symmetry

MDPI

Article

A Continuous Terminal Sliding-Mode Observer-Based Anomaly Detection Approach for Industrial Communication Networks

Long Xu [1,2,3,*], Wei Xiong [1,2,3], Minghao Zhou [4] and Lei Chen [5]

[1] Key Laboratory of Measurement and Control of CSE, Ministry of Education, School of Automation, Southeast University, Nanjing 210096, China; 230199035@seu.edu.cn
[2] 3onedata Co., Ltd., Shenzhen 518055, China
[3] 3onedata Qitong Co., Ltd., Shanghai 201601, China
[4] School of Electrical and Electronic Engineering, Harbin University of Science and Technology, Harbin 150001, China; zhouminghao@hrbust.edu.cn
[5] Advanced Research Institute of Multidisciplinary Science, Beijing Institute of Technology, Beijing 100081, China; 6120210013@bit.edu.cn
* Correspondence: long_xu@seu.edu.cn

Abstract: Dynamic traffic monitoring is a critical part of industrial communication network cybersecurity, which can be used to analyze traffic behavior and identify anomalies. In this paper, industrial networks are modeled by a dynamic fluid-flow model of TCP behavior. The model can be described as a class of systems with unmeasurable states. In the system, anomalies and normal variants are represented by the queuing dynamics of additional traffic flow (*ATF*) and can be considered as a disturbance. The novel contributions are described as follows: (1) a novel continuous terminal sliding-mode observer (TSMO) is proposed for such systems to estimate the disturbance for traffic monitoring; (2) in TSMO, a novel output injection strategy is proposed using the finite-time stability theory to speed up convergence of the internal dynamics; and (3) a full-order sliding-mode-based mechanism is developed to generate a smooth output injection signal for real-time estimations, which is directly used for anomaly detection. To verify the effectiveness of the proposed approach, the real traffic profiles from the Center for Applied Internet Data Analysis (CAIDA) DDoS attack datasets are used.

Keywords: network traffic monitoring; sliding-mode observers; industrial switches; industrial communication network; TCP/IP; DDoS attacks; anomaly detection

Citation: Xu, L.; Xiong, W.; Zhou, M.; Chen, L. A Continuous Terminal Sliding-Mode Observer-Based Anomaly Detection Approach for Industrial Communication Networks. *Symmetry* **2022**, *14*, 124. https://doi.org/10.3390/sym14010124

Academic Editors: Haifeng Ma, Huazhou Hou and José Carlos R. Alcantud

Received: 31 October 2021
Accepted: 4 January 2022
Published: 10 January 2022

1. Introduction

An industrial network is a communication network that applied in an industrial environment, i.e., manufacturing, power generation, energy distribution, and transportation, with protocols to provide real-time control and monitoring of industrial systems. Due to the development of the Industrial Internet of Things (IIoT), a variety of technologies, such as sensors, wireless communications, and computing, have paved the way from local to remote networks for performing remote operations, monitoring, and maintenance through the Internet. Security concerns about the IIoT have been raised. On 21 October 2016, attackers utilize the Mirai IoT botnet to launch high-impact distributed denial of service (DDoS) attacks against the Dyn DNS service, which caused an extended Internet outage [1]. Therefore, the vulnerability of industrial networks have reinforced the importance of safety and security to protect industrial systems against cyber threats [2]. To detect and prevent the attacks, researchers are focused on designing traffic monitoring devices, such as firewalls and intrusion detection systems (IDSs), placed at different levels of industrial networks to detect and prevent attacks [3].

In the past years, many IDS methods have been proposed for monitoring malicious activities in industrial networks. By the types of information source, IDSs can be classified into two types: host-based IDSs (HIDSs) and network-based IDSs (NIDSs). HIDSs monitor the characteristics of information in hosts to detect anomalous behavior. A data stream mining-based HIDS is proposed for the advanced metering infrastructure to collect and analyze energy usage data [4]. A novel multiattribute HIDS is developed in supervisory control and data acquisition (SCADA) cybersystems [5]. On the other hand, NIDSs analyze network activities in terms of traffic volume, protocol usage, IP address, and so on. Several NIDSs are proposed at network gateways, e.g., firewalls or routers, to online monitor the whole networks. For example, a deep packet inspection method is proposed to deal with high-layer protocols in terms of performance indexes at firewalls [6]. However, the typical case of limited-size data packets are not considered. A Markov chain NIDS is investigated to study the performance of rule-based IP traffic include throughput, packet loss, and packet delay at firewalls [7]. Furthermore, a filtering system-based NIDS is developed to block spurious traffic by using an IP packet queuing engine [8]. With the increased complexity and the growing amount network usages, the static analytical approach fails to meet the monitoring criteria in accuracy and efficiency. Thus, the real-time monitoring approach is needed to analyze network traffic at network gateways to detect malicious attacks. The dynamics of industrial TCP networks in routers can be expressed as a fluid-flow model by using stochastic differential nonlinear equations [9]. Based on the model, some observers have been proposed for the dynamical network monitoring system [10]. The observers are capable to detect anomalies. Since the anomalies are being considered as perturbations in the systems, observers can be designed to estimate the anomalies [11].

The current observers for traffic monitoring can be classified into two categories: linear observers and nonlinear observers. The linear observer strategy is developed to feed back the output errors in a linear manner. For example, the Luenberger observers (LOs) are developed to monitor the TCP traffic flows [12]. Moreover, LOs are synthesized to reconstruct the unmeasurable congestion window, i.e., C_{wnd}, for traffic estimations. The time-delay observers are applied to supervise the network via TCP flow estimations and detecting anomalies. However, they are unable to accurately estimate the system states in the presence of unknown signals or uncertainties [13]. Thus, the fuzzy observers (FOs) are designed by using a Takagi-Sugeno (T-S) system that consists of a number of linear time-invariant models to achieve global performance [14], whereas the local linear observers of FOs are still hardly able to force the estimation errors to zero. The nonlinear observers, such as sliding-mode observers (SMOs), are applied for traffic monitoring [15,16]. SMOs are designed using sliding-mode control (SMC) method. SMC has unique properties, such as low sensitivity to parameter variations and strong robustness to external disturbances, and has been applied in many areas [17–20]. The existing SMOs can be classified into two types, i.e., linear SMOs and terminal SMOs. The linear SMOs that include conventional SMOs (CSMOs) and super-twisting observers (STOs) use the linear hypersurface with asymptotic stability. For example, CSMOs are proposed for traffic monitoring and detecting anomalies [21]. In the CSMOs, low-pass filters are used to soften the signals with high frequency components, which cause a phase lag and delay. To deal with the chattering phenomenon, STOs are proposed to estimate *ATF* without any low-pass filters [22]. However, the STOs are activated when the estimate errors converged to zero, which results in a long start-up time. In contrast, terminal SMOs employ the nonlinear a hypersurface and drive the estimate errors to the hypersurface in finit-time [23–27].

Different from the existing observer methods for anomaly detection under the network communication scenario [28–30], the novel terminal sliding-mode observer (TSMO) is proposed with the contributions described as: (1) TSMO is designed for disturbance estimation with the properties of finite-time convergence of the estimation error; (2) the proposed TSMO can increase the convergence speed of the internal dynamics to meet the criteria for real-time anomaly detection; (3) a full order sliding mode is designed to achieve a smooth output injection and is directly applied for estimation; and (4) the

TSMO is proposed to increase the estimation dynamics of the abnormal traffic, in which the estimation error will converge to a bounded small area within a finite-time and then converge to zero asymptotically. For the network communication scenarios, it is required to meet two criterias: robustness and smooth output injection signals. The results of the estimation for *ATF* can be further used for the anomaly detection. The paper aims at overcoming the following three challenges from the theoretical viewpoints:

1. How to develop an observer for a class of systems where parts of states are unmeasurable.
2. How to increase the convergence speed of the internal dynamics in the observer.
3. How to design a smooth output injection of the observer and apply it directly for the estimation algorithm.

The remainder of the paper is organized as follows. The fluid-flow model of industrial networks is described in Section 3. The sliding-mode observer for the system is proposed in Section 4. In Section 5, the practical traffic replay is carried out to illustrate the effectiveness of the proposed method. Finally, conclusions are given in Section 6.

2. Problem Formulation and Preliminaries

Consider a class of linear time-varying delay systems represented by

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{A}_d\boldsymbol{x}(t-\tau) + \boldsymbol{b}u(t) + \boldsymbol{d}\delta(t), \tag{1}$$

where $\boldsymbol{x}(t) = [x_1(t), x_2(t)]^T \in \mathbb{R}^2$ is the system state, $u(t) \in \mathbb{R}$ is the control input, $\tau = \tau(t) \in \mathbb{R}$ is the time delay, $\delta(t) \in \mathbb{R}$ is the disturbance, and $\boldsymbol{A} = [a_{11}, a_{12}; a_{21}, a_{22}]$, $\boldsymbol{A}_d = [a_{11d}, a_{12d}; a_{21d}, a_{22d}]$, $\boldsymbol{b} = [1, 0]^T$, and $\boldsymbol{d} = [0, 1]^T$ are time invariant system parameters.

Some assumptions are made as: (1). the system (1) is stable; (2). the state x_2 is measurable; and (3). the state x_1 is unmeasurable.

The objective in the paper is to design an observer for estimating the disturbance $\delta(t)$ in (1). Now, an observer is proposed for the system (1) in the form

$$\dot{\hat{\boldsymbol{x}}}(t) = \boldsymbol{A}\hat{\boldsymbol{x}}(t) + \boldsymbol{A}_d\hat{\boldsymbol{x}}(t-\tau) + \boldsymbol{b}u(t) + \boldsymbol{v}(t), \tag{2}$$

where $\hat{\boldsymbol{x}}(t) = [\hat{x}_1(t), \hat{x}_2(t)]^T \in \mathbb{R}^2$ is the estimate of $\boldsymbol{x}(t)$, and $\boldsymbol{v}(t) = [v_1(t), v_2(t)]^T \in \mathbb{R}^2$ is the output injection of the observer.

