machines

MDPI

Article

Adaptive Sliding Mode Resilient Control of Multi-Robot Systems with a Leader–Follower Model under Byzantine Attacks in the Context of the Industrial Internet of Things

Muhammad Nasir and Ananda Maiti *

School of ICT, University of Tasmania, Invermay 7248, Australia; muhammad.nasir@utas.edu.au
* Correspondence: anandamaiti@live.com

Abstract: In this paper, an adaptive and resilient consensus control mechanism for multi-robot systems under Byzantine attack, based on sliding mode control, is proposed. The primary aim of the article is to develop a finite-time consensus control strategy even in the presence of a Byzantine attack. In the start, a finite-time consensus control mechanism is proposed to identify the essential conditions required for ensuring consensus accuracy in multi-robot systems, even when faced with Byzantine attacks using Lyapunov theory. Subsequently, a sliding mode control is combined with an adaptive technique for multi-robot systems that lack prior knowledge of Byzantine attack. Later, an attack observer is proposed to estimate the performance of multi-robot systems in the presence of a Byzantine attack. Additionally, chattering effects are mitigated by employing integral sliding mode control. As a result, resilient consensus performance of multi-robot systems can be achieved in a finite time interval. A simulation example is also presented to validate the effectiveness of the proposed model. Furthermore, we delve into the data structure of the proposed method and explore its integration with Artificial Intelligence for seamless incorporation into the Industrial Internet of Things applications.

Keywords: resilient consensus; multi-robot system; sliding mode control; Byzantine attack; Industrial Internet of Things; recurrent neural network; time series; digital twins

Citation: Nasir, M.; Maiti, A. Adaptive Sliding Mode Resilient Control of Multi-Robot Systems with a Leader–Follower Model under Byzantine Attacks in the Context of the Industrial Internet of Things. *Machines* **2024**, *12*, 205. https://doi.org/10.3390/machines12030205

Academic Editor: Dan Zhang

Received: 29 January 2024
Revised: 12 March 2024
Accepted: 14 March 2024
Published: 20 March 2024

1. Introduction

Over the past decade, a multitude of consensus control algorithms for multi-robot systems (MRS) have emerged, showcasing their effectiveness across diverse domains, such as agriculture, search and rescue, industry, autonomous vehicles, and power grids [1–6]. The primary goal of MRS consensus control is to facilitate the convergence of all robots toward a desired state (such as a specific position or heading) while engaging robots in dedicated or shared tasks, including tracking, monitoring, capturing, enclosing, and lifting [7,8]. To ensure effective control of MRS, various consensus control techniques have been proposed in the literature. These include behavior-based control, structure-based control, leader–follower control, etc., [9–11]. The leader–follower control technique has proven particularly valuable due to its scalability and simplicity. Information exchange between the leader robot and all other robots is crucial for task completion within this control framework.

The exchange of information within the cooperating MRS plays a pivotal role in achieving the desired cooperative consensus objectives [12]. Typically, wireless networks facilitate intercommunication among robots, allowing them to exchange information such as position, velocity, and heading within an MRS [13]. Wireless networks introduce various constraints for the robots, including induced delays, parameter uncertainties, and external disturbances [14,15]. These delays can significantly impact the performance of MRS and may even lead to instability [16]. Various techniques can be employed to address the induced constraints posed by wireless networks in multi-agent systems [17]. Hence, an ideal wireless network for the MRS can be assumed, excluding induced constraints. However,

rather than induced constraints, several security considerations can impact the secure transmission of information among the robots [18]. Thus, designing an appropriate model to mitigate the adverse effects of security concerns on the consensus performance of MRS requires meticulous consideration.

The security concern during the exchange of information among robots is significant and cannot be ignored [19]. For example, the communication among robots via wireless networks is susceptible to various cyber attacks [20]. These attacks can be deception attacks [21], denial of service attacks [22], replay attacks [23], or Byzantine attacks [24]. Among all these attacks, the Byzantine attack stands out as one of the most severe and challenging to detect. It can be described as a situation where certain components of a distributed system have failed. However, identifying these failures remains difficult due to the lack of relevant attack information [25]. Existing literature highlights that components of individual robots, including actuators, sensors, robot operating systems, and motion controllers, are susceptible to cyber attacks. These vulnerabilities create opportunities for attackers to infiltrate robots, gaining full control and potentially leading to a Byzantine attack within the MRS [26]. In a cooperative MRS, all robots coordinate with each other. Consequently, if one of the robots falls victim to a Byzantine attack, it can compromise the performance of other robots, potentially leading to a system-wide collapse [27].

To address security challenges, such as Byzantine attacks on MRS, various control mechanisms have been proposed. One commonly used technique involves applying advanced encryption and authentication methods to safeguard information sharing among robots and verify the identity of each robot [28]. However, these approaches often overlook the dynamic behavior of individual robots. Consequently, there remains a need for resilient consensus control in MRS when facing Byzantine attacks. While a few control designs have been introduced to address this issue, one notable example is a fuzzy logic-based control technique aimed at countering Byzantine attacks within MRS [29]. Similarly, to solve the inconsistent and unintended behaviors of the robots in MRS, a blockchain-based leader–follower control mechanism for MRS is proposed [30]. In addition, to tackle the challenges related to sensed data sharing and energy efficiency in swarm operations for multi-drone collaboration, a secure blockchain-based technique has been proposed to counter Byzantine robots [31]. In the same way, to address issues related to Byzantine tolerance and decision making under partition tolerance, a distributed control strategy has been devised using IoT and ROS2 [32]. Likewise, to empower swarm robots in identifying malicious robots and data, a knowledge validation-based algorithm has been proposed that utilizes Hashgraph [33].

Numerous control methods have been proposed to address the uncertainties and disturbances of the MRS. For example, [34–36] worked to focus cyber threats on actuators, sensors, and designed observers, which can monitor the performance of cyber–physical systems in the presence of attacks and external disturbances. All these proposed techniques contributed to solving the issues of cyber–physical systems, but still considerable contributions are required to improve the performance of MRS and solve the consensus problems of MRS. Furthermore, chattering is one of the important crucial problems which needs further improvement. Similarly, a resilient adaptive and distributed control technique for the MRS has been proposed [37].

The proposed technique maintained the stability of the MRS under sensor attacks and solved the high gain sensitivity problem. The proposed technique is limited to sensor attacks only, but it did not consider the other possible attacks on the MRS, such as reachable robots, root robots, non-root robots, etc. Furthermore, the convergence rate of the proposed technique is low, which can raise concerns about coordination and stability in MRS. Furthermore, a consensus control mechanism for an MRS to minimize the denial-of-service attack effects based on an event-triggered and cooperative localization approach is proposed [38]. The proposed event-triggered control approach is a decent solution for MRS under attack, but the proposed technique can generate jitters due to variations of updates, which can result in performance degradation and communication delay. Furthermore, the proposed

technique cannot solve the Byzantine attack on MRS. Furthermore, a bio-inspired SMC-based formation control and tracking of MRS is proposed in [39]. The proposed scheme solved the consensus formation of MRS, but the proposed technique lacks in dealing with several constraints, such as misleading data and package loss due to a Byzantine robot. Hence, this conversation leads to the need for a resilient controller to overcome issues.

For the above-mentioned problems, a sliding mode control (SMC) can be the best choice due to its ability to deal with performance issues in finite time intervals. SMC is a well-known and widely used controller for nonlinear control of practical applications due to its strong robustness to interference and uncertainties, such as attacks and speed of response. Similarly, using the SMC method has many other advantages, such as higher precision and perturbation performance compared to asymptotic performance and faster convergence in finite time intervals. Furthermore, SMC has gained tremendous attraction due to its certain benefits while considering the system's performance in finite time intervals [40].

The robustness and phase reaching are the prominent issues of MRS in the presence of uncertainties and disturbances due to Byzantine attacks. Hence, a combination of robust techniques with SMC to solve such issues is the conventional method. This paper presents an adaptive sliding mode resilient technique for the consensus control of MRS under Byzantine attack. Compared to existing techniques, the paper's main contributions are as follows:

1. First, an investigation of finite-time resilient consensus tracking for MRS is performed. By bounded time derivative of the attack signal, transient performance within a finite time interval is achieved.
2. Second, an SMC-based resilient consensus control law to analyze finite-time resilient consensus in MRS under Byzantine attacks is developed. Additionally, an observer is integrated into the controller design to track attack effects and mitigate chattering.
3. Third, an adaptive technique based on integral SMC has been proposed. This technique automatically adjusts the gain to ensure the stability of MRS by minimizing the impact of Byzantine attacks.
4. Finally, we show that SMC's data structure can be used for advanced computational algorithms, such as Artificial Intelligence, to identify the events and conditions in the MRS in the context of the Industrial Internet of Things. This is achieved by deriving a computational model of the same problem addressed by the SMC.

The rest of the paper is summarized as follows: Section 2 presents the problem formulation and attack effects, Sections 3–6 presents the design of the control technique, Section 7 presents the simulation results, and Sections 8–9 concludes the paper discussing the data structure and possibilities with Artificial Intelligence.

2. Mathematical Preliminaries

Consider a graph G consisting of n number of coordinating robots such that $G = \{V, E, A\}$, where $V = \{1, 2, 3, \ldots, n\}$ and $E \subseteq V \times V$ represents the vertices and edges of the graph, respectively. Suppose an undirected path from robot i to robot j such that the path consists of a successive sequence of edges, which can be denoted as $(V_i, V_j), (V_k, V_l), \ldots, (V_i, V_j)$. Let A be $n \times n$ adjacency matrix, which is also a diagonal matrix, can be written as $A = \begin{cases} 1, & \text{if } (V_i, V_j) \in E \\ 0, & \text{otherwise} \end{cases}$ and $A = [a_{ij}]_{n \times n}$. Similarly, the degree matrix $D = \{d_{ij}\}$ is a diagonal matrix such that the degree of the i^{th} robot is represented by d_{ij}. Furthermore, consider a semi-positive and symmetric definite matrix denotes the Laplacian matrix L of the graph G, where $L = D - A$ and $L = [l_{ij}]_{n \times n}$. If $j \neq i, l_{ij} = -a_{ij}$; otherwise, $\quad l_{ij} = \sum_{j=1}^{n} a_{ij}$ [3].

