
25. Gasmi, E.; Amine Sid, M.; Hachana, O. Nonlinear event-based state estimation using particle filter under packet loss. *ISA transactions* **2024**, *144*, 176–187. [CrossRef] [PubMed]
26. Wang, M.; Li, P.; Li, X. Event-triggered delayed impulsive control for input-to-state stability of nonlinear impulsive systems. *Nonlinear Anal. Hybrid Syst.* **2023**, *47*, 101277. [CrossRef]
27. Yin, L.; Xu, L.; Zhu, H.; Zhu, Y.; Wu, C. Input-output data based tracking control under DoS attacks. *Int. J. Control* **2023**, 1–11.
28. Zalluhoglu, U.; Venkataraman, R.; Ceze, M.; Carson, H.; Szmuk, M.; McFarl, ; C.; Friedman, D. Assessment of metrics that measure the effectiveness of control allocation and their use in linear closed-loop analysis. In Proceedings of the AIAA SciTech 2023 Forum, National Harbor, MA, USA, 23–27 January 2023; p. 1052.
29. Liu, X.; Deng, F.; Zeng, P.; Gao, X.; Zhao, X. Sampled-data resilient control for stochastic nonlinear CPSs under DoS attacks. *Int. J. Syst. Sci.* **2023**, *54*, 1165–1171. [CrossRef]
30. Yan, J.; Shi, L.; Xia, Y.; Zhang, Y. Quantized output feedback control for switched systems with DoS attacks and event-triggered sampling. *J. Frankl. Inst.* **2022**, *359*, 8522–8538. [CrossRef]
31. Wang, C.; Xie, W.; Gao, J.; Wu, P.; Liu, P.X. Adaptive Event-Based Dynamic Output Feedback Control for Unmanned Marine Vehicle Systems under Denial-of-Service Attack. *Electronics* **2024**, *13*, 515. [CrossRef]
32. Ye, Z.; Zhang, D.; Cheng, J.; Wu, Z.G. Event-triggering and quantized sliding mode control of UMV systems under DoS attack. *IEEE Trans. Veh. Technol.* **2022**, *71*, 8199–8211. [CrossRef]
33. Shawky, M.A.; Shah, S.T.; Abbasi, Q.H.; Hussein, M.; Imran, M.A.; Hasan, S.F.; Ansari, S.; Taha, A. RIS-Enabled Secret Key Generation for Secured Vehicular Communication in the Presence of Denial-of-Service Attacks. *Sensors* **2023**, *23*, 4104. [CrossRef]
34. Kato, R.; Cetinkaya, A.; Ishii, H. Linearization-based quantized stabilization of nonlinear systems under DoS attacks. *IEEE Trans. Autom. Control* **2021**, *67*, 6826–6833. [CrossRef]
35. Li, Z.; Zhou, C.; Che, W.; Deng, C.; Jin, X. Data-based security fault tolerant iterative learning control under denial-of-service attacks. *Actuators* **2022**, *11*, 178. [CrossRef]
36. Amini, A.; Asif, A.; Mohammadi, A. RQ-CEASE: A resilient quantized collaborative event-triggered average-consensus sampled-data framework under denial of service attack. *IEEE Trans. Syst. Man, Cybern. Syst.* **2020**, *51*, 7027–7039. [CrossRef]
37. Yin, J.; Lu, A. Observer-Based Active Control Strategy for Networked Switched Systems against Two-Channel Asynchronous DoS Attacks. *Actuators* **2023**, *12*, 335. [CrossRef]
38. Shrivastava, P.; Soon, T.K.; Idris, M.Y.I.B.; Mekhilef, S. Overview of model-based online state-of-charge estimation using Kalman filter family for lithium-ion batteries. *Renew. Sustain. Energy Rev.* **2019**, *113*, 109233. [CrossRef]
39. Revach, G.; Shlezinger, N.; Ni, X.; Escoriza, A.L.; Van Sloun, R.J.; Eldar, Y.C. KalmanNet: Neural network aided Kalman filter algorithm for partially known dynamics. *IEEE Trans. Signal Process.* **2022**, *70*, 1532–1547. [CrossRef]
40. Xia, X.; Hashemi, E.; Xiong, L.; Khajepour, A. Autonomous vehicle kinematics and dynamics synthesis for sideslip angle estimation based on consensus Kalman filter. *IEEE Trans. Control Syst. Technol.* **2022**, *31*, 179–192. [CrossRef]
41. Mor, B.; Garhwal, S.; Kumar, A. A systematic review of hidden Markov models and their applications. *Arch. Comput. Methods Eng.* **2021**, *28*, 1429–1448. [CrossRef]
42. Liu, L.; Liu, Y.J.; Chen, A.; Tong, S.; Chen, C.P. Integral barrier Lyapunov function-based adaptive control for switched nonlinear systems. *Sci. China Inf. Sci.* **2020**, *63*, 1–14. [CrossRef]
43. Yuan, S.; Lv, M.; Baldi, S.; Zhang, L. Lyapunov-equation-based stability analysis for switched linear systems and its application to switched adaptive control. *IEEE Trans. Autom. Control* **2020**, *66*, 2250–2256. [CrossRef]
44. Gao, M.; Li, Z.; Pang, T.; Xu, H.; Chen, S. Event-Based Security Control for Markov Jump Cyber–Physical Systems under Denial-of-Service Attacks: A Dual-Mode Switching Strategy. *Appl. Sci.* **2023**, *13*, 11815. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.