If the errors between the estimates and the true states are written as $\boldsymbol{e}(t) = \hat{\boldsymbol{x}}(t) - \boldsymbol{x}(t)$, then, from (1) and (2), the following error system is obtained

$$\dot{\boldsymbol{e}}(t) = \boldsymbol{A}\boldsymbol{e}(t) + \boldsymbol{A}_d\boldsymbol{e}(t-\tau) - \boldsymbol{d}\delta(t) + \boldsymbol{v}(t), \tag{3}$$

and the estimate of the disturbance $\delta(t)$ follows that

$$\hat{\delta}(t) = \lim_{\boldsymbol{e}(t)\to 0} v_2(t). \tag{4}$$

The estimation process includes the following two steps:

1. The error system (3) converges to zero asymptotically or in finite-time by using the output injection of the observer.
2. Once the error system (3) converges to zero, the disturbance in (1) can be estimated using (4).

The output injection of the observer $\boldsymbol{v}(t)$ in (2) can only utilize the measurable error e_2, i.e., $v_1 = v_1(e_2)$, $v_2 = v_2(e_2)$. The output injection $v_2 = v_2(e_2)$ can be designed to force e_2 converging to zero, although there exists unmeasurable e_1 and disturbance $\delta(t)$ in the error system (3). However, in the conventional observer [22], there is no output injection v_1 for the internal dynamics of error system (3). In such a case, the error state e_1 will converge to zero asymptotically due to the assumption 1. As a result, the convergence of e_1 cannot be affected by the signal v_2 and may be very slow. To address this problem in the conventional

methods, an output injection signal v_1 is proposed to the error system (3), which aims at speeding up the convergence of the internal dynamics of the error system (3).

When the error system (3) converges to zero, the estimate of the disturbance can be obtained using (4). Hence, the output injection of the observer $v_2(t)$ is required to be smooth, which is a challenge to the design of the SMO.

Two Lemmas are stated below and will be used in the proof of the Theorems later.

Lemma 1 ([31]). *Given a nonlinear system $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x})$, where $\boldsymbol{x} \in \mathbb{R}^n$, $\boldsymbol{f}(0) = 0$, and $\boldsymbol{f}(\cdot) : \mathbb{R}^n \to \mathbb{R}^n$ is a continuous function. If there exists a continuous positive definite function $V(\boldsymbol{x})$ such that $\dot{V}(\boldsymbol{x}) + cV^{\alpha}(\boldsymbol{x}) \leq 0$, where $c > 0$ and $\alpha \in (0, 1)$ are two constants. Then, $V(\boldsymbol{x})$, $\forall V(\boldsymbol{x}_0) \neq 0$, approaches to zero in a finite-time T, where $T \leq V^{1-\alpha}(\boldsymbol{x}(0))/(c(1-\alpha))$.*

To prove the Theorems in the paper, the stability of the following form of linear systems with time-varying delay is considered:

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{A}_d\boldsymbol{x}(t - \tau(t)), & t > 0, \\ \boldsymbol{x}(t) = \boldsymbol{\varphi}(t), & t \in [-\tau_2, 0] \end{cases}, \tag{5}$$

where $\boldsymbol{x}(t) \in \mathbb{R}^n$ is the state, $\boldsymbol{A}$ and $\boldsymbol{A}_d$ are constant matrices with appropriate dimensions, the time delay, $\tau(t)$, is a time-varying continuous function that satisfies $\tau_1 < \tau(t) < \tau_2$ and $\dot{\tau}(t) \leq \mu$, where τ_1, τ_2, and μ are all known positive constants, and the initial condition, $\boldsymbol{\varphi}(t) \in \mathbb{R}^n$, is a continuous function of $t \in [-\tau_2, 0]$.

Lemma 2 ([32]). *The system (5) is asymptotically stable if there exist matrices $\boldsymbol{P} > 0$; $\boldsymbol{Q}_i > 0$, $\boldsymbol{Z}_j > 0$, for $i = 1, 2, 3$, and $j = 1, 2$; $\boldsymbol{N}_i$, $\boldsymbol{M}_i$, and $\boldsymbol{S}_i$, $i = 1, 2$ with appropriate dimensions such that the following LMI holds:*

$$\boldsymbol{\Phi} = [\boldsymbol{\phi}_{\iota\nu}]_{8\times 8} < 0, \tag{6}$$

where $\boldsymbol{\Phi}$ is the symmetric matrix, $\iota, \nu = 1, 2, \cdots, 8$, $\boldsymbol{\phi}_{11} = 2\boldsymbol{P}\boldsymbol{A} + \boldsymbol{Q}_1 + \boldsymbol{Q}_2 + \boldsymbol{Q}_3 + 2\boldsymbol{N}_1$, $\boldsymbol{\phi}_{12} = \boldsymbol{P}\boldsymbol{A}_d + \boldsymbol{N}_2 - \boldsymbol{N}_1 + \boldsymbol{S}_1 - \boldsymbol{M}_1$, $\boldsymbol{\phi}_{13} = \boldsymbol{M}_1$, $\boldsymbol{\phi}_{14} = -\boldsymbol{S}_1$, $\boldsymbol{\phi}_{15} = \tau_2\boldsymbol{N}_1$, $\boldsymbol{\phi}_{16} = \tau_{12}\boldsymbol{S}_1$, $\boldsymbol{\phi}_{17} = \tau_{12}\boldsymbol{M}_1$, $\boldsymbol{\phi}_{18} = \boldsymbol{A}_{11}\boldsymbol{v}$, $\boldsymbol{\phi}_{22} = -(1-\mu)\boldsymbol{Q}_3 + 2\boldsymbol{S}_2 - 2\boldsymbol{N}_2 - 2\boldsymbol{M}_2$, $\boldsymbol{\phi}_{23} = \boldsymbol{M}_2$, $\boldsymbol{\phi}_{24} = -\boldsymbol{S}_2$, $\boldsymbol{\phi}_{25} = \tau_2\boldsymbol{N}_2$, $\boldsymbol{\phi}_{26} = \tau_{12}\boldsymbol{S}_2$, $\boldsymbol{\phi}_{27} = \tau_{12}\boldsymbol{M}_2$, $\boldsymbol{\phi}_{28} = \boldsymbol{A}_{11d}\boldsymbol{v}$, $\boldsymbol{\phi}_{33} = -\boldsymbol{Q}_1$, $\boldsymbol{\phi}_{44} = -\boldsymbol{Q}_2$, $\boldsymbol{\phi}_{55} = -\tau_2\boldsymbol{Z}_1$, $\boldsymbol{\phi}_{66} = -\tau_{12}(\boldsymbol{Z}_1 + \boldsymbol{Z}_2)$, $\boldsymbol{\phi}_{77} = -\tau_{12}\boldsymbol{Z}_2$, $\boldsymbol{\phi}_{88} = -\boldsymbol{v}$, $\boldsymbol{\phi}_{\iota\nu} = 0$, for $\nu > \iota$ and $\iota = 3, 4, \cdots, 7$, $\boldsymbol{v} = \tau_2\boldsymbol{Z}_1 + \tau_{12}\boldsymbol{Z}_2$, and $\tau_{12} = \tau_2 - \tau_1$.

3. Fluid-Flow Model of Industrial Networks

Industrial networks interconnect various industrial control systems (ICS), e.g., local-area switched networks, such as distributed control systems, and wide-area routed networks, such as SCADA, to support the communication between devices. Most ICSs adopt some specialized protocols, such as Open Platform Communications, Modbus, Distributed Network Protocol, Inter-Control Center Protocol, Profibus, etc. However, these protocols were initially designed for serial communications and must been adapted to operate over TCP/IP networks, which is a standard Ethernet link layer and has been widely implemented at common network infrastructures. To this end, the industrial TCP/IP networks will be studied in the paper.

An industrial TCP/IP network consists of multiple hosts and clients in industrial control systems, which are physically connected in any number of topologies including star, tree, and even full-mesh. In industrial networks, a star topology is extremely common to connect to end devices [33]. So, a typical industrial TCP/IP network in a star topology is adopted in this study. In the topology, all nodes (hosts or any other industrial control systems peripherals) are connected to an industrial router. Each connected host has a dedicated, point-to-point connection between the host and the router. It is assumed that there are N homogeneous sources, i.e., all sources are the same in structure, nature, parameters, and software implementations. They connect to a destination (a host or a client devices)

through a router, where two mechanisms are embedded: an Active Queue Management (AQM) and an observer. The AQM regulates the queue length in the router buffer with a randomization of choosing connections to notify the congestion, so that the network utilization can be improved. The observer is used to estimate the traffic flow and further detect its abnormal behavior of the traffics in industrial TCP/IP networks.

To describe the behavior of the traffics in industrial networks, the following fluid-flow model of TCP behavior can be used [9]:

$$\begin{cases} \dot{w}(t) = \dfrac{1}{\tau(t)} - \dfrac{w(t)}{2}\dfrac{w(t-\tau(t))}{\tau(t-\tau(t))}p(t-\tau(t)) \\ \dot{q}(t) = N\dfrac{w(t)}{\tau(t)} - C + \delta(t) \\ \tau(t) = \dfrac{q(t)}{C} + T_p \end{cases}, \tag{7}$$

where $w(t)$ is the average TCP congestion window size in packets. Congestion Window (C_{wnd}) is a TCP state variable that limits the amount of data the TCP can send into the network before receiving an ACK. $q(t)$ is expected queue length in packets. w and q are positive and bounded, i.e., $w \in [0, \bar{w}]$ and $q \in [0, \bar{q}]$, where $\bar{w}$ and $\bar{q}$ are known and denote maximum window size and buffer size, respectively. $\tau(t)$ is the round-trip time in seconds which induces time varying delay in the communication channel. $p(t)$ is the probability of packet loss and takes value at $[0, 1]$. T_p is the propagation delay in seconds. N and C are the numbers of TCP sections and the link bandwidth in packets/second, respectively.