Let $\mathfrak{r}_o$ be the leader robot and the remaining $\mathfrak{r}_1, \mathfrak{r}_2, \ldots, \mathfrak{r}_n$ the follower robots in the MRS. Then, the role of the leader robot is to send and receive information to some of the follower robots. In other words, the leader robot does not need to receive information from all followers. Suppose a connection weight $\boldsymbol{q_i}$ is used between the sender and follower

robots such that $q_i > 0$, if the information is received by i^{th} follower robot from the leader robot; otherwise, $q_i = 0$ [9].

3. Problem Formulation

Suppose MRS consists of n cooperating robots, then the dynamics of each robot can be written as:

$$\dot{y}_i(t) = u_i(t) + f_i(t), \tag{1}$$

where $u_i(t), y_i(t)$, and $f_i(t)$ denote the control input, state of the i^{th} follower robot, and attack signal on the i^{th} follower in the MRS, respectively.

Similarly, the dynamics of the leader robot in the MRS can be written as:

$$\dot{y}_0(t) = u_0(t), \tag{2}$$

where $u_0(t)$ and $y_0(t)$ denote the control input and state of the leader robot, respectively.

Then, an error $\bar{y}_i(t)$ between the leader and follower robots can be represented as $\bar{y}_i(t) = y_i(t) + y_0(t) + \mathscr{R}_i$, where $\mathscr{R}_i$ denote deviation of state between the leader robot and follower robots.

3.1. Attack on the Multi-Robot System

This section describes the modeling and analysis of an attack on MRS.

3.1.1. Attack Modeling

In this section, modeling of the attack on the MRS has been presented. Specifically, the MRS under actuator attack can be expressed as:

$$u_i^c(t) = u_i(t) + \alpha_i u_i^a(t), \tag{3}$$

where $u_i(t), u_i^c(t)$, and $u_i^a(t)$ represent the control input, corrupted control input, and attack signal. Similarly, α_i denotes the binary constant such that if $\alpha_i = 1$, then i^{th} robot of MRS is under actuator attack; otherwise, $\alpha_i = 0$. Furthermore, MRS under sensor attack can be written as:

$$y_i^c(t) = y_i(t) + \beta_i y_i^a(t), \tag{4}$$

where $y_i(t), y_i^c(t)$ and $y_i^a(t)$ represent the nominal state, corrupted state, and attack signal. Furthermore, β_i is a binary constant such that if $\beta_i = 1$, then i^{th} robot of MRS is under sensor attack; otherwise, $\beta_i = 0$.

According to Equations (3) and (4), the overall attack effects on the i^{th} robot of MRS can be written as:

$$f_i(t) = \alpha_i u_i^a(t) + ck \sum_{n_i} a_{ij}(\beta_j y_j^a(t) - \beta_i y_i^a(t)), \tag{5}$$

where $y_i^a(t)$ and $u_i^a(t)$ represent the attack signals into the sensor and actuator, respectively, and $y_j^a(t)$ represents the attack signals injected into the neighborhood j of the robot i. Similarly, c, k, and a_{ij} represent the scalar gain, feedback gain, and (i, j) adjacency of the adjacency matrix A, respectively.

Based on the above discussion, attacks on the MRS can be divided into two types, such as Byzantine attack and non-Byzantine attack. In a Byzantine attack, a trusted robot that has successfully passed all verification and authentication processes turns out to be rogue. In such a scenario, the rogue robot can easily launch an attack on the MRS, affecting functionalities, such as destabilization and performance degradation [29]. This type of attack can be designed as follows:

$$\dot{f}_i(t) = \sigma f_i(t), \tag{6}$$

where $\sigma \in R$, which can be used to design all types of attack which are not in the form of Equation (6), written as:

$$\Delta = \{\lambda_1(\sigma), \lambda_2(\sigma), \ldots, \lambda_n(\sigma)\}, \tag{7}$$

where $\lambda_i(\sigma)$ denotes the set of eigenvalues of the attack signal generator dynamics σ.

Definition 1. *A robot is said to be a compromised robot if it is under the influence of attacks, represented by n_{com}; otherwise, it is called an intact robot, represented as n_{int}, i.e., $= n/n_{com}$ [3].*

Definition 2. *A robot i is called reachable to robot j if and only if there exists a path between them in the graph, such that $v_v = [v_{v1}, v_{v2}, \cdots, v_{vn}]$, such that $a_{jv_{v1}}, a_{jv_{v2}}, ..., a_{jv_{vn}} \neq 0$ [3].*

3.1.2. Attack Analysis

This section provides an analysis of the Byzantine attacks on the MRS based on graph theory. Certain lemmas and notations are used for this purpose.

Suppose L denotes the partitioned Laplacian graph, written as:

$$L = \begin{bmatrix} L_{r\times r} & 0_{r\times nr} \\ L_{nr\times r} & L_{nr\times nr} \end{bmatrix}, \tag{8}$$

where r and nr denote the root and non-root robots of the MRS. Similarly, $L_{r\times r}$ and $L_{nr\times nr}$ matrices denote the root robot and non-root robots of the subgraph.

Lemma 1, given below, can be used to prove that local neighborhood error tracking converges to zero and the MRS ensures the resilient consensus despite Byzantine attack.

Lemma 1. *Consider a Laplacian matrix L, as given in Equation (8), then $L_{r\times r}$ and $L_{nr\times nr}$ denotes the singular M-matrix and non-singular M-matrix, respectively, [41].*

Similarly, the following given Lemma 2 is used to derive the necessary consensus condition of MRS.

Lemma 2. *The resilient consensus control of MRS in the presence of attacks can be ensured if the following conditions are fulfilled [40]:*

$$\bar{u}_i(t)^{\text{nor}} = Y_i^{\zeta}(t), \tag{9}$$

where ζ denotes the ratio of odd numbers such that $\zeta \in (0.5, 1)$. Suppose a scalar $\xi_i > 0$ and number of neighbouring robots $\mathfrak{r}_i$ of any i^{th} robot where $\mathfrak{r}_i \in [1, n]$, then $Y_i(t)$ can be modeled as follows:

$$\begin{aligned} Y_i(t) &= -\frac{\xi_i}{\mathfrak{r}_i + 1} \sum_{j\in n_i} b_{ij}\left[y_i(t) - y_0(t) + \mathscr{R}_i - (y_j(t) - y_0(t) + \mathscr{R}_i)\right] + a_{ij}(y_i(t) - y_0(t) + \mathscr{R}_i) \\ &= -\frac{\xi_i}{\mathfrak{r}_i + 1} \sum_{j\in n_i} b_{ij}(\bar{y}_i(t) - \bar{y}_j(t)) + a_{ij}\bar{y}_i(t). \end{aligned} \tag{10}$$

Lemma 3. *Suppose a linear MRS whose state space representation is written as:*

$$\dot{y}(t) = g(x, t), g(0, t) = 0, \tag{11}$$

where $y \in R^n$. Let $O(x) > 0$ be a continuously differentiable function, which can be defined in the locality of root such that two real numbers must meet $a \in (0, 1)$ and $c > 0$. Then, origin stabilization in the MRS can be guaranteed in the settling time if the function $O(x)$ verifies $\dot{O}(x) \leq -cO(x)^a$ [40].

One can calculate the upper bound value of the settling time of the following:

$$T \leq \frac{O^{1-a}}{c^{1-a}}. \tag{12}$$

Lemma 4. *For $y_i \in R, \pi \in (0,1]$, then $(\sum_{i=1}^{n} |y_i|)^{\pi} \leq (\sum_{i=1}^{n} |y_i|^{\pi})$ [40].*

Assumption 1. *Suppose a positive scalar μ_i and attack signal $f_i(t)$ of the follower robots, which satisfies $\|\dot{f}_i(t)\|_{\infty} \leq \mu_i$.*

Assumption 2. *Suppose graph G has a directed spanning tree and directed communication topology with a leader robot at the root.*

4. Continuous-Sliding-Mode-Based Consensus

This section provides a control law for the MRS under Byzantine attack based on continuous-sliding-mode-based consensus.

4.1. Sliding Mode Control

The design procedure of SMC includes switching surface and control law. The switching surface is designed through a linear combination of state variables, whereas the control law involves the design of a suitable control law. The switching surface is crucial to classifying the SMC techniques into lower or higher orders. The conventional first-order sliding surface of the first-order SMC technique can be defined as:

$$S(t) = \{y(t) \in R^n : s(t) = 0\}, \tag{13}$$

where $y(t) \in R^n$ denotes the state vector and $s(t) = 0$ shows that the sliding surface trajectory is obeyed. The control law of the first-order SMC scheme can be written as:

$$u(t) = u_e(t) + u_d(t), \tag{14}$$

where $u_e(t)$ and $u_d(t)$ define linear or equivalent control and nonlinear or discontinuous control parts, respectively. The goal of the discontinuous part is to move the state trajectories near to switching surface. Therefore, for an ideal sliding motion, the linear control and nonlinear control become $\dot{s}(y(t), u(t), y(t))|_{u(t)-u_e(t)} = 0$, and $u_d(t) = -ksin(s)$.