In system (7), $\delta(t)$ represents the unmeasurable queuing dynamics of *ATF* in the network. It includes the modeling errors and anomalies. Both of them are uncertain and perturb the normal TCP/IP network behavior at the router level. In normal working conditions, $\delta(t)$ is around a fixed value, which forms a layer near the value; however, when an anomaly intrusion happens, it will suddenly increase.

The purpose of the paper is to estimate $\delta(t)$ only using $q(t)$ in (7). After obtaining the estimate of $\delta(t)$, we can detect and further analyze the anomalies.

The equilibrium point of system (7) is assumed as (w_0, q_0), where w_0 is the equilibrium window size, and q_0 is the required queue length set by the AQM. p_0 is the equilibrium input value, and τ_0 is the equilibrium round-trip time. They can be determined as follows by $\dot{w}(t) = 0$ and $\dot{q}(t) = 0$:

$$\begin{cases} \tau_0 = q_0/C + T_p \\ w_0 = \tau_0 C/N \\ p_0 = 2\Big/w_0^2 \end{cases}.$$

The system (7) can be linearized around its equilibrium point. Defining the perturbation of the equilibrium point as $\Delta w(t) = w(t) - w_0$ and $\Delta q(t) = q(t) - q_0$, the dynamics of the industrial TCP networks (7) can be linearized to

$$\begin{cases} \Delta\dot{w}(t) = -\dfrac{N}{\tau_0^2 C}\left(\Delta w(t) + \Delta w(t-\tau(t))\right) - \dfrac{1}{\tau_0^2 C}\left(\Delta q(t)\right. \\ \qquad\qquad \left. - \Delta q(t-\tau(t))\right) - \dfrac{\tau_0 C^2}{2N^2}\Delta p(t-\tau(t)) \\ \Delta\dot{q}(t) = \dfrac{N}{\tau_0}\Delta w(t) - \dfrac{1}{\tau_0}\Delta q(t) + \delta(t) \end{cases}, \tag{8}$$

where $q(t)$ and $p(t)$ are available in the router. Some software programs, such as Netflow, PacketScope, and Loss Measurement Management, have been installed in routers. They can monitor and measure $p(t)$ [34]. The congestion window $w(t)$ cannot be used in the AQM or the observer because it is unmeasurable.

To simplify the design of the observer for the linearized model of the industrial TCP/IP network (8), a state transformation is made first.

Define a new state variable $x(t) = \Delta w(t) \in \mathbb{R}$, an output $y(t) = \Delta q(t) \in \mathbb{R}$, and a control $u(t) = \Delta p(t) \in \mathbb{R}$. Then, system (8) can be rewritten as

$$\begin{cases} \dot{x}(t) = -a_{11}x(t) - a_{11}x(t-\tau(t)) - a_{12}y(t) \\ \qquad\quad + a_{12}y(t-\tau(t)) - b_d u(t-\tau(t)) \\ \dot{y}(t) = a_{21}x(t) - a_{22}y(t) + \delta(t) \end{cases}, \tag{9}$$

where $a_{11} = N/{\tau_0}^2\, C$, $a_{12} = 1/{\tau_0}^2\, C$, $b_d = \tau_0 C^2/2N^2$, $a_{21} = N/\tau_0$, and $a_{22} = 1/\tau_0$. C and N are defined in (7).

The time-delay $\tau(t)$ in (9) satisfies the following inequality:

$$T_p \le \tau(t) \le \bar{q}/C + T_p, \tag{10}$$

where $\bar{q}$, C and T_p are defined in (7).

It should be noted that the lower bound of $\tau(t)$ is T_p as defined in (10). T_p is the propagation delay at the circumstance of neither congestion nor queuing delay in a router. In addition, the upper bound of $\tau(t)$ in (10) is the combination of the propagation delay and the maximum queuing delay under the worst case of congestion in the router buffer, i.e., $\tau(t)$, cannot exceed $\bar{q}/C + T_p$.

The derivative of $\tau(t)$ can be assumed to satisfy

$$\dot{\tau}(t) \le \mu, \tag{11}$$

where μ is a known positive constant.

The condition of (10) and (11) can be obtained as below. Differentiating the last equation in (7) with the time t gives

$$\dot{\tau}(t) = \frac{1}{C}\left(\frac{Nw(t) + \delta(t)\tau(t)}{\tau(t)} - C\right). \tag{12}$$

The term $Nw(t) + \delta(t)\tau(t)$ in (12) is actually the amount of data being transmitted in the TCP/IP network, which is physically constrained to the TCP/IP network capacities, namely $Nw(t) + \delta(t)\tau(t) \le BDP + \bar{q}$ where $\bar{q}$ is the buffer capacity defined in (7). BDP is the Bandwidth-Delay Product, which represents the amount of data that can be in transit [35]. BDP refers to the product of a data link's capacity C and its round-trip delay time $\tau(t)$, i.e., $BDP = C\tau(t)$, where C and $\tau(t)$ are defined in (7). Normally, the buffer capacity of a router in (7) $\bar{q}$ is dependent on the BDP, i.e., $\bar{q} = \mu C\tau(t)$, where $\mu = 1/\sqrt{N}$ is a constant [36]. Then, it can be obtained that $Nw(t) + \delta(t)\tau(t) \le C\tau(t) + \mu C\tau(t)$ and furthermore, we have the condition (11) is true.

The state variable $x(t)$ in the linearized model of the TCP/IP network (9) satisfies the inequality as follows:

$$|x(t)| \le \bar{w}, \tag{13}$$

where $\bar{w}$ is the known positive constant, i.e., the maximum window size, and is defined in (7).

In TCP/IP networks, the window size refers to the amount of dada that a host is currently willing to send. Normally, the maximum window size $\bar{w}$ at a host is configured as a constant, i.e., $\bar{w}$ is set as 65,535 (0xFFFF) bytes [37]. As seen as in (8) and (9), $x(t)$ is the perturbation around the equilibrium point of $w(t)$ that is limited to the known constant maximum window size $\bar{w}$. As $x(t) = \delta w(t)$, so $|x(t)|$ cannot exceed the maximum value of $w(t)$, i.e., the inequality (13) is true.

The aforementioned amount of data being transmitted in the TCP/IP network, $Nw(t) + \delta(t)\tau(t)$, in (12) includes traffic flow of all N TCP sections $Nw(t)$, as well as

the dynamics of *ATF* $\delta(t)\tau(t)$. It is physically constrained to the TCP/IP network capacities, namely $\frac{Nw(t)}{\tau(t)} + \delta(t) \leq C + \mu C$, which means that $|\delta(t)| \leq (1+\mu)C$ holds because of $w(t) > 0$, $\tau(t) > 0$, i.e., $|\delta(t)| \leq d_m$, where $d_m \leq (1+\mu)C$ is a known positive constant which can be determined in the experiments.

As $\delta(t)$ is physically limited to the router communication capacity, its change rate is always constrained to $\left|\dot{\delta}(t)\right| \leq d_m/T$, where T is the sampling period and kept as a constant $1/C$ [9]. Hence, we have $\left|\dot{\delta}(t)\right| \leq d_m/T \leq (1+\mu)C^2$, i.e., $\left|\dot{\delta}(t)\right| \leq d_1$, where $d_1 \leq (1+\mu)C^2$ is a known positive constant. Summarizing the analysis above gives

$$|\delta(t)| \leq d_m, \quad \left|\dot{\delta}(t)\right| \leq d_1, \tag{14}$$

where both d_m and d_1 are known positive constants.

The block diagram of the AQM and observer in a router is shown in Figure 1. The AQM is utilized to control the queue length $q(t)$ to a required value by regulating the probability of packets loss $p(t)$. The inputs of the observer, i.e., $q(t)$ and $p(t)$, are measurable states. The outputs of the observer is the estimate of $\delta(t)$. The paper aims to design an observer for estimating the dynamics of *ATF* in real-time and further detecting anomalies in industrial networks.

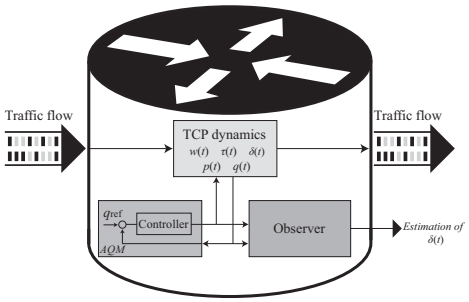

Figure 1. Block diagram of the AQM and observer in an industrial switch/router.

4. Design of the TSM Observer

In the fluid-flow model of TCP/IP networks in (9), the *ATF* dynamics $\delta(t)$ can be considered as a disturbance. The estimate of $\delta(t)$ can be used for anomaly detection. To estimate $\delta(t)$, an observer is proposed as

$$\begin{cases} \dot{\hat{x}}(t) = -a_{11}\hat{x}(t) - a_{11}\hat{x}(t-\tau(t)) - a_{12}y(t) \\ \qquad\qquad + a_{12}y(t-\tau(t)) - b_d u(t-\tau(t)) + v_1(t), \\ \dot{\hat{y}}(t) = a_{21}\hat{x}(t) - a_{22}y(t) + v_2(t) \end{cases} \tag{15}$$

where $\hat{x}(t)$ and $\hat{y}(t)$ represent the estimates of the system state $x(t)$ and output $y(t)$, respectively, and $v_1(t)$ and $v_2(t)$ are output injection for the observer.