Higher-order SMC is used to increase the tracking accuracy of switching surface under sliding motion represented as in [40]:

$$s^r = y \in R^n : s = \dot{s} = \ddot{s} = \cdots = s^{r-1} = 0 \tag{15}$$

4.2. Integral-Sliding-Mode-Control-Based Consensus

According to Equations (1) and (9), a control law for the MRS using the sliding mode control mechanism can be modified. Thus, integral SMC can be represented as

$$s_i(t) = -\bar{y}_i(0) - \int_0^t \bar{u}_i(\tau)\, d\tau + \bar{y}_i(t), \tag{16}$$

where $\bar{y}_i(0)$ denotes the initial state value of $\bar{y}_i(t)$. The integral sliding mode state can be ensured for the MRS, i.e., $s_i(t) = \dot{s}_i(t) = 0$. Thus, one can write the following:

$$\dot{\bar{y}}_i(t) = \bar{u}_i(t)^{\text{nor}}. \tag{17}$$

Subsequently, an updated sliding mode consensus control protocol can be written as:

$$\begin{aligned} \bar{u}_i(t) &= \bar{u}_i(t)^{\text{nor}} + \bar{u}_i(t)^{\text{up}}, \\ \bar{u}_i(t)^{\text{up}} &= -g_1 \text{sig}^{\frac{1}{2}}(s_i) + \mathfrak{w}_i(t), \\ \dot{\mathfrak{w}}_i(t) &= -g_2 \text{sgn}(s_i). \end{aligned} \tag{18}$$

Equation (18) can be written in vector form, as given below:

$$\begin{aligned} \bar{u}(t) &= \bar{u}(t)^{\text{nor}} + \bar{u}(t)^{\text{up}}, \\ \bar{u}(t)^{\text{up}} &= -g_1 \text{sig}^{\frac{1}{2}}(s) + \mathfrak{w}(t), \\ \dot{\mathfrak{w}}(t) &= -g_2 \text{sgn}(s), \end{aligned} \tag{19}$$

where $\bar{u}(t) = [\bar{u}_1(t), \ldots, \bar{u}_n(t)]^T$, $\bar{u}(t)^{nor} = [\bar{u}_1(t)^{nor}, ..., \bar{u}_n(t)^{nor}]^T$, $\mathfrak{w}(t) = [\mathfrak{w}_1(t), ..., \mathfrak{w}_n(t)]^T$, and $\bar{u}(t)^{up} = [\bar{u}_1(t)^{up}, ..., \bar{u}_n(t)^{up}]^T$, which shows the consensus control with $g_1 > 0, g_2 > \mu$, where μ is a positive scalar value.

5. Controller Design

In this section, the proposed integral sliding mode scheme is analyzed to ensure that the MRS remains on a sliding surface even under a Byzantine attack. Additionally, the resilient consensus performance of MRS in the presence of a Byzantine attack is also addressed. Finally, the necessary conditions for designing a controller are given below.

Theorem 1. *The consensus control law for the MRS is discussed in Section 4. According to Assumptions 1 and 2, MRS on the sliding mode surface in the finite time should be satisfied.*

Proof. By taking the derivative of $s_i(t)$ and combining it with Equation (9), one can obtain:

$$\dot{s}_i(t) = \bar{u}_i(t)^{up} + f_i(t), \tag{20}$$

where $s_i(t), u_i(t)^{up}$, and $f_i(t)$ are the sliding state, updated control law, and attack signal, respectively, which are already defined in the aforementioned sections. Equation (20) can also be written as:

$$\begin{aligned} \dot{s}_i(t) &= -g_1(t) \text{sig}^{\frac{1}{2}}(s_i) + f_i + \mathfrak{w}_i, \\ \dot{\mathfrak{w}}_i(t) &= -g_2 \text{sgn}(s_i). \end{aligned} \tag{21}$$

Let $\boldsymbol{e}_i = f_i + \mathfrak{w}_i$ then Equation (21) can be modified as:

$$\begin{aligned} \dot{s}_i(t) &= -g_1 \text{sig}^{\frac{1}{2}}(s_i) + \boldsymbol{e}_i, \\ \dot{\boldsymbol{e}}_i(t) &= -g_2 \text{sgn}(s_i) + \dot{f}_i. \end{aligned} \tag{22}$$

The Lyapunov function candidate can be created as:

$$V(t) = \sum_{i=1}^{n} V_i(t) = \sum_{i=1}^{n} \phi_i(t)^T R_i(t) \phi_i(t), \tag{23}$$

where $\phi_i(t) = [\text{sig}^{\frac{1}{2}}(s_i)\, e_i], R_i \in \mathbb{R}^{2\times 2} > 0$.

The derivative of the $\phi_i(t)$ can be written as follows:

$$\begin{aligned} \dot{\phi}_i(t) &= \begin{bmatrix} \frac{1}{2}|S_i|^{-\frac{1}{2}} \dot{S}_i \\ \dot{e}_i \end{bmatrix} \\ &= \frac{1}{2}|S_i|^{-\frac{1}{2}} \begin{bmatrix} -g_1(t)\text{sig}^{\frac{1}{2}}(s_i) + e_i \\ -2\left[g_2 - \dot{f}_i \text{sgn}(s_i)\right] \text{sig}^{\frac{1}{2}}(s_i) \end{bmatrix} \\ &= |S_i|^{-\frac{1}{2}} W_i \phi_i(t), \end{aligned} \tag{24}$$

where $W_i = \begin{bmatrix} -\frac{1}{2}g_1(t) & \frac{1}{2} \\ -[g_2 - \dot{f}_i \text{sgn}(s_i)] & 0 \end{bmatrix}$.

Now, by calculating the derivative of the Lyapunov function given in Equation (23), with system dynamics given in Equation (22), one obtains:

$$\dot{V}(t) = \sum_{i=1}^{n} \dot{V}_i = \sum_{i=1}^{n} |S_i|^{-\frac{1}{2}} \phi_i(t)^T Q_i \phi_i(t) < 0, \tag{25}$$

where Q_i and W_i are connected to each other based on the Lyapunov equation, given as:

$$W_i^T R_i + R_i W_i = -Q_i. \tag{26}$$

From Equation (26), the solution $W_i > 0$ is unique for every $Q_i > 0$. Thus, V_i is purely the Lyapunov function.

The inequality given in Equation (25) can be modified based on the fact that $|S_i|^{\frac{1}{2}} = |sig^{\frac{1}{2}}(s_i)| \leq \|\phi_i\|_2 \leq \mu_{min}^{-\frac{1}{2}}(R_i) V_i^{\frac{1}{2}}$, given below:

$$\dot{V}(t) \leq -\sum_{i=1}^{n} \mu_{\min}^{-\frac{1}{2}} V_i^{-\frac{1}{2}}(t) \frac{\mu_{\min}(Q_i)}{\mu_{\max}(R_i)} V_i(t) \leq -\delta \sum_{i=1}^{n} V_i^{\frac{1}{2}}(t). \tag{27}$$

where $\delta = \min_{i=1,2,\ldots,n} \left\{ \frac{\mu_{\min}^{\frac{1}{2}}(W_i)\mu_{\min}(Q_i)}{\mu_{\max}(R_i)} \right\} > 0$. The expression $\sum_{i=1}^{n} V_i^{\frac{1}{2}}(t) \geq (\sum_{i=1}^{n} V_i)^{\frac{1}{2}}(t)$ holds in the light of Lemma 4. Therefore, one can write $\dot{V}(t) \leq -\delta V^{\frac{1}{2}}(t)$. □

According to the above discussions, we have $V(\theta(t, s(0), e(0))) \leq -\delta V^{1/2}(\theta(t, s(0), e(0)))$. Furthermore, one can verify that $V(\theta(t, s(0), e(0)))$ and $\theta(t, s(0), e(0))$ approach zero using Lemma 3 and its equation in the finite time, which is smaller than $T = \frac{2}{\delta} V^{1/2}(s(0), e(0))$. Furthermore, $\theta(s(0), e(0)) \neq 0$ because $s(0) = 0$, but $e(0) \neq 0$.

Remark 1. *The Lyapunov function given in Equation (25) is absolutely continuous, but it is not locally Lipschitz on the set* $\Xi = \{(s_i, \varpi_i) \in \mathbb{R}^2 \,|\, s_i = 0, i = 1, 2, 3, \ldots, n\}$, *as it includes* $sig(s_i)^{\frac{1}{2}}$. *This term requires the designed Lyapunov function to be locally Lipschitz different from the typical Lyapunov function. According to Zubov theorem, it is important to have a continuous Lyapunov function. In this section, the analysis of the MRS stability is performed using* $V(\phi_i)$. *It is worth noting that a combination of absolute continuous functions is not always absolute continuous. In the above analysis,* $V(\theta(t, s(0), e(0)))$ *is absolutely continuous with the trajectories* $\theta(t, s(0), e(0)) = [\theta_1(t, s_1(0), e_1(0)), \theta_2(t, s_2(0), e_2(0)), \ldots, \theta_n(t, s_n(0), e_n(0))]^T$ *and it is important to verify it carefully.*

Furthermore, Theorem 2 is presented below to describe the consensus tracking of MRS under Byzantine attack on the sliding surface.

Theorem 2. *MRS operating under a Byzantine attack achieves consensus tracking, as per Assumptions 1 and 2, by maintaining the MRS on the integral sliding mode surface within finite time [40].*

Proof. To prove Theorem 2, first, there is a need to choose a suitable Lyapunov function given below:

$$V(t) = \frac{1}{2} \bar{y}(t)((L + B) \bigotimes I_n)^T ((L + B) \bigotimes I_n) \bar{y}(t) = \frac{1}{2} M^T M, \tag{28}$$

where L is Laplacian matrix, B is the input matrix, I_n is an identity matrix, and M_i^T is a vector associated with robot i such that $M = [M_1^T, M_2^T, \ldots, M_n^T]^T$ and $M_i^T = \sum_{i=1}^{n} a_{ij}(\bar{y}_i(t) - \bar{y}_j(t)) + b_{ij}\bar{y}_i(t)$.

The derivative of Equation (29) gives:

$$\begin{aligned}\dot{V}(t) &= M^T((L+B)\otimes I_n)\dot{\tilde{y}}(t)\\ &= M^T((L+B)\otimes I_n)Y_i^{\zeta}(t)\\ &\leq -\mu_{\min}(\varphi(t)\otimes I_n)\mu_{\min}((L+B)\otimes I_n)\|M\|^{1+a}\\ &\leq -\mu_{\min}(\varphi(t)\otimes I_n)\mu_{\min}((L+B)\otimes I_n)\|M^TM\|^{\frac{1+a}{2}}\\ &\leq -\mu_{\min}(\varphi(t)\otimes I_n)\mu_{\min}((L+B)\otimes I_n)2V(t)^{\frac{1+a}{2}}\\ &\leq \mathfrak{z}V(t)^{\frac{1+a}{2}},\end{aligned} \tag{29}$$

where ζ represents the ratio of odd positive numbers, i.e., $\text{sign}((.)^{\zeta}) = \text{sign}(.)$. Furthermore, $\varphi = \text{diag}\left\{\left(\frac{\xi_1}{\mathfrak{r}_1+1}\right)^a, \left(\frac{\xi_2}{\mathfrak{r}_2+1}\right)^a, \ldots, \left(\frac{\xi_n}{\mathfrak{r}_n+1}\right)^a\right\}$ and $\mathfrak{z} = \mu_{\min}(\varphi(t)\otimes I_n)\mu_{\min}((L+B)\otimes I_n)2V(t)^{\frac{1+a}{2}}$.

From Lemma 3, it is clear that $V(t)$ approaches to 0 in fixed time. Therefore, settling time can be written as:

$$T \leq \frac{2V(\bar{y}(0))^{\left(\frac{1+a}{2}\right)}}{\mathfrak{z}(1-a)}. \tag{30}$$

□

Thus, $V(t) = 0, \forall t \neq T$ and $y_i(t) = y_0(t) - \mathscr{R}_i \forall t \neq T$. Hence, the consensus performance of MRS under a Byzantine attack can be assured at a specific time.

Remark 2. *Since it is already assumed that $e_i = f_i + \mathfrak{w}_i$, $\bar{u}_i(t)^{up}$, therefore, represent the control of the MRS attack with $g_1 > 0$ and $g_2 > \mu$. It is also worth mentioning that if the term $e_i = f_i + \mathfrak{w}_i$, then the control $\bar{u}_i(t)^{up}$ acts as an attack observer, i.e., $\int_o^t g_2 sgn(s)d\tau = f, t > T$.*

6. Consensus Control of a Multi-Robot System with an Attack Observer

Sometimes, it is very difficult to obtain a bond between malicious information (attack) and topology information, especially in the case of a Byzantine attack, where an attacker is an authenticated robot of the MRS. Furthermore, to ensure the adaptive consensus performance, a large switching gain ∇ is selected, because it will create the actuator's critical chattering and high energy consumption in practical situations. Chattering in the actuator can be raised through friction. Therefore, to analyze this phenomenon developed through $\dot{\nabla}_i = \varepsilon(\|s_i\| - \rho\nabla_i), \quad \nabla_i(0) \neq 0, \varepsilon$ and ρ are selected positive. The limited growth of the switching gain can be prevented through a term $-\rho\nabla_i$. First, an attack observer is presented to estimate the attacks on the MRS. The dynamics of the attack observer can be written as:

$$\begin{aligned}\dot{\mathfrak{Z}}(t) &= -\phi(\mathfrak{q}(t) + [\phi\bar{y}_i(t) + \bar{u}_i(t)]),\\ \bar{f}_i(t) &= \mathfrak{q}(t) + \phi\bar{y}_i(t),\end{aligned} \tag{31}$$

where $\bar{f}_i(t), \mathfrak{q}(t)$ and ϕ represent the attack, observer's internal state, and observer gain, respectively. Using this attack observer, one can get:

$$\begin{aligned}\dot{\hat{f}}_i(t) &= \dot{f}_i(t) + \phi\mathfrak{q}(t) + \phi[\phi\bar{y}_i(t) + \bar{u}_i(t)] - \phi(\bar{u}_i(t) + f_i(t))\\ &= \phi\hat{f}_i(t) + \dot{f}_i(t),\end{aligned} \tag{32}$$

where $\hat{\bar{f}}_i(t) = f_i(t) - \bar{f}_i(t)$, where $i = 1, 2, \ldots, n$. From the arguments for stability in input states, the condition $\hat{\bar{f}}_i(t) \leq \frac{\mu_i}{\phi}$ holds true after an adequately long time.

Second, the control law contains discontinuous dynamics, which may result in chattering, poor MRS performance, and the life of the actuator can even be shortened. Therefore,

it is important to consider continuous dynamics while designing an adaptive consensus law in the presence of attacks, written as:

$$\gamma(s_i) = \begin{cases} -\nabla_i \frac{s_i}{\|s_i\|}, & \text{if } \nabla_i \|S_i\| \geq \beth \\ \nabla_i^2 \frac{s_i}{\beth}, & \text{if } \nabla_i \|s_i\| < \beth, \end{cases} \tag{33}$$

Therefore, to minimize the attack effects, an adaptive resilient sliding mode controller is designed given below

$$s_i = \bar{y}_i(t) + \bar{y}_i(0) - \int_0^t (\bar{u}_i(\tau)^{nor} + \bar{f}_i(\tau))d(\tau). \tag{34}$$

The states of the MRS remain sliding on the resilient sliding mode, i.e., $s_i = \dot{s}_i = 0$. If $\dot{s}_i = 0$, which means that:

$$\dot{\bar{y}}_i(t) = \bar{u}_i(t)^{nor} + \bar{f}_i(t). \tag{35}$$

Thus, a resilient consensus control mechanism can be modeled as follows:

$$\bar{u}(t) = \bar{u}_i(t)^{nor} + \bar{u}_i(t)^{cn}, \tag{36}$$

where $\bar{u}_i(t)^{cn} = [\gamma(s_1)^T, \gamma(s_2)^T, \ldots, \gamma(s_n)^T]^T$.

Furthermore, Theorem 3 is given below to discuss the adaptive sliding mode control law of MRS under Byzantine attacks.

Theorem 3. *Suppose that Assumptions 1 and 2 are true, then the consensus control issue of MRS in the presence of a Byzantine attack with resilient control technique can be resolved by using continuous adaptive sliding mode control law [40].*

Proof. To prove this theorem, the first derivative of Equation (34), i.e., sliding surface s_i, is calculated. Thus, the candidate of the Lyapunov function can be written as:

$$V(t) = \frac{1}{2} s^T s + \frac{1}{2\varepsilon} \sum_{i=1}^{n} (\nabla_i - \bar{\nabla})^2, \tag{37}$$

where the upper bound of the ∇_i is represented by $\bar{\nabla}$. Moreover, $\bar{\nabla}$ is considered to be $\bar{\nabla} > \frac{\mu}{\phi} + \nabla_0, \mu = [\mu_1^T, \mu_2^T, \ldots, \mu_n^T]^T, \nabla_0 > 0$.

Now, by calculating the differential of the $V(t)$ with consensus control trajectory given in Equation (12) gives:

$$\begin{aligned} \dot{V}(t) &= s^T \dot{s} + \frac{1}{\varepsilon} \sum_{i=1}^{n} (\nabla_i - \bar{\nabla}) \dot{\bar{\nabla}} \\ &\leq \frac{\mu}{\phi} \|s\| + s^T \bar{u}(t)^{\text{cn}} + \sum_{i=1}^{n} (\nabla_i - \bar{\nabla})(\|s_i\| - \rho \nabla_i) \end{aligned} \tag{38}$$

□

Case 1: $\nabla_i \|s_i\| \geq \beth$, for $i = 1, 2, \ldots, n, s^T(t)\bar{u}(t)^{\text{cn}} = -\sum_{i=1}^{n} \nabla_i \|s_i\|$.
Since:

$$\begin{aligned} \dot{V}(t) &= \frac{\mu}{\phi} \|s\| - \sum_{i=1}^{n} \nabla_i \|s_i\| + \sum_{i=1}^{n} (\nabla_i - \bar{\nabla})(\|s_i\| - \rho \nabla_i) \\ &= \frac{\mu}{\phi} \|s\| - \bar{\nabla} \sum_{i=1}^{n} \|s_i\| - \rho \sum_{i=1}^{n} (\nabla_i - \bar{\nabla}) \nabla_i \\ &\leq \left(\frac{\mu}{\phi} - \bar{\nabla} \right) \|s\| + \frac{\rho}{4} \sum_{i=1}^{n} \bar{\nabla}^2 \\ &\leq -\nabla_0 \|s\| + \gamma_1, \end{aligned} \tag{39}$$

where $\gamma_1 = \frac{\rho n}{4}\bar{\nabla}^2$.

Case 2: If $\nabla_i\|s_i\| < \beth$, for $i = 1, 2, \ldots, n, s^T(t)\bar{u}(t)^{\text{cn}} = -\sum_{i=1}^{n}\frac{\nabla_i^2}{\beth}\|s_i\|$.

$$\begin{aligned}\dot{V}(t) &\leq \frac{\mu}{\phi}\|s\| - \sum_{i=1}^{n}\frac{\nabla_i^2}{\beth}\|s_i\|^2 + \sum_{i=1}^{n}(\nabla_i - \bar{\nabla})(\|s_i\| - \rho\nabla_i)\\ &\leq -\nabla_0\|s\| + \gamma + \sum_{i=1}^{n}\left(-\frac{\nabla_i^2}{\beth}\|s_i\|^2 + \nabla_i\|s_i\|\right).\end{aligned} \tag{40}$$

Since $\nabla_i\|s_i\| \geq \beth$, therefore, it is easy to understand that $-\left(\frac{\nabla_i^2}{\beth}\|s_i\|^2 + \nabla_i\|s_i\|\right)$ attains the highest value $\beth/4$ when $\nabla_i\|s_i\| = \beth/2$. Hence, one can obtain $\dot{V}(t) \leq -\nabla_0\|s\| + \gamma_2$, here $\gamma_2 = \gamma_1 + \frac{\beth n}{4}$.

Case 3: If $\nabla_i\|s_i\|$ for some robots of the network, then $\nabla_i\|s_i\| < \beth$ for some remaining robots of network. Similarly, one can obtain as given below:

$$\dot{V}(t) \leq -\nabla_0\|s\| + \gamma_3, \tag{41}$$

where $\gamma_1 \leq \gamma_3 \leq \gamma_2$.

Based on the above discussion, the below given expression is verifiable for any $\nabla_i\|s_i\|$ such that:

$$\begin{aligned}\dot{V}(t) &\leq -\nabla_0\|s\| + \gamma\\ &\leq -\nabla_0\|s\| + \partial\nabla_0\|s\| - \partial\nabla_0\|s\| + \gamma\\ &\leq -(1-\partial)\nabla_0\|s\|, \quad \forall\|s\| \geq \frac{\gamma}{\partial\nabla_0},\end{aligned} \tag{42}$$

where $\partial \in (0,1), \gamma = \max\{\gamma_1, \gamma_2, \gamma_3\} = \frac{n(\rho\bar{\nabla}^2 + \beth)}{4}$.

Based on the above cases, the boundary layer can be reached in a finite time in the designed sliding surface.

The below given Theorem 4 is being presented for the adaptive resilient consensus control of MRS using directed communication topology under attack.