Define $\xi_1(t) := \hat{x}(t) - x(t)$ and $\xi_2(t) := \hat{y}(t) - y(t)$ as the errors between the system states and their estimates. The error system can be obtained from (9) and (15) as follows:

$$\begin{cases} \dot{\xi}_1(t) = -a_{11}\xi_1(t) - a_{11}\xi_1(t-\tau(t)) + v_1(t) \\ \dot{\xi}_2(t) = a_{21}\xi_1(t) + v_2(t) - \delta(t) \end{cases}. \tag{16}$$

It should be noted that the state ξ_2 in error system (16) is measurable and can be used in the design of the output injection. However, the state ξ_1 is unmeasurable and cannot be used in the design of the output injection, i.e., v_1 and v_2 in (16) can include only ξ_2.

4.1. Measurable Error Subsystem

The measurable error subsystem in (16) is firstly considered, namely

$$\dot{\xi}_2(t) = a_{21}\xi_1(t) + v_2(t) - \delta(t). \tag{17}$$

A TSM manifold is chosen as the following form [38,39]:

$$s(t) = \dot{\xi}_2(t) + \alpha\xi_2(t) + \beta{\xi_2}^{\phi/\rho}(t), \tag{18}$$

where $\alpha, \beta > 0$ are constants, and ρ and ϕ are positive odd integers which satisfy $1 < \rho/\phi < 2$.

Theorem 1. *The measurable error subsystem (17) will reach the ideal sliding manifold $s(t) = 0$ firstly from any nonzero initial condition $s(0) \neq 0$ in a finite-time $t_r \leq |s(0)|/\eta_2$, then converge to zero along $s(t) = 0$ in another finite-time $t_s = \rho/(\alpha(\rho-\phi))\Big(\ln(\alpha{\xi_2}^{(\rho-\phi)/\rho}(t_r) + \beta) - \ln\beta\Big)$, if $s(t)$ is selected as (18), and the output injection is given by*

$$v_2(t) = v_{2eq}(t) + v_{2n}(t) \tag{19}$$

$$v_{2eq}(t) = -a_{21}\hat{x}(t) - \alpha\xi_2(t) - \beta\xi_2(t)^{\phi/\rho} \tag{20}$$

$$\dot{v}_{2n}(t) = -a_{12}a_{21}y(t) + a_{12}a_{21}y(t-\tau(t)) - a_{21}b_d u(t-\tau(t)) - k_2\mathrm{sgn}(s(t)), \tag{21}$$

where $k_2 = 2a_{11}a_{21}\bar{w} + d_1 + \eta_2$, $\eta_2 > 0$ is a constant, and $\bar{w}$ and d_1 are defined in (7) and (14), respectively.

Proof. From (17), the manifold (18) can be rewritten as

$$s(t) = a_{21}\xi_1(t) + v_2(t) - \delta(t) + \alpha\xi_2(t) + \beta{\xi_2}^{\phi/\rho}(t).$$

Substituting (19) and (20) into the above gives

$$s(t) = -a_{21}x(t) + v_{2n}(t) - \delta(t). \tag{22}$$

Differentiating $s(t)$ in (22) with respect to time t along the measurable error subsystem (17) yields

$$\begin{aligned}\dot{s}(t) =& -a_{21}\dot{x}(t) + \dot{v}_{2n}(t) - \dot{\delta}(t)\\ =& -a_{21}(-a_{11}x(t) - a_{11}x(t-\tau(t)) - a_{12}y(t)\\ &+ a_{12}y(t-\tau(t)) - b_d u(t-\tau(t))) + \dot{v}_{2n}(t) - \dot{\delta}(t).\end{aligned}$$

Further substituting (21) into the above equation gives

$$\begin{aligned}\dot{s}(t) =& -a_{21}(-a_{11}x(t) - a_{11}x(t-\tau(t))) - (2a_{11}a_{21}\bar{w}\\ &+ d_1 + \eta_2)\mathrm{sgn}(s(t)) - \dot{\delta}(t).\end{aligned}$$

Introduce a candidate Lyapunov function given by $V_1(t) = 0.5s^2(t)$. Taking the derivative of $V_1(t)$ along the trajectories of (16), and using the above expression, it follows that

$$\begin{aligned}s(t)\dot{s}(t) =& -a_{21}(-a_{11}x(t) - a_{11}x(t-\tau(t)))s(t)\\ &- (2a_{11}a_{21}\bar{w} + d_1 + \eta_2)|s(t)| - \dot{\delta}(t)s(t)\\ \leq& a_{21}(a_{11}|x(t)| + a_{11}|x(t-\tau(t))| - 2a_{11}\bar{w})|s(t)|\\ &+ (|\dot{\delta}(t)| - d_1)|s(t)| - \eta_2|s(t)|\end{aligned}$$

From the conditions (13), (14) and the above, we have

$$\dot{V}_1(t) = s(t)\dot{s}(t) \leq -\eta_2\sqrt{2}{V_1}^{1/2}(t) < 0, \text{ for } s(t) \neq 0;$$

it can be seen that measurable error subsystem (17) will reach to $s(t) = 0$ within the finite-time $t_r \leq |s(0)|/\eta_2$; in other words, $s(t) = 0, \forall t \geq t_r$. Once the ideal sliding-mode $s(t) = 0$ is established, the measurable error subsystem (17) will maintain on $s(t) = 0$ thereafter and behaves in an identical fashion as $\dot{\xi}_2(t) = -\alpha\xi_2(t) - \beta{\xi_2}^{\phi/\rho}(t)$, which will converge to zero along $s(t) = 0$ in the finite-time t_s. □

Theorem 1 yields a method of designing the output injection in (17) by only using the measurable $\xi_2(t)$, which forces $\xi_2(t)$ to converge to zero in a finite-time, although there exist unmeasurable $\xi_1(t)$ and unknown disturbance $\delta(t)$ in (17).

4.2. Unmeasurable Error Subsystem

For the unmeasurable error subsystem in (16), namely

$$\dot{\xi}_1(t) = -a_{11}\xi_1(t) - a_{11}\xi_1(t - \tau(t)) + v_1(t). \tag{23}$$

Define an area Γ for unmeasurable ξ_1 near zero as

$$\Gamma = \left\{\xi_1 : \left|\xi_1 - a_{21}^{-1}\delta\right| \leq \varphi\right\}, \tag{24}$$

where φ is a positive constant and defined as $\varphi = a_{21}^{-1}d_m + \varepsilon$, d_m is defined in (14), and ε is a positive constant, which can be chosen by $0 < \varepsilon < a_{21}^{-1}d_m/2$.

The purpose of introducing the area Γ is to design a output injection strategy in the following Theorem for increasing the convergence speed of the error ξ_1, when it is outside Γ.

Theorem 2. *The unmeasurable error subsystem (23) will converge to zero asymptotically, if the output injection is given by*

$$v_1(t) = \begin{cases} 0, & \left|\tilde{\xi}_1(t)\right| \leq \varphi \\ -k_1\text{sgn}(\tilde{\xi}_1(t)), & \left|\tilde{\xi}_1(t)\right| > \varphi \end{cases} \tag{25}$$

$$\tilde{\xi}_1(t) = \hat{x}(t) - a_{21}^{-1}v_{2n}(t) \tag{26}$$

where $k_1 = a_{11}\bar{w} + \eta_1$, $\bar{w}$ is a constant defined in (7), and $\eta_1 > 0$ is a constant.

Proof. The error state space of ξ_1 can be divided into two different areas, Γ_o and Γ, and defined, respectively, as $\Gamma_o = \left\{\xi_1 : \left|\xi_1 - a_{21}^{-1}\delta\right| > \varphi\right\}$ and $\Gamma = \left\{\xi_1 : \left|\xi_1 - a_{21}^{-1}\delta\right| \leq \varphi\right\}$, where $\varphi > 0$ is defined in (24). So, two different cases, i.e., Case 1 and 2, are considered.

Case 1: the error state ξ_1 is in area Γ_o. The measurable error subsystem (17) will move toward the sliding manifold $s = 0$ under the output injection (19)–(21). When the measurable error subsystem reaches and stays on the sliding manifold, $s(t) = 0$, under the output injection in Theorem 1, it follows from (22) that

$$s(t) = a_{21}\xi_1(t) - a_{21}\hat{x}(t) + v_{2n}(t) - \delta(t) = 0. \tag{27}$$

From the above equation and (26), it gives that

$$\tilde{\xi}_1(t) = \xi_1(t) - a_{21}^{-1}\delta(t). \tag{28}$$

As ξ_1 is in area Γ_o, the inequality $\left|\xi_1 - a_{21}^{-1}\delta\right| > \varphi$ holds. According to (28) and the above inequality, we can have that $\left|\tilde{\xi}_1(t)\right| > \varphi$. So, the output injection (25) can be rewritten as

$$v_1(t) = -k_1 \mathrm{sgn}\left(\tilde{\xi}_1(t)\right). \tag{29}$$

As we have that $\tilde{\xi}_1(t) = \xi_1(t) - a_{21}^{-1}\delta(t) < -\varphi < 0$, where $\varphi = a_{21}^{-1}d_m + \varepsilon$ is defined in (24), and d_m is defined in (14), further, we can obtain that $\xi_1(t) < -\varphi + a_{21}^{-1}\delta(t) = -a_{21}^{-1}(d_m - \delta(t)) - \varepsilon < 0$. For the case of $\tilde{\xi}_1(t) = \xi_1(t) - a_{21}^{-1}\delta(t) > \varphi > 0$, similarly, we can have that $\xi_1(t) > a_{21}^{-1}(d_m + \delta(t)) + \varepsilon > 0$. So, it can be concluded that

$$\mathrm{sgn}\left(\tilde{\xi}_1(t)\right) = \mathrm{sgn}(\xi_1(t)). \tag{30}$$

According to the above equation, the output injection (29) can be rewritten as

$$v_1(t) = -k_1 \mathrm{sgn}(\xi_1(t)); \tag{31}$$

further substituting (31) into (23), the unmeasurable error subsystem (23) can be reformed as

$$\dot{\xi}_1(t) = -a_{11}\xi_1(t) - a_{11}\xi_1(t - \tau(t)) - k_1 \mathrm{sgn}(\xi_1(t)). \tag{32}$$

Consider a candidate Lyapunov function $V_2(t) = 0.5\xi_1^2(t)$. Taking the time-derivative of $V_2(t)$ yields

$$\begin{aligned} \dot{V}_2 =& \xi_1(t)\dot{\xi}_1(t) = -a_{11}\xi_1^2(t) - a_{11}\xi_1(t - \tau(t))\xi_1(t) \\ & - k_1|\xi_1(t)| \\ \leq & -\eta_1|\xi_1(t)| < 0, \text{ for } |\xi_1(t)| \neq 0, \end{aligned}$$

which means that, in Case 1, the error state ξ_1 in area Γ_o must converge into the area Γ in a finite-time.