Theorem 4. *Let MRS follow a directed communication topology. The resilient consensus problem of MRS under Byzantine attack can be solved by proposing a continuous adaptive sliding mode controller and nominal protocol [40].*

Proof. Using Theorem 2, a suitable Lyapunov function can be constructed as follows:

$$V_2(t) = \frac{1}{2}\bar{y}(t)^T((L+B)\otimes I_n)^T((L+B)\otimes I_n)\bar{y}(t) + V(t) = \frac{1}{2}M^TM + V(t). \tag{43}$$

One gets:

$$\dot{V}_2(t) = M^T((L+B)\otimes I_n)\dot{\bar{y}}(t) + \dot{V}(t) \tag{44}$$

By using expression in Equation (42), one can rewrite $\dot{V}_2(t)$ as follows:

$$\begin{aligned}\dot{V}_2(t) &\leq M^T((L+B)\otimes I_n)\dot{\bar{y}}(t) - \nabla_0\|s\| + \gamma\\ &\leq -\mu_{\min}(\varphi(t)\otimes I_n)\mu_{\min}((L+B)\otimes I_n)\|M\|^{1+a} - \nabla_0\|s\| + \gamma\\ &\leq -(1-\partial_1)\|M\|^{1+a}, \quad \forall\|M\|^{1+a} \geq \frac{\gamma}{\partial_1\mathfrak{z}},\end{aligned} \tag{45}$$

where $\mathfrak{z} = \mu_{min}(\varphi(t)\otimes I_n)\mu_{min}((L+B)\otimes I_n)2^{1+a}$ and $\partial_1 \in (0,1)$. One can get $V_2(t) < 0$.

If $\|M\| \in [0,1)$, one gets:

$$\begin{aligned}\dot{V}_2(t) &\leq -\mathfrak{z}\|M\|^2 + \gamma\\ &\leq -(1-\partial_1)\mathfrak{z}\|M\|^2.\end{aligned} \tag{46}$$

Then, the bounded limit of $\|M\| \geq \sqrt{\frac{\gamma}{\partial_1 \mathfrak{z}}}$.

If $\|M\| \in [1, \infty)$, one gets:

$$\begin{aligned} \dot{V}_2(t) &\leq -\mathfrak{z}\|M\| + \gamma, \\ &\leq -(1-\partial_1)\mathfrak{z}\|M\|. \end{aligned} \tag{47}$$

Therefore, it is verifiable that $\|M\| \geq \frac{\gamma}{\partial_1 \mathfrak{z}}$.

Hence, it is concluded that $V_2(t) < 0$ and adaptive consensus control of MRS under Byzantine attack using sliding mode control protocol can be assured. If $\Delta = \left\{\sqrt{\frac{\gamma}{\partial_1 \mathfrak{z}}}, \frac{\gamma}{\partial_1 \mathfrak{z}}\right\}$, then MRS can reach to the set of trajectories $\Delta_1 = \left\{\|M\| \leq \Delta, \|s\| \leq \frac{\gamma}{\nabla_0 z}\right\}$. □

Remark 3. *The parameter ε affects the reaction time of the adaptive gain for the proposed SMC technique. The value of the parameters ⊐ and ρ are kept small to boost the tracking performance. Although a small value of ⊐ may lead to chattering effects due to the presence of time delays. The proposed work is chattering-free due to the continuous integral sliding mode controller rather than a discontinuous controller. Furthermore, the proposed technique is independent of communication topology and attack effect on the MRS due to the adaptive mechanism.*

7. Simulation

This section presents the effectiveness of the proposed mechanism in ensuring adaptive, resilient consensus control of MRS in the presence of a Byzantine attack. To verify the proposed model, consider a communication topology of the five cooperating robots, as shown in Figure 1. According to Figure 1, Robot 1 serves as the root (leader) robot, while the remaining four robots function as non-root (leader–follower) robots. Let us borrow the dynamics of the MRS from [34], given as:

$$A = \begin{bmatrix} -1.175 & 0.987 \\ -8.487 & -8.878 \end{bmatrix}, \quad B = \begin{bmatrix} -0.194 & -0.036 \\ -19.29 & -3.803 \end{bmatrix}.$$

The diagonal and Laplacian matrices, based on the communication topology as depicted in Figure 1, can be expressed as follows:

$$L = \begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 2 & -1 \\ -1 & 0 & 0 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 2 & -1 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

An adaptive, resilient control scheme for the MRS under a Byzantine attack is designed by choosing the parameters, given as $\rho_i = 0.5$, $\mathfrak{r}_1 = 3$, $\mathfrak{r}_2 = 1$, $\mathfrak{r}_3 = 2$, $\mathfrak{r}_4 = 2$, $g_1 = 0.5491$, $g_2 = 1.6878$, and $g_2 > \mu = 1$. Furthermore, a step signal is regarded as an attack signal in MRS due to its simplicity of implementation. Let the initial state trajectories of the MRS under Byzantine attack be at $y_i = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ to design an adaptive and resilient consensus controller.

In Figure 2, the performance of the MRS is observed in the absence of attacks, where all signals converge to the consensus state. Specifically, Figure 2a demonstrates that MRS successfully achieves consensus, with all state values converging towards the desired input state. This result validates that MRS, employing a resilient SMC, achieves consensus and corroborates the findings presented in Theorem 1. Similarly, Figure 2b shows the error signal of the MRS.

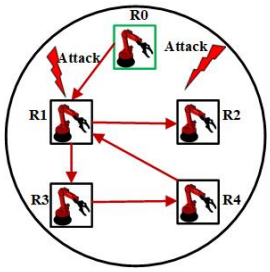
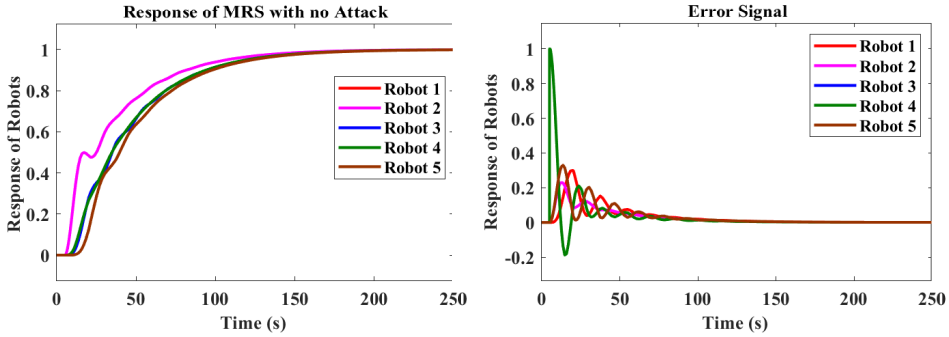


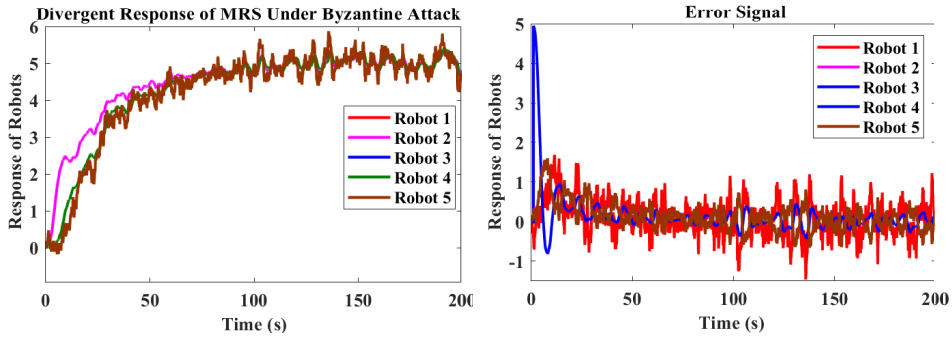
Figure 1. Communication topology of MRS.



(**a**) Response of MRS. (**b**) Error signal.

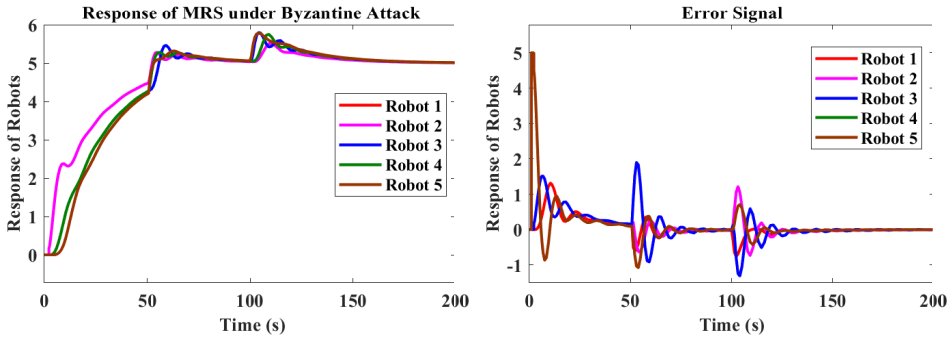
Figure 2. Convergence response of the MRS in the absence of a Byzantine attack.

Let us consider a scenario where the MRS is subjected to a Byzantine attack. In such a situation, the collaborating MRS cannot attain a consensus state, as in Figure 3. Specifically, Figure 3a shows random ripples in the response, indicating instability due to Byzantine attacks. Figure 3b plots the error signal of MRS under a Byzantine attack. Figure 4 depicts that the MRS is prevented from phase reaching in the presence of Byzantine attacks and boosts the robustness. Particularly, Figure 4a illustrates the response of MRS under a Byzantine attack. It is observed that during a brief interval, the collaboration or communication among the robots is disrupted, resulting in spikes in the MRS response. However, after this transient disturbance, all the robots eventually converge to the desired input state. This observation underscores the effectiveness of the resilient, adaptive SMC technique. Furthermore, Figure 4b shows the error signal of stable MRS in the presence of a Byzantine attack.



(**a**) Response of MRS. (**b**) Error signal.

Figure 3. Divergence response of MRS under Byzantine attack.

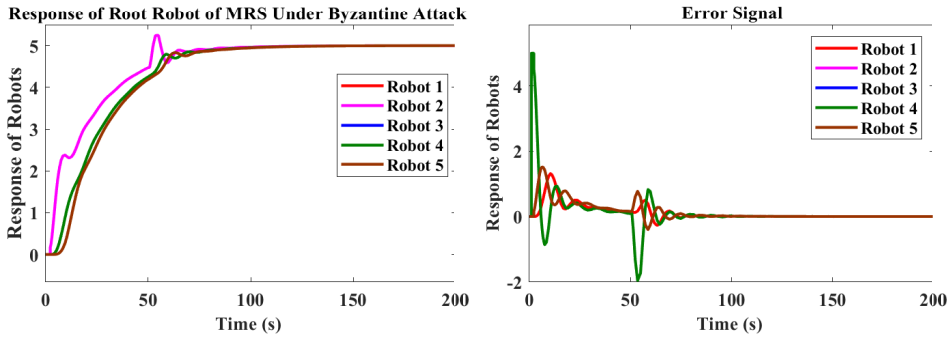


(**a**) Response of MRS (**b**) Error signal.