Case 2: ξ_1 is in area Γ. The inequality $\left|\xi_1 - a_{21}^{-1}\delta\right| \leq \varphi$ holds. According to (28) and the above inequality, it can be obtained that $\left|\tilde{\xi}_1(t)\right| \leq \varphi$. Therefore, the output injection (25) becomes $v_1(t) = 0$, and the system (23) is rewritten as

$$\dot{\xi}_1(t) = -a_{11}\xi_1(t) - a_{11}\xi_1(t - \tau(t)). \tag{33}$$

To prove the stability of the system (33), consider the Lyapunov function [32] as

$$\begin{aligned} V_3 =& g\xi_1^2(t) + h_1 \int_{t-T_p}^{t} \xi_1^2(s)ds + h_2 \int_{t-(\bar{q}/C+T_p)}^{t} \xi_1^2(s)ds \\ & + h_3 \int_{t-\tau(t)}^{t} \xi_1^2(s)ds + \int_{-(\bar{q}/C+T_p)}^{0} \int_{t+\theta}^{t} z_1\dot{\xi}_1^2(s)d\theta \\ & + \int_{-(\bar{q}/C+T_p)}^{-T_p} \int_{t+\theta}^{t} z_2\dot{\xi}_1^2(s)d\theta \end{aligned},$$

where g, h_i, for $i = 1, 2, 3$, and z_j, for $j = 1, 2$, are all positive constants to be determined.

Define $X = [\xi_1(t), \xi_1(t - \tau(t)), \xi_1(t - T_p), \xi_1(t - (\bar{q}/C + T_p))]^T$, $A = [-a_{11}, -a_{11}, 0, 0]^T$, and $\Phi = [\phi_{\iota\nu}]_{4\times4}$ is the symmetric matrix, where $\iota, \nu = 1, 2, \cdots, 4$, $\phi_{11} = -2ga_{11} + h_1 + h_2 + h_3 + 2n_1$, $\phi_{12} = -2ga_{11} + n_2 - n_1 + s_1 - m_1$, $\phi_{13} = m_1$, $\phi_{13} = -s_1$, $\phi_{22} = -(1 - \mu)h_3 + 2s_2 - 2n_2 - 2m_2$, $\phi_{23} = m_2$, $\phi_{24} = -s_2$, $\phi_{33} = -q_1$, $\phi_{34} = 0$, $\phi_{44} = -q_2$, $M = [m_1, m_2, 0, 0]^T$, $N = [n_1, n_2, 0, 0]^T$, $S = [s_1, s_2, 0, 0]^T$, and γ is a sufficient small positive value.

Differentiating $V_3(t)$ with respect to time t along the error subsystem (33) gives

$$\begin{aligned}\dot{V}_3 =& 2g\xi_1(t)\dot{\xi}_1(t) + h_1\Big({\xi_1}^2(t) - {\xi_1}^2(t-T_p)\Big) + h_2({\xi_1}^2(t) \\ & - {\xi_1}^2\Big(t-(\bar{q}/C+T_p)\Big)\Big) - (1-\dot{\tau}(t))h_3{\xi_1}^2(t-\tau(t))) \\ & + (\bar{q}/C+T_p)z_1\dot{\xi}_1^2(t) + \tfrac{\bar{q}}{C}z_2\dot{\xi}_1^2(t) + h_3{\xi_1}^2(t) \\ & - z_1\int_{t-(\bar{q}/C+T_p)}^{t}\dot{\xi}_1^2(s)ds - \int_{t-(\bar{q}/C+T_p)}^{t-T_p} z_2\dot{\xi}_1^2(s)ds \\ \\ \leq & X^T\Big[\Phi + A\Big((\bar{q}/C+T_p)z_1 + \tfrac{\bar{q}}{C}z_2\Big)A^T + \tfrac{\bar{q}}{C}Mz_2{}^{-1}M^T \\ & + (\bar{q}/C+T_p)Nz_1{}^{-1}N^T + \tfrac{\bar{q}}{C}S(z_1+z_2)^{-1}S^T\Big]X \\ & - \int_{t-(\bar{q}/C+T_p)}^{t-\tau(t)}(z_1+z_2)^{-1}\Big[X^TS + \dot{\xi}_1(s)(z_1+z_2)\Big] \\ & \times\Big[S^TX + (z_1+z_2)\dot{\xi}_1(s)\Big]ds \\ & - \int_{t-\tau(t)}^{t} z_1{}^{-1}\Big[X^TN + \dot{\xi}_1(s)z_1\Big]\Big[N^TX + z_1\dot{\xi}_1(s)\Big]ds \\ & - \int_{t-\tau(t)}^{t-T_p} z_2{}^{-1}\Big[X^TM + \dot{\xi}_1(s)z_2\Big]\Big[M^TX + z_2\dot{\xi}_1(s)\Big]ds\end{aligned}$$

From (6) in Lemma 2 and the above inequality, it can be obtained as

$$\dot{V}_3 < -\gamma|\xi_1(t)|^2 < 0, \tag{34}$$

which ensures the asymptotic stability of the error system (33), i.e., $\xi_1(t)$, will converge to zero asymptotically.

The state space of ξ_1 can be divided into two different areas, Γ_o and Γ. In Case 1, when the state ξ_1 is in Γ_0, the output injection strategies (25)–(26) drive the error system (32) converging to the area Γ in a finite time. Once the state ξ_1 reached and entered the area Γ, namely Case 2 occurred, and the error system (33) will converge to zero asymptotically. That means the the unmeasurable error subsystem (23) will converge to zero asymptotically. □

Remark 1. *In practice, the output injection strategies (25)–(26) are implemented by* $\prod_{-\sigma,\sigma}(s) \times v_1$, *where* $\prod_{-\sigma,\sigma}(s)$ *is a boxcar function and expressed by*

$$\prod\nolimits_{-\sigma,\sigma}(s) = \begin{cases} 1, & |s| \leq \sigma \\ 0, & |s| > \sigma \end{cases},$$

where $\sigma > 0$ *is a constant.*

The whole state space of ξ_1 *and* ξ_2 *can be divided into two different areas,* Ω_1 *and* Ω_2, *defined as* $\Omega_1 = \{(\xi_1, \xi_2) : |s| > \sigma\}$ *and* $\Omega_2 = \{(\xi_1, \xi_2) : |s| \leq \sigma\}$.

When the system states ξ_1, ξ_2 *are in* Ω_1, *the boxcar function* $\prod_{-\sigma,\sigma}(s) = 0$, *and then* $v_1(t)$ *in (25) is equal to zero, which means that the measurable error subsystem (17) has not reached to the sliding manifold* $s(t) = 0$. *In this case, the output injection (25) has not been applied in the unmeasurable error subsystem (23).*

The measurable error subsystem (17) will move toward the sliding manifold $s = 0$ *under the output injection (19)–(21). Once it reaches to* $s = 0$, *the system states* ξ_1, ξ_2 *enter into the area* $\Omega_2 = \{(\xi_1, \xi_2) : |s| \leq \sigma\}$. σ *is selected as a small constant for practical implementation.*

The output injection strategies (19)–(21) in Theorem 1 drive the error subsystem (17) toward the sliding manifold $s = 0$ *and remain on the manifold thereafter, which guarantees the system states* ξ_1, ξ_2 *to converge into the area* Ω_2 *in a finite-time. Then, the unmeasurable error system (23) will converge to zero asymptotically.*

In ideal condition, $\sigma = 0$, i.e., the ideal sliding-mode $s = 0$ can be detected. However, in practical environments, detecting ideal $s = 0$ is not possible. So, we can just only detect an area near zero, $|s| < \sigma$. In this case, substituting (19) and (20) into (18), we have $a_{21}\xi_1(t) - \delta(t) = a_{21}\hat{x}(t) - v_{2n}(t) + s(t)$, where $|s(t)| < \sigma$. Hence, it can be chosen σ as $\sigma = \kappa|a_{21}\tilde{\xi}_1(t)|$, where $\kappa = 0.02 - 0.05$. It should be noted that σ can affect only the convergence speed in dynamical process but cannot affect the final observation.

Theorem 3. *If the two output injection signals in the error system (16) are designed using Theorems 1 and 2, respectively, the estimation errors $\lim_{t\to(t_r+t_s)} \xi_2(t) = 0$ and $\lim_{t\to\infty} \xi_1(t) = 0$. Then, the ATF dynamics $\delta(t)$ in (9) can be estimated by as*

$$\lim_{t\to\infty} v_2(t) = \lim_{t\to\infty} \delta(t), \tag{35}$$

where $v_2(t)$ is designed in (19).