Figure 4. Convergence response of MRS under Byzantine attack.

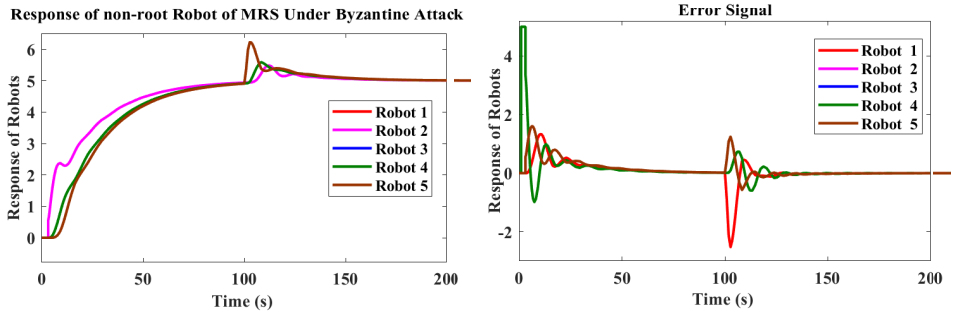
While the proposed technique demonstrates adaptability and robustness for MRS under attack, it is essential to consider the leader–follower topology. In this configuration, an attacker could potentially target the root robot, non-root robots, or any reachable robot within the MRS.

In accordance with Section 2, an MRS comprises a collaboration of n robots with a leader–follower communication topology. Consequently, an attacker can launch attacks on both the root robot and non-root robots within the MRS. Furthermore, the attacker can exploit reachable robots to execute attacks. Therefore, it becomes crucial to assess the performance of the proposed resilient, adaptive control mechanism under such scenarios. Figures 5–7 shows the response of MRS under Byzantine attack on the root robot, non-root robot, and reachable robot. It is easy to validate that although attacks impacted the performance of MRS, i.e., spikes in the response of MRS for a short interval; after that, MRS achieved the input state.



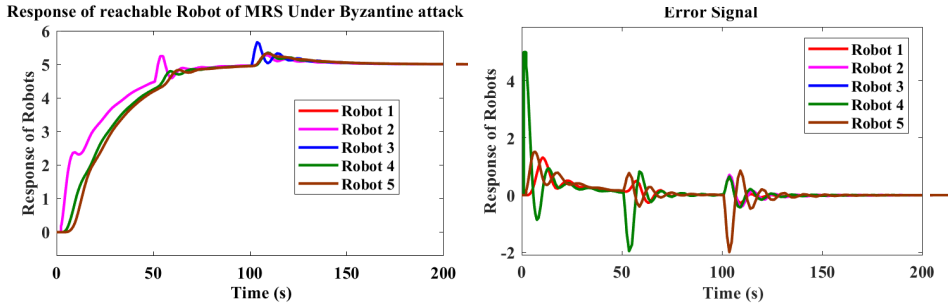
(**a**) Response of MRS. (**b**) Error signal.

Figure 5. Response of the root robot of MRS under Byzantine attack.



(**a**) Response of MRS. (**b**) Error signal.

Figure 6. Response of the non-root robot of MRS under Byzantine attack.



(**a**) Response of MRS. (**b**) Error signal.

Figure 7. Response of the reachable robot of MRS under Byzantine attack.

According to simulation results, one can verify that the proposed control technique verifies the Theorems 1 and 2 to provide consensus tracking within finite time tracking. Furthermore, the proposed technique provides a consensus control, which is resilient for the MRS under Byzantine attacks and independent of communication topology, according to Theorems 3 and 4. Therefore, it is easy to say that MRS achieves consensus despite Byzantine attacks on different robots using resilient, adaptive sliding mode controllers in a finite time.

8. Discussions

In this section, we discuss the impact of the outcome of our proposed SMC architecture and articulate its limitations. Furthermore, we convert this control problem to a corresponding computational problem to address some of those limitations.

8.1. Limitations in the Context of the Industrial Internet of Things

The proposed approach of SMC has some limitations in the context of the Industrial Internet of Things (IIoT). An IIoT can have multiple MRS operations simultaneously. Each MRS may be doing the same task, such as in an Assembly line, or different tasks, such as in a smart building.

- *Scalability*: In IIoT, multiple machines need to connect and retrieve information from the same cloud-based platforms. This means that cloud-based platforms need to store and maintain a large amount of information about a wide variety of devices, their tasks, and constraints over a period of time. While the proposed SMC can operate within a single network of MRS in a localized environment, it will become difficult to achieve the same results if there is an adverse change to the structure of the network, such as a specific robot being replaced or when there is additional latency in the network.
- *Device Characterization*: For an IIoT to operate smoothly, it needs to understand the operational model, i.e., the normal vs. abnormal changes in the state space of each machine. Only when each device is in the acceptable range of state space, both historically and in the expected near future, the IIoT can achieve a smooth operation within a given MRS. While the SMC-based approach can achieve success for a given MRS, it may be difficult for the IIoT to identify the source or the cause of the problem and then potentially resolve it, if ad hoc devices with different configurations are used to do the same task.

In order to solve these issues, it is necessary to convert this control problem into a computational problem. Once the MRS operation can be modeled as a set of streaming data, it can open wide-ranging possibilities for IIoT applications.

8.2. The Dataset from MRS

The data used in this paper are based on a simulated environment in MATLAB and according to the simulation results, the tracking of the performance of MRS, as given in Equation (1), can also be recorded as in Table 1 given below. Table 1 shows the change in

the dynamics of the robots in the MRS. It is also clear from Table 1 that, for time intervals, the states of robots are changing based on their activities. If there are disturbances within MRS, such as Byzantine attacks, then the state of robots would have different values, which can be minimized by our proposed controller. The time gap between the data is in milliseconds or lower. This tabular form of data can also be fed into AI algorithms.

Table 1. Simulation data (snippet).

Time	Robot 1	Robot 2	Robot 3	Robot 4	Robot 5
6.0867797	0.011526677	0.011526677	0.00000750	0.0000284	0.0000000923
6.6949063	0.028332115	0.028332115	7.28×10^{-5}	0.000249229	0.00000797
7.2702540	0.051661765	0.051661765	0.000334421	0.000997438	0.00000194
7.8456017	0.080865055	0.080865055	0.000967632	0.002576603	0.00000129
8.4083543	0.113812034	0.113812034	0.002142051	0.005176358	0.0000475
9.0975471	0.157742522	0.157742522	0.004448755	0.00980112	0.000145903
9.9972364	0.219070324	0.219070324	0.009357638	0.018625688	0.000442586
10.978108	0.287433046	0.287433046	0.018519446	0.033050535	0.001244096
11.831678	0.342413388	0.342413388	0.031352352	0.050596698	0.002848768
12.640486	0.387468685	0.387468685	0.047089502	0.069898913	0.005431664
13.610870	0.43317562	0.43317562	0.069433143	0.095037967	0.009993675
14.733735	0.471740672	0.471740672	0.100646537	0.126665105	0.018196414
15.887332	0.492845701	0.492845701	0.138161633	0.160421107	0.031336091
17.066103	0.498886848	0.498886848	0.179118543	0.193642133	0.050370389
18.416865	0.495163287	0.495163287	0.225244768	0.228426584	0.078504275

9. Future Applications with Discrete Event Systems and Artificial Intelligence

The proposed control strategy is resilient enough against the Byzantine attacks on the MRS and provides robust performance of the MRS. However, the real-time tracking of the performance of MRS, as given in Equation (1), can be ensured through intelligent techniques, such as digital twin, machine learning, deep learning, reinforcement learning, etc. For example, the resilience of MRS against cyber attacks such as Byzantine attacks can be increased through IoT-based digital twin technology.

Regarding operation, the above MRS can be viewed as a Discrete Event System (DES). Each robot in the system uses a microcontroller with an expected range of state spaces and the change of the states. Suppose that the IIoT (Industrial Internet of Things) devices contain a controller that generates control instructions for the machine to change its state or orientation. There can be multiple controllers within an IIoT system, and they can be operated cooperatively. For example, in the MRS, controllers are responsible for deciding how much power is supplied to a particular robot within an MRS, depending on its task type. Similarly, the allocation of a task to the robot in an MRS is also controlled by the controller based on time consumption or other factors. Every time an MRS receives a control signal, the state also changes with time. Therefore, the change of state space or orientation in an MRS can be derived from Equations (1) and (11) as:

$$\begin{aligned} \text{Input states} &= AX + BU, \\ \text{Output states} &= CX \end{aligned}$$

where A represents the state of the MRS evolving with the change in time T, X is the input state vector at a particular time, B contains the controlled inputs (generated by the controllers), U is the desired input value, and C is the output matrix used to represent how X contributes to the system's output.

Based on state space relation, the data of any IIoT system having a complex control system can be represented through the data given below in Table 2.

Table 2. States of the IIoT system including three actuators with time.

Time	State (m_1)	State (m_2)	State (m_3)
t_1	a_{11}	a_{12}	a_{13}
t_2	a_{21}	a_{22}	a_{23}
t_3	a_{31}	a_{32}	a_{33}

This is an equivalent rendering of the data in Table 1 concerning the state space of a particular device in the IIoT system. Here:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix},$$

represent the states of the IIoT system, which changes with respect to the time t_1, t_2, t_3. Hence, it is clear that these data are used to make decisions, such as predictions of the current state, future state, and performance, or it can be used for other operations. An MRS can perform a task β_t at a given time t. β contains a set of states $\{\alpha_{xy}\}$ as defined by the state of the actuators m. A set of α with size k^i may be followed by another set of time-bound α states. Each of these time-bound sets of α is non-time-bound with respect to each other.

Every time a machine receives a control signal, the state is expected to change. After getting data matrices representing the state of $(m_1, m_2...)$ at every interval, it can be fed into machine learning or any other intelligent algorithm to predict the expected future states with decreasing order of probabilities. This can be compared to the current state information to determine whether it has fulfilled the required conditions at the current time. The data can be analyzed using a machine learning algorithm that can be useful to establish an autonomous system, which can further predict the machine's performance, future possible failure, possible solutions to faults, attacks, etc. Based on the above explanation, future research can investigate the following:

1. In the case of the complex IIoT control system, we can design a '*model*' with the help of intelligent schemes such as Artificial Intelligence/Machine learning/Deep Reinforcement Learning. Given that the control systems' architecture is fixed but *unknown*, a behavioral model of the devices must be created. Training of the *Neural Network* can be completed based on the set of α, which can be used to classify the current state β_t and predict the future states, i.e., β_{t+1}, as shown in Figure 8.
2. It can also be used to classify *faults* or *errors*, i.e., $(\beta_{predicted} - \beta_{actual})$, an IIoT system faces with minimal supervisory data and training. In designing such a device, suppose a closed-loop feedback complex IIoT system that uses its feedback information to diagnose the variations and faults, as shown in Figure 8. A controller can be designed to ensure adaptive stability if the IIoT system contains faults due to internal or external disturbance (communication and induced delays, cyber attacks). A method can be developed based on recurrent neural networks (RNN) and SMC to measure the expected model's variations based on the system's known control state space.
3. The architecture of the IIoT system is based on IoT, and it is changing periodically due to the evolution of advanced technologies used to implement it. Therefore, IIoT systems often inherit the security challenges of IoT. Since IIoT systems are desired to be distributed rather than centralized, they are vulnerable to certain cyber attacks such as DoS attacks, deception attacks, Byzantine attacks, false data injection attacks, etc. Hence, there is a requirement to consider such attacks carefully. For this, a model can be designed to detect the attacks and types of attacks and minimize the attack effects.

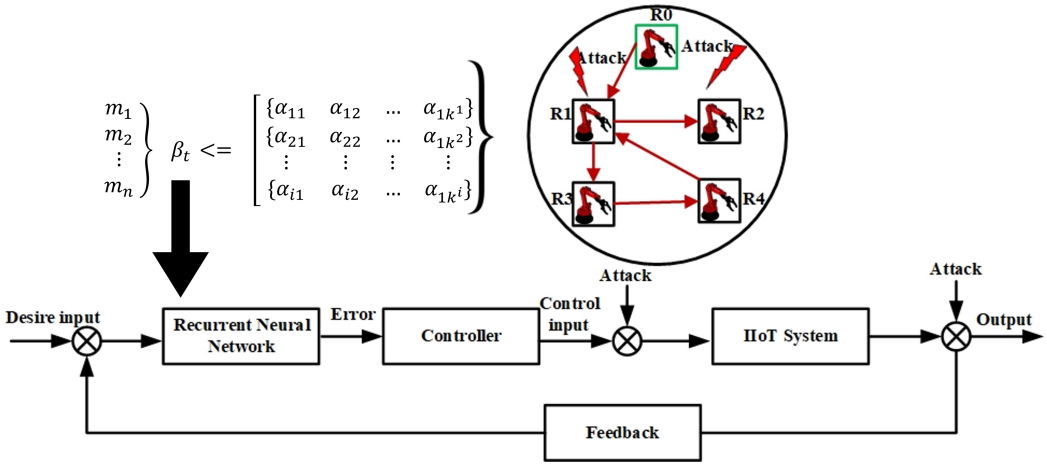


Figure 8. RNN- and SMC-based closed-loop feedback control mechanism for an IIoT system.

9.1. Example Applications 1—Detecting Network Attacks

The proposed techniques will be able to detect the type of Byzantine attack on IIoT systems. For example, in the case of MRS, whether attacks are either root robot or non-root or the whole MRS is under attack, whenever the attack is detected, an observer algorithm based on a what-if state can be deployed to take corrective actions to ensure seamless and safe MRS operations. Furthermore, digital twins can present a constructible active model for communicating between the attackers and the defense technique.

For creating a digital twin and processing the data stream in real-time, the computational algorithms need the condition of the MRS as a set of matrices or similar data structures. These can be used with existing machine learning and deep learning algorithms for *behavior modeling* or *state space modeling* of the MRS. The mathematical modeling of MRS in terms of digital twins is given below.

According to Equations (1) and (2), the state space representations of the physical thing of MRS can be written as:

$$\begin{aligned} \dot{Y}^{\psi} &= A^{\Phi} Y^{\psi} + B^{\Phi} U^{\psi} \\ X^{\psi} &= C^{\Phi} Y^{\psi} \end{aligned} \tag{48}$$

where Y^{ψ} and U^{ψ} denote the states and input to the physical MRS, respectively.

The attack signal, given in Equation (5), on the physical MRS, can be represented as a feature vector at time t:

$$f_i^{\psi}(t) = \beta_i u_i^{\psi}(t) + ck \sum_{n_i} a_{ij}(\alpha_j y_j^{\psi} - \alpha_i y_i^{\psi}). \tag{49}$$

Similarly, state space representations of cyber MRS can be written as:

$$\begin{aligned} \dot{Y}^{\theta} &= A^{\theta} Y^{\theta} + B^{\theta} U^{\theta} \\ X^{\theta} &= C^{\theta} Y^{\theta} \end{aligned} \tag{50}$$

where θ is used to represent cyber things. Furthermore, Y^{θ} and U^{θ} denote the states and input to the cyber MRS, respectively.

The attack on the cyber MRS can be written as:

$$f_i^{\theta}(t) = \beta_i u_i^{\theta}(t) + ck \sum_{n_i} a_{ij}(\alpha_j y_j^{\theta} - \alpha_i y_i^{\theta}). \tag{51}$$

Based on Equations (48) and (50), the hybrid MRS model to represent the overall behavior of MRS can be represented as:

$$\begin{bmatrix} \dot{Y}^{\theta} \\ \dot{Y}^{\psi} \end{bmatrix} = \begin{bmatrix} A^{\theta} & 0 \\ B^{\Phi}C^{\theta} & A^{\Phi} \end{bmatrix} \begin{bmatrix} Y^{\theta} \\ Y^{\psi} \end{bmatrix} + \begin{bmatrix} B^{\theta} \\ 0 \end{bmatrix} U^{\theta}$$
$$\begin{bmatrix} Y^{\theta\psi} \end{bmatrix} = \begin{bmatrix} 0 & C^{\Phi} \end{bmatrix} \begin{bmatrix} Y^{\theta} \\ Y^{\psi} \end{bmatrix} \quad (52)$$

These can be streamed in real time and sampled or batched for further processing. Such batches can be used to train a model based on existing data on the MRS performance and known deviations. A deviation beyond an acceptable threshold can be used to classify the current and future state of the MRS in a desired future time frame.

Equation (52) can be used to monitor the performance of MRS due to the sharing of information between physical things and cyber things in the hybrid model. Any anomaly in the MRS can be detected very easily using digital twin technology. Therefore, more accurate and safer MRS operations can be ensured than other conventional techniques. Furthermore, the performance of the MRS will also be increased due to the corrective actions in the presence of anomalies such as Byzantine attacks. Furthermore, it is known that a Byzantine robot is hard to identify. Therefore, a digital twin for resilient control of MRS in the presence of a Byzantine attack can be a very useful technique.

Similarly, the proposed work can be extended using AI-based algorithms. In this work, a supervisory robot *Rl* can be well-trained using recorded information of Equations (1), (2), and (5). The trained supervisory robot *Rl* will be placed at the top of the other five robots, as shown in Figure 9. If the supervisory robot *Rl* is well trained, then it can be used to detect and prevent the attack from happening based on Equation (5). For example, if the supervisory robot can detect that an attack has started to occur. Then, it can prevent the attack effects by notifying all the other robots that an attack has happened to come to the default state, e.g., reboot. This can be achieved by classification of data obtained through Equations (1), (2), and (5).

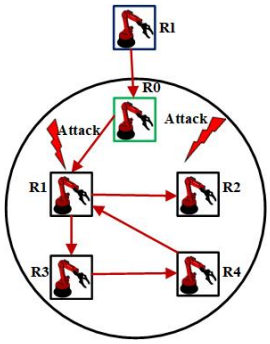


Figure 9. Future communication topology.

9.2. Example Applications 2—Comparative Digital Twins

Let us consider a developer company that manufactures high-cost equipment and sells it to many users. The device has a high level of flexibility in usage. This means the device can be used in a variety of ways, i.e., flexible in state space. Typically, the manufacturer has no direct control over the device after the device is installed. If the manufacturer wants to monitor the device in real time, it can create a comparative digital twin to monitor and analyze the use of devices by different customers. In this way, the manufacturer will be able to determine the reasons for the customer's device performance degradation at various rates concerning time between multiple users. Using the proposed outcomes and artifacts of the above research, the developer can compare the different users (human or master devices) using the same or similar devices and potentially suggest factors of what a user/customer did incorrectly, causing their devices to break down earlier compared to others. The proposed research outcomes will play an important role in Industry 5.0 practices. It can enable human users to adopt machine technology or autonomous systems and quickly set up their business aims.

10. Conclusions

This article proposed an adaptive, resilient consensus control technique for the MRS under the Byzantine technique using the SMC method. First, the accuracy of the proposed resilient consensus control scheme was ensured using the SMC method, and then the robustness of the proposed SMC-based scheme in the presence of Byzantine attacks was proved. Second, an attack observer is designed to approximate the effects of Byzantine attacks on the MRS and the effects of chattering removed through integral SMC. Similarly, the proposed integral SMC method can automatically tune the gain and performs well without prior knowledge of Byzantine attacks. In the end, the effectiveness of the proposed mechanism is verified through simulation results. The time series data used in controlling the MRS can be used for training machine learning models, such as RNN, in the future. Such a method can be used to create a model of any machine without knowing the actual mechanics of the device, which will be an extension of this in the future.