Proof. Based on Theorem 1, the measurable error subsystem (16) under the output injection (19) will reach to the sliding manifold $s(t) = 0$ in the finite-time t_r and maintain on $s(t) = 0$ thereafter. The unmeasurable error subsystem (17) will converge to zero in the finite-time along $s(t) = 0$. Then, it follows from (17) that

$$\dot{\xi}_2(t) = a_{21}\xi_1(t) + v_2(t) - \delta(t) = 0. \tag{36}$$

From Theorem 2, the unmeasurable error state $\xi_1(t)$ under the output injection (25) will converge to zero asymptotically. From (36), the *ATF* dynamics $\delta(t)$ can be estimated directly by the smooth $v_2(t)$ in (19) when the unmeasurable error state $\xi_1(t)$ converges to zero asymptotically. This completes the proof. □

5. Real Traffic Replay Results

The real traffic replay results are given to varify the effectiveness of the proposed TSMO method in real-time.

5.1. Real Traffic Replay Setup

For experimental purposes, we used the real traffic dataset from CAIDA, which is governed by the Regents of the University of California and located at the University of California San Diego (UCSD) [40].

In the paper, the CAIDA "DDoS Attack 2007" dataset is used to test the proposed method. This dataset contains approximately one hour of anonymized traffic traces from a DDoS attack on 4 August 2007 (20 : 50 : 08 UTC to 21 : 56 : 16 UTC). The DDoS attack attempts to disrupt access to the targeted server and all of the bandwidth of the network connecting the server to the Internet, by consuming computing resources on the server. The 1-h trace is split up into 5-min pcap files, where pcap is an application programming interface for capturing network traffic. The total uncompressed size of the dataset is 21 GB. The traces only include attack traffic to the victim and responses to the attack from the victim. The non-attack traffic in the traces has been removed as much as possible. Traces in this dataset are anonymized using CryptoPAn prefix-preserving anonymization using a single key. The payload has been removed from all packets. These traces can be read with any software that reads the format of packet capture (pcap), including the CoralReef Software Suite, Tcpdump, Wireshark, and many others. The details of traffic features are shown in Table 1. In this experiment, the real-time DDoS attack scenarios for the CAIDA datasets are considered. This collection groups the backscatter datasets, which were created from the massive amount of data continuously collected from the UCSD Network Telescope.

To study the network traffic behavior, a network simulator is used to set up network environments. It is a discrete event-based network simulator for networking research,

which contains the necessary features, e.g., a traffic trace generator, to replay the real traffic traces profiles.

Table 1. Traffic features of Caida "DDoS Attack 2007" dataset [40].

Maximum capture length for interface	0:65,000
First timestamp:	1,186,260,576.487629
Last timestamp:	1,186,260,876.482457
Unknown encapsulation:	0
IPv4 bytes:	37,068,253
IPv4 pkts:	166,448
IPv4 traffic:	8079
Unique IPv4 addresses:	136
Unique IPv4 source addresses:	132
Unique IPv4 destination addresses:	136
Unique IPv4 TCP source ports:	4270
Unique IPv4 TCP destination ports:	3348
Unique IPv4 UDP source ports:	1
Unique IPv4 UDP destination ports:	1
Unique IPv4 ICMP type/codes:	2

A typical star topology of the TCP/IP network consisting of a number of hosts and clients with one network gateway is considered in the study. There are N source agents and destination agents being created to represent the hosts and clients in the network, respectively, where $N = 60$. The '*newreno tcp*' agents are used for the sources with '*ftp*' connections to generate long-lived TCP flows to the destination clients. The maximum value of C_{wnd} in each '*tcp*' agent is set to be the same as 0.12 Mb. The link capacity C of the network gateway router is set to be 15 Mb. Moreover, the packet size is set to be 500 bytes. The connections between each host/client and the router are set by '*full-duplex*', which construct bi-directional links at propagation delay $T_p = 200$ ms. The proportional integral (PI) *AQM* mechanism is applied to regulate the queue length (QL) at a desired value of $q_0 = 175$ packets in router buffer [41]. The capacity of router buffer $\bar{q}$ is set to be 800 packets. A traffic trace generates payload bursts according to the given trace file of the DDoS attack profile from the CAIDA Dataset. In the network simulator, traffic trace is implemented by using the C++ class '*TrafficTrace*', which is bound to the specified real DDoS attack traffic trace file in the OTcl domain.

A hundred distributed attackers are created and attached with the real traffic trace files from the CAIDA datasets. In the paper, an increasing rate attack profile of the CAIDA DDoS 2007 datasets is used to test the proposed method. This DoS attack lasts a period of five min.

The parameters in the linearized TCP/IP network model (9) are: $a_{11} = 0.2630$, $a_{12} = 0.0044$, $b_d = 481.7708$, $a_{21} = 243.2432$, and $a_{22} = 4.0541$.

5.2. Real Traffic Replay Results and Discussion

Figures 2–7 depict the experimental results of the proposed TSMO-based NTM in the scenarios of CAIDA Dataset-6 and Dataset-11. Figures 2 and 5 shows the traffic dynamics of QL captured at the router, which includes the normal traffic flows and the DDoS attack profiles. With simple observations at this traffic dynamics of QL, the anomalies displayed in the traffic dynamics cannot be identified and detected in real-time. By contrast, the TSMO-based real-time NTM scheme, which is implemented at the router, is capable to extract TCP traffic flows from the total traffic dynamics in the buffer and estimate the dynamics of *ATF* for anomaly detection.

As the Theorem 1, the measurable error subsystem (17) will reach to the predesigned manifold (18), i.e., $s(t) = 0$, within the finite-time t_r. Therefore the estimation error ξ_2 of

QL is governed by the output injection (19) to converge to zero in the finite-time t_s along $s(t) = 0$.

In addition to forcing the estimation error ξ_2 to zero in the finite-time, the other aim is to speed up the convergence of the internal dynamics of the error system (16) for precision estimation to meet the real-time criteria. By Theorem 2, the internal dynamics, i.e., the estimation error ξ_2, is forced to the defined area (24) in the finite-time and then converges to zero asymptotically. As presented in Figures 3 and 6, the congestion window is accurately estimated, which reflects the serious degradations in sending rate, throuput and bandwidth utilization in the networks when the DDoS attacks started in the scenario. From the Theorem 3, the dynamics of ATF, i.e., $\delta(t)$, which is represented by the increasing rate attack profile and the subgroup attack profile from the CAIDA datasets, is quickly and exactly estimated. The results of the estimated dynamics of DDoS rate are depicted in Figures 4 and 7.

As the experimental results illustrated in Figures 2 to 7, the proposed TSMO-based NTM presents a good tracking performances of the real traffic trace profile for anomaly detection with the main features of the SMC systems. This real traffic replay experimental results demonstrated the effectiveness and efficiency of the proposed TSMO algorithms in a real-time monitoring capability under real traffic profile environments.

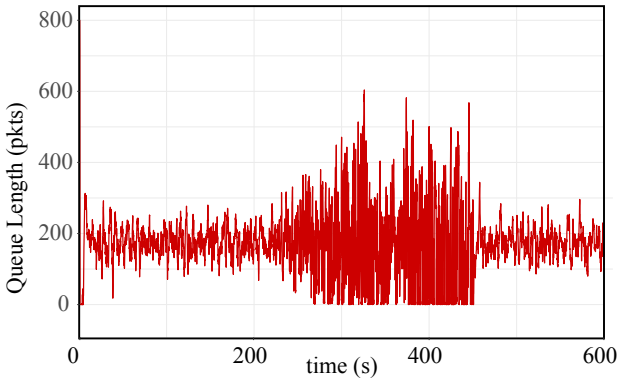

Figure 2. Queue length measured in router buffer in increasing rate attack profile of CAIDA Dataset-6.

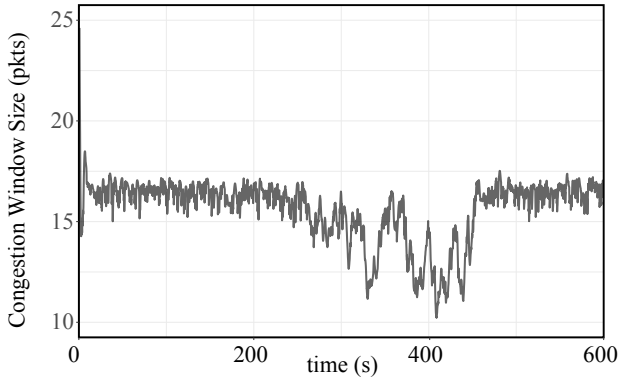

Figure 3. Estimation of C_{wnd} in increasing rate attack profile of CAIDA Dataset-6.

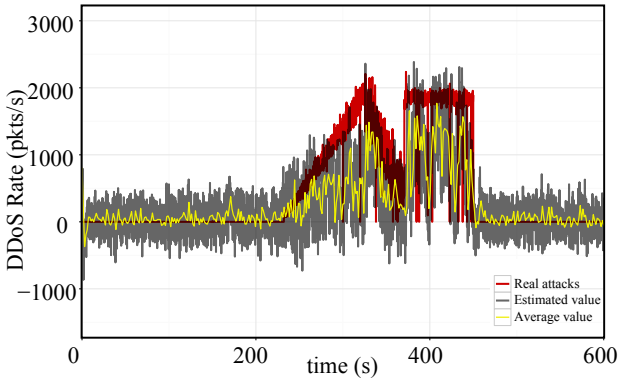

Figure 4. Estimation of attack rate in increasing rate attack profile of CAIDA Dataset-6.

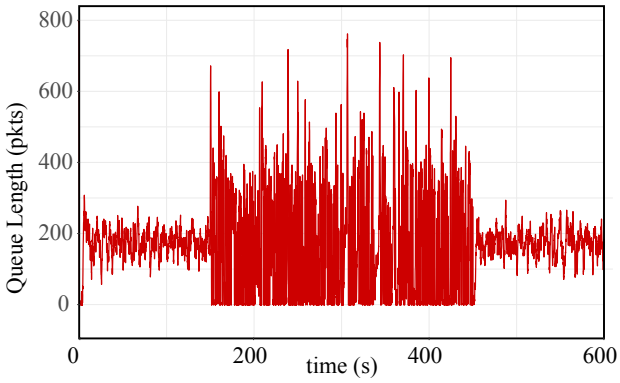

Figure 5. Queue length measured in router buffer in increasing rate attack profile of CAIDA Dataset-11.

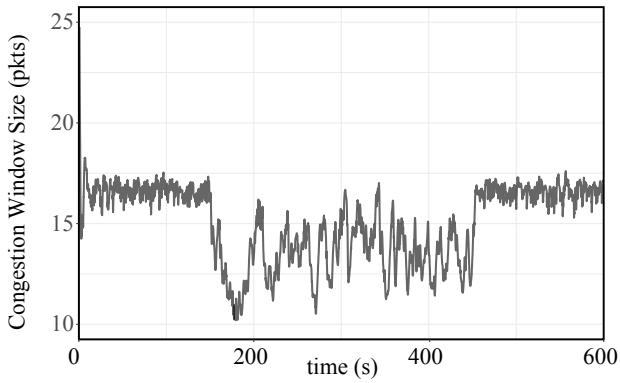

Figure 6. Estimation of C_{wnd} in increasing rate attack profile of CAIDA Dataset-11.

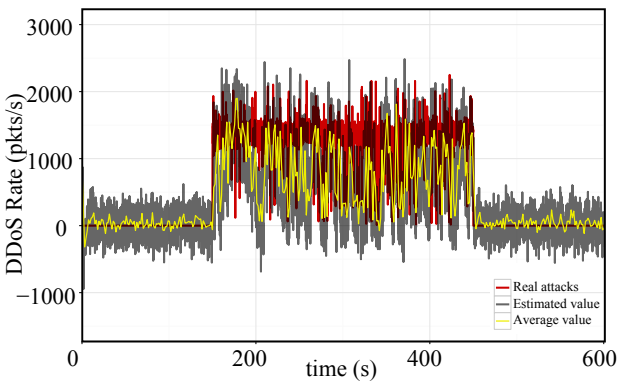

Figure 7. Estimation of attack rate in increasing rate attack profile of CAIDA Dataset-11.

5.3. Comparative Studies

Four different observer algorithms are evaluated in the real traffic replay tests.

5.3.1. The Luenberger Observer (LO)

The output injection strategies of the LO can be designed as [12]:

$$\begin{cases} v_1^{\mathrm{lo}}(t) = -L_1^{\mathrm{lo}}(y(t) - \hat{y}_{\mathrm{lo}}(t)), \\ v_2^{\mathrm{lo}}(t) = -L_2^{\mathrm{lo}}(y(t) - \hat{y}_{\mathrm{lo}}(t)), \end{cases}$$

where $\hat{y}_{\mathrm{lo}}(t)$ is the estimate of $y(t)$ in (9), $v_1^{\mathrm{lo}}(t)$ and $v_2^{\mathrm{lo}}(t)$ are the output injection signals of the observer, and L_1^{lo} and L_2^{lo} are the gains of the output injection.

5.3.2. The Conventional Sliding Mode Observer (CSMO)

The CSMO chooses the linear sliding surface by the following:

$s_{\mathrm{csmo}}(t) = c_{\mathrm{csmo}}\xi_2^{\mathrm{csmo}}(t)$, where $c_{\mathrm{csmo}} > 0$ is a constant, and the estimation error $\xi_2^{\mathrm{csmo}}(t)$ is defined by $\xi_2^{\mathrm{csmo}}(t) = \hat{y}^{\mathrm{csmo}}(t) - y(t)$. The output injection $v_1^{\mathrm{csmo}}(t)$ is equal to zero, and the output injection $v_2^{\mathrm{csmo}}(t)$ is designed as [21]:

$$v_2^{csmo}(t) = L_{\mathrm{csmo}}\xi_2^{\mathrm{csmo}}(t) - k_{\mathrm{csmo}}\mathrm{sgn}(s_{\mathrm{csmo}}(t)),$$

with $L_{\mathrm{csmo}} < 0$, $k_{\mathrm{csmo}} > 0$ is the gain of the output injection.

As highly frequent switching phenomenon existed in $v_2^{csmo}(t)$ due to the signum function, a low-pass filter is needed to extract the equivalent signal.

5.3.3. The Super-Twisting Observer (STO)

A sliding-mode surface is selected as $s_{\mathrm{sto}}(t) = \xi_2^{\mathrm{sto}}(t)$, where $\xi_2^{\mathrm{sto}}(t) = \hat{y}^{\mathrm{sto}}(t) - y(t)$. The $v_1^{\mathrm{sto}}(t)$ is equal to zero, and the $v_2^{\mathrm{sto}}(t)$ is designed by [22]:

$$\begin{cases} v_2^{\mathrm{sto}}(t) = -k_1^{sto}|s_{\mathrm{sto}}(t)|^{0.5}\mathrm{sgn}(s_{\mathrm{sto}}(t)) + v_{2n}^{\mathrm{sto}}(t) \\ \dot{v}_{2n}^{\mathrm{sto}}(t) = -k_2^{sto}\mathrm{sgn}(s_{\mathrm{sto}}(t)) \end{cases},$$

where both k_1^{sto} and k_2^{sto} are positive constant.

5.3.4. The Terminal Sliding Mode Observer (TSMO)

The output injection strategies of the proposed TSMO are designed using Theorem 1 and 2.

Four observers are implemented as: (1). The parameters of the LO are designed as $L_1^{\mathrm{lo}} = 5$ and $L_2^{\mathrm{lo}} = 32$, and (2). for the CSMO, the parameters are designed as: $c_{\mathrm{csmo}} = 20$, $L_{\mathrm{csmo}} = -100$, and $k_{\mathrm{csmo}} = 1600$. (3). The parameters of the STO are chosen as $k_1^{\mathrm{sto}} = 100$ and $k_2^{\mathrm{sto}} = 1600$. (4). The proposed TSMO: $\alpha = 15$, $\beta = 5$, $\rho = 5$, $\phi = 3$, $k_1 = 7.5$, and $k_2 = 1600$.

In order to make a fair comparison, the parameters of the four types of observer schemes are repeatedly tested, and, thereby, the optimal parameters are obtained. In the processing, the tradeoff between the dynamic performances and the steady-state performances of the closed-loop error system is made. In this condition, the convergence speed and steady-state performances are compared each other for these observers.

To make the quantitative comparisons among the four kinds of observer algorithms in terms of the steady-state performances of closed-loop error systems, Table 2 provides the average displacement error (ADE) and the standard deviation of displacement error (SDE) in the scenario. From the comparative results in Table 2, the proposed TSMO features the fastest dynamical response and the best steady-state accuracies of estimating $w(t)$ and $\delta(t)$ compared to other existing three observers.

Table 2. Comparisons of steady-state performances of four observers in scenario I.

Observers		LO	CSMO	STO	TSMO
t_r (sec)		/	4.2	2.5	2.1
t_s (sec)		/	Asymptoticaly	Asymptoticaly	2.2
ξ_1 (pkt/s)	ADE	1.97	1.97	1.97	0.73
	SDE	2.15	2.15	2.15	2.16
ξ_2 (pkt/s)	ADE	6.36	35.36	3.26	0.50
	SDE	21.68	48.03	50.56	14.44
e_{ATF} (pkt/s)	ADE	829.43	1092.28	562.18	267.51
	SDE	780.45	616.56	267.61	273.54

6. Conclusions

This paper has proposed an SMO-based network traffic monitoring approach to estimate the *ATF* dynamics. The main contributions of this work can be summarized as follows: (i) One output injection of the observer is specially designed to be smooth using the full-order SMC technique. It can be directly used for the estimation of traffic flows in real time, does not need any low-pass filter. (ii) The novel strategy for another output injection of the observer is proposed to increase the convergence speed of the internal dynamics of the observer, which can improve the speed of the estimation algorithms. (iii) The proposed TSMO can be used for a class of linear systems with time-varying delay where some system states are unmeasurable. For the proposed observer, the parameters in the algorithms are to be carefully set. The experimental results have verified the efficiency of the proposed TSMO by comparative studies in real traffic profiles from the CAIDA DDoS attack datasets. The future work will focus on anomaly detection applications considering the multiple area communication networks.