Author Contributions: Conceptualization, M.N. and A.M.; methodology, M.N. and A.M.; software, M.N.; validation, M.N. and A.M.; formal analysis, M.N.; investigation, M.N. and A.M.; resources, M.N. and A.M.; data curation, M.N.; writing—original draft preparation, M.N.; writing—review and editing, M.N. and A.M.; visualization, M.N. and A.M.; supervision, A.M.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors do not have any conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MRS	Multi-robot system
IoT	Internet of Things
ROS	Robot operating system
SMC	Sliding mode control

References

1. Wei, H.; Lv, Q.; Duo, N.; Wang, G.; Liang, B. Consensus algorithms based multi-robot formation control under noise and time delay conditions. *Appl. Sci.* **2019**, *9*, 1004. [CrossRef]
2. Mao, W.; Liu, Z.; Liu, H.; Yang, F.; Wang, M. Research progress on synergistic technologies of agricultural multi-robots. *Appl. Sci.* **2021**, *11*, 1448. [CrossRef]
3. Nasir, M.; Ahmed, Z.; Ali, N.; Saeed, M.A. H_∞ performance tracking and group consensus of delayed multiagent systems under attack. *J. Vib. Control* **2023**. [CrossRef]
4. Liang, W.; Ning, Z.; Xie, S.; Hu, Y.; Lu, S.; Zhang, D. Secure fusion approach for the internet of things in smart autonomous multi-robot systems. *Inf. Sci.* **2021**, *579*, 468–482. [CrossRef]
5. Chen, D.; Chen, K.; Li, Z.; Chu, T.; Yao, R.; Qiu, F.; Lin, K. Powernet: Multi-agent deep reinforcement learning for scalable powergrid control. *IEEE Trans. Power Syst.* **2021**, *37*, 1007–1017. [CrossRef]
6. Al-Hussaini, S.; Gregory, J.M.; Gupta, S.K. Generating Task Reallocation Suggestions to Handle Contingencies in Human-Supervised Multi-Robot Missions. *IEEE Trans. Autom. Sci. Eng.* **2023**, *21*, 367–381. [CrossRef]
7. Aranda, M.; Aragüés, R.; López-Nicolás, G. Combined leaderless control of translational, shape-preserving and affine multirobot formations. *IEEE Robot. Autom. Lett.* **2023**, *8*, 7567–7574. [CrossRef]
8. Fu, J.; Wen, G.; Yu, X.; Huang, T. Robust collision-avoidance formation navigation of velocity and input-constrained multirobot systems. *IEEE Trans. Cybern.* **2023**, *54*, 1734–1746. [CrossRef]
9. Dong, S.; Li, Y. Adaptive Fuzzy Event-Triggered Formation Control for Nonholonomic Multirobot Systems with Infinite Actuator Faults and Range Constraints. *IEEE Internet Things J.* **2023**, *11*, 1361–1373. [CrossRef]

10. Herguedas, R.; Aranda, M.; López-Nicolás, G.; Sagüés, C.; Mezouar, Y. Double-integrator multirobot control with uncoupled dynamics for transport of deformable objects. *IEEE Robot. Autom. Lett.* **2023**, *8*, 7623–7630. [CrossRef]
11. Hu, B.B.; Zhang, H.T.; Yao, W.; Ding, J.; Cao, M. Spontaneous-Ordering Platoon Control for Multirobot Path Navigation Using Guiding Vector Fields. *IEEE Trans. Robot.* **2023**, *39*, 2654–2668. [CrossRef]
12. Rossi, E.; Tognon, M.; Ballotta, L.; Carli, R.; Cortés, J.; Franchi, A.; Schenato, L. Coordinated multi-robot trajectory tracking control over sampled communication. *Automatica* **2023**, *151*, 110941. [CrossRef]
13. Ferranti, L.; Lyons, L.; Negenborn, R.R.; Keviczky, T.; Alonso-Mora, J. Distributed nonlinear trajectory optimization for multi-robot motion planning. *IEEE Trans. Control Syst. Technol.* **2022**, *31*, 809–824. [CrossRef]
14. He, S.; Lyu, W.; Liu, F. Robust H_∞ sliding mode controller design of a class of time-delayed discrete conic-type nonlinear systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *51*, 885–892. [CrossRef]
15. Song, J.; Wang, Y.K.; Niu, Y.; Lam, H.K.; He, S.; Liu, H. Periodic event-triggered terminal sliding mode speed control for networked PMSM system: A GA-optimized extended state observer approach. *IEEE/ASME Trans. Mechatron.* **2022**, *27*, 4153–4164. [CrossRef]
16. Tasooji, T.K.; Marquez, H.J. Decentralized event-triggered cooperative localization in multirobot systems under random delays: With/without timestamps mechanism. *IEEE/ASME Trans. Mechatron.* **2022**, *28*, 555–567. [CrossRef]
17. Nasir, M.; Hayat, M.F.; Jamal, A.; Ahmed, Z. Frequency domain consensus control analysis of the networked multi-agent system with controller area network bus–induced delay. *J. Vib. Control* **2022**, *28*, 2900–2912. [CrossRef]
18. Zhang, K.; Li, Z.; Wang, Y.; Louati, A.; Chen, J. Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control. *Automatica* **2022**, *139*, 110182. [CrossRef]
19. Alsamhi, S.H.; Shvetsov, A.V.; Shvetsova, S.V.; Hawbani, A.; Guizani, M.; Alhartomi, M.A.; Ma, O. Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration. *IEEE Trans. Green Commun. Netw.* **2022**, *7*, 328–338. [CrossRef]
20. Zhou, L.; Kumar, V. Robust multi-robot active target tracking against sensing and communication attacks. *IEEE Trans. Robot.* **2023**, *39*, 1768–1780. [CrossRef]
21. Bonczek, P.J.; Peddi, R.; Gao, S.; Bezzo, N. Detection of nonrandom sign-based behavior for resilient coordination of robotic swarms. *IEEE Trans. Robot.* **2022**, *38*, 92–109. [CrossRef]
22. Han, Z.; Wang, W.; Huang, J.; Wang, Z. Distributed adaptive formation tracking control of mobile robots with event-triggered communication and denial-of-service attacks. *IEEE Trans. Ind. Electron.* **2022**, *70*, 4077–4087. [CrossRef]
23. Yin, T.; Gu, Z.; Xie, X. Observer-based event-triggered sliding mode control for secure formation tracking of multi-UAV systems. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 887–898. [CrossRef]
24. Usevitch, J.; Panagou, D. Resilient trajectory propagation in multirobot networks. *IEEE Trans. Robot.* **2021**, *38*, 42–56. [CrossRef]
25. He, W.; Xu, W.; Ge, X.; Han, Q.L.; Du, W.; Qian, F. Secure control of multiagent systems against malicious attacks: A brief survey. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3595–3608. [CrossRef]
26. Szynkiewicz, W.; Niewiadomska-Szynkiewicz, E.; Lis, K. Deep Learning of Sensor Data in Cybersecurity of Robotic Systems: Overview and Case Study Results. *Electronics* **2023**, *12*, 4146. [CrossRef]
27. Dutta, V.; Zielińska, T. Cybersecurity of robotic systems: Leading challenges and robotic system design methodology. *Electronics* **2021**, *10*, 2850. [CrossRef]
28. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **2022**, *21*, 115–158. [CrossRef]
29. Deng, G.; Zhou, Y.; Xu, Y.; Zhang, T.; Liu, Y. An investigation of byzantine threats in multi-robot systems. In Proceedings of the RAID '21: 24th International Symposium on Research in Attacks, Intrusions and Defenses, San Sebastian, Spain, 6–8 October 2021; pp. 17–32.
30. Ferrer, E.C. ; Jiménez, E.; Lopez-Presa, J.L.; Martín-Rueda, J. Following leaders in byzantine multirobot systems by using blockchain technology. *IEEE Trans. Robot.* **2021**, *38*, 1101–1117. [CrossRef]
31. Kumar, A.; Bhatia, S.; Kaushik, K.; Gandhi, S.M.; Devi, S.G.; Diego, A.D.J.; Mashat, A. Survey of promising technologies for quantum drones and networks. *IEEE Access* **2021**, *9*, 125868–125911. [CrossRef]
32. Keramat, F.; Queralta, J.P.; Westerlund, T. Partition-tolerant and byzantine-tolerant decision-making for distributed robotic systems with iota and ROS 2. *IEEE Internet Things J.* **2023**, *10*, 12985–12998. [CrossRef]
33. Luo, J.; Shu, X.; Zhai, Y.; Fu, X.; Ding, B.; Xu, J. A Fast and Robust Solution for Common Knowledge Formation in Decentralized Swarm Robots. *J. Intell. Robot. Syst.* **2022**, *106*, 68. [CrossRef]
34. Lü, S. ; Jin, X.; Ding, L.; Tan, Q. Adaptive sliding-mode control of a class of disturbed cyber–physical systems against actuator attacks. *Comput. Electr. Eng.* **2021**, *96*, 107492. [CrossRef]
35. Corradini, M.; Cristofaro, A. A sliding-mode scheme for monitoring malicious attacks in cyber-physical systems. *IFAC-PapersOnLine* **2017**, *50*, 2702–2707. [CrossRef]
36. Li, M.; Chen, Y.; Zhang, Y.; Liu, Y. Adaptive sliding-mode tracking control of networked control systems with false data injection attacks. *Inf. Sci.* **2022**, *585*, 194–208. [CrossRef]
37. Mukherjee, P.; Santilli, M.; Gasparri, A.; Williams, R.K. Distributed Adaptive and Resilient Control of Multi-Robot Systems With Limited Field of View Interactions. *IEEE Robot. Autom. Lett.* **2022**, *7*, 5318–5325. [CrossRef]

38. Tasooji, T.K.; Marquez, H.J. Event-triggered consensus control for multirobot systems with cooperative localization. *IEEE Trans. Ind. Electron.* **2022**, *70*, 5982–5993. [CrossRef]
39. Tasooji, T.K.; Khodadadi, S.; Marquez, H.J. Event-Based Secure Consensus Control for Multirobot Systems With Cooperative Localization Against DoS Attacks. *IEEE/ASME Trans. Mechatron.* **2023**, *29*, 715–729. [CrossRef]
40. He, S.; Xu, Y.; Wu, Y.; Li, Y.; Zhong, W. Adaptive consensus tracking of multi-robotic systems via using integral sliding mode control. *Neurocomputing* **2021**, *455*, 154–162. [CrossRef]
41. Ahmed, Z.; Saeed, M.A.; Jenabzadeh, A.; Xu, X.; Zhang, W. Frequency domain resilient consensus of multi-agent systems under IMP-based and non IMP-based attacks. *Automatica* **2022**, *146*, 110582. [CrossRef]