Author Contributions: Conceptualization, L.X.; Data curation, L.X. and W.X.; Formal analysis, L.X. and M.Z.; Funding acquisition, L.X. and W.X.; Investigation, L.X.; Methodology, L.X. and M.Z.; Project administration, L.X.; Resources, L.X.; Software, L.X. and W.X.; Supervision, L.X.; Validation, L.X. and L.C.; Visualization, L.X.; Writing—original draft, L.X.; Writing—review & editing, L.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China under Grant No. 62003086, and by Shanghai Pujiang Program under Grant No. 21PJ1422000, and by Guangdong Basic and Applied Basic Research Foundation under Grant No. 2020A1515110148, and by Heilongjiang Industrial Revitalization Major Project on Engineering and Science under Grant No. 2019ZX02A01.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Yan, Q.; Huang, W.; Luo, X.; Gong, Q.; Yu, F.R. A multi-level DDoS mitigation framework for the industrial internet of things. *IEEE Commun. Mag.* **2018**, *56*, 30–36. [CrossRef]
2. Sarker, I.H.; Abushark, Y.B.; Alsolami, F.; Khan, A.I. Intrudtree: A machine learning based cyber security intrusion detection model. *Symmetry* **2020**, *12*, 754. [CrossRef]
3. Zegzhda, D.; Lavrova, D.; Pavlenko, E.; Shtyrkina, A. Cyber attack prevention based on evolutionary cybernetics approach. *Symmetry* **2020** , *12*, 1931. [CrossRef]
4. Faisal, M.A.; Aung, Z.; Williams, J.R.; Sanchez, A. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study. *IEEE Syst. J.* **2015**, *9*, 31–44. [CrossRef]

5. Yang, Y.; McLaughlin, K.; Sezer, S.; Littler, T.; Im, E.G. Multiattribute SCADA-specific intrusion detection system for power networks. *IEEE Trans. Power Del.* **2014**, *29*, 1092–1102. [CrossRef]
6. Skybakmoen, T. *Next Generation Firewall Comparative Analysis- Security*; NSS Labs: Austin, TX, USA, 2014; pp. 1–20.
7. Niu, Y.; Ho, D.W.C. Design of sliding mode control subject to packet losses. *IEEE Trans. Autom. Control* **2010**, *55*, 2623–2628. [CrossRef]
8. Zhang, S.S.; Shang, W.L.; Wan, M.; Zhang, H.; Zeng, P. Security defense module of Modbus TCP communication based on region/enclave rules. *Comput. Eng. Des.* **2014**, *35*, 3701–3707.
9. Misra, V.; Gong, W.; Towsley, D. Fluid-based analysis of a network of AQM routers supporting TCP flows with an application to RED. *Comput. Commun. Rev.* **2000**, *30*, 151–160. [CrossRef]
10. Ariba, Y.; Gouaisbaut, F.; Labit, Y. 'Feedback control for router management and TCP/IP network stability. *IEEE Trans. Netw. Service Manag.* **2009**, *6*, 255–266. [CrossRef]
11. Hollot, C.V.; Misra, V.; Towsley, D.; Gong, W. Analysis and design of controllers for AQM routers supporting TCP flows. *IEEE Trans. Autom. Control* **2002**, *47*, 945–959. [CrossRef]
12. Ariba, Y.; Gouaisbaut, F.; Rahme, S.; Labit, Y. Traffic monitoring in transmission control protocol/active queue management networks through a time-delay observer. *IET Control Theory Appl.* **2012**, *6*, 506–517. [CrossRef]
13. Cao, L.; Li, H.; Wang, N.; Zhou, Q. Observer-based event-triggered adaptive decentralized fuzzy control for nonlinear large-scale systems. *IEEE Trans. Fuzzy Syst.* **2018**, *27*, 1201–1214. [CrossRef]
14. Wang, Y.; Xie, X.; Chadli, M.; Xie, S.; Peng, Y. Sliding mode control of fuzzy singularly perturbed descriptor systems. *IEEE Trans. Fuzzy Syst.* 2020, early access. [CrossRef]
15. Hou, H.; Yu, X.; Xu, L.; Restam, K.; Cao, Z. Finite-time continuous terminal sliding mode control of servo motor systems. *IEEE Trans. Ind. Electron.* **2020**, *67*, 5647–5656. [CrossRef]
16. Hou, H.; Yu, X.; Fu, Z. Sliding-mode control of uncertain time-varying systems with state delays: A non-negative constraints approach. *IEEE Trans. Syst. Man, Cybern. Syst.* **2020**, early access. [CrossRef]
17. Xu, W.; Qu, S.; Zhao, L.; Zhang, H. An Improved Adaptive Sliding Mode Observer for Middle- and High-Speed Rotor Tracking. *IEEE Trans. Power Electron.* **2021**, *36*, 1043–1053. [CrossRef]
18. Gong, C.; Hu, Y.; Gao, J.; Wang, Y.; Yan, L. An improved delay-suppressed sliding-mode observer for sensorless vector-controlled PMSM. *IEEE Trans. Ind. Electron.* **2021**, *67*, 5913–5923. [CrossRef]
19. Li, H.; Shi, P.; Yao, D. Adaptive Sliding-Mode Control of Markov Jump Nonlinear Systems with Actuator Faults. *IEEE Trans. Autom. Control* **2017**, *62*, 1933–1939. [CrossRef]
20. Wang, Y.; Gao, Y.; Karimi, H.R.; Shen, H.; Fang, Z. Sliding Mode Control of Fuzzy Singularly Perturbed Systems With Application to Electric Circuit. *IEEE Trans. Syst. Man, Cybern. Syst.* **2018**, *48*, 1667–1675. [CrossRef]
21. Rahme, S.; Labit, Y.; Gouaisbaut, F. Sliding mode observer for anomaly detection in TCP/AQM networks. In Proceedings of the IEEE Second International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ'2009), Colmar, France, 20–25 July 2009; pp. 113–118.
22. Rahme, S.; Labit, Y.; Gouaisbaut, F.; Floquet, T. Sliding modes for anomaly observation in TCP networks: From theory to practice. *IEEE Trans. Control Syst. Technol.* **2013**, *21*, 1031–1038. [CrossRef]
23. Hou, H.; Yu, X.; Xu, L.; Chuei, R.; Cao, Z. Discrete-time terminal sliding-mode tracking control with alleviated chattering. *IEEE ASME Trans. Mechatron* **2019**, *24*, 1808–1817. [CrossRef]
24. Hou, H.; Yu, X.; Fu, Z. Sliding mode control of networked control systems: An auxiliary matrices-based approach. *IEEE Trans. Autom. Control* 2021, early access. [CrossRef]
25. Yang, H.; Yin, S. Reduced-Order Sliding-Mode-Observer-Based Fault Estimation for Markov Jump Systems. *IEEE Trans. Autom. Control* **2019**, *64*, 4733–4740. [CrossRef]
26. Chen, S.; Zhang, X.; Wu, X.; Tan, G.; Chen, X. Sensorless Control for IPMSM Based on Adaptive Super-Twisting Sliding-Mode Observer and Improved Phase-Locked Loop. *Energies* **2019**, *12*, 1225. [CrossRef]
27. Zheng, W.; Xia, B.; Wang, W.; Lai, Y.; Wang, M.; Wang, H. State of Charge Estimation for Power Lithium-Ion Battery Using a Fuzzy Logic Sliding Mode Observer. *Energies* **2019**, *12*, 2491. [CrossRef]
28. Khalil, H.K.; Praly, L. High-gain observers in nonlinear feedback control. *Int. J. Robust. Nonlinear Control.* **2014**, *24*, 993–1015. [CrossRef]
29. Beltran-Carbajal, F.; Valderrabano-Gonzalez, A.; Favela-Contreras, A.R.; Rosas-Caro, J.C. Active disturbance rejection control of a magnetic suspension system. *Asian J. Control* **2015**, *17*, 842–854. [CrossRef]
30. Kim, K.S.; Rew, K.H.; Kim, S. Disturbance observer for estimating higher order disturbances in time series expansion. *IEEE Trans. Autom. Control* **2015**, *17*, 842–854.
31. Bhat, S.P.; Bernstein, D.S. Finite-time stability of continuous autonomous systems *SIAM J. Control Optim.* **2000**, *38*, 751–766. [CrossRef]
32. He, Y.; Wang, Q.; Linb, C.; Wua, M. Delay-range-dependent stability for systems with time-varying delay. *Automatica* **2007**, *43*, 371–376. [CrossRef]
33. Hatzivasilis, G.; Fysarakis, K.; Soultatos, O.; Askoxylakis, I.; Demetriou, G. The Industrial Internet of Things as an enabler for a Circular Economy Hy-LP: A novel IIoT protocol, evaluated on a wind park's SDN/NFV-enabled 5G industrial network. *Comput. Commun.* **2018**, *119*, 127–137. [CrossRef]

34. Chuck, F.; Moon, S.; Lyles, B.; Cotton, C.; Khan, M.; Moll, D.; Rockell, R.; Seely, T.; Diot, S.C. Packet level traffic measurements from the sprint IP backbone. *IEEE Netw.* **2003**, *17*, 6–16.
35. Jacobson, V.; Braden, R.T. TCP extensions for long-delay paths. Network Working Group Request for Comments: 1072. 1988. Available online: https://www.rfc-editor.org/info/rfc1072 (accessed on 17 May 2020)
36. Appenzeller, G.; Keslassy, I.; McKeown, N. Sizing router buffers. *Comput. Commun. Rev.* **2004**, *34*, 281–292. [CrossRef]
37. Stevens, W. TCP slow start, congestion avoidance, fast retransmit, and fast recovery algorithms. Network Working Group Request for Comments: 2001. 1996. Available online: https://datatracker.ietf.org/doc/html/rfc2001 (accessed on 17 May 2020)
38. Feng, Y.; Yu, X.; Man, Z. Non-singular terminal sliding mode control of rigid manipulators. *Automatica* **2002**, *38*, 2159–2167. [CrossRef]
39. Feng, Y.; Han, F.; Yu, X. Chattering free full-order sliding-mode control. *Automatica* **2014**, *50*, 1310–1314. [CrossRef]
40. The CAIDA UCSD "DDoS Attack 2007" Dataset. Available online: https://www.caida.org/data/passive/ddos-20070804_dataset.xml (accessed on 17 May 2020)
41. Hollot, C.V.; Misra, V.; Towsley, D.; Gong, W. On designing improved controllers for AQM routers supporting TCP flows. In Proceedings of the IEEE INFOCOM' 2001, Anchorage, AK, USA, 24–26 April 2001, Volume 3, pp. 1726–1734.