Article

Mean Square Consensus of Nonlinear Multi-Agent Systems under Markovian Impulsive Attacks

Huan Luo [1,2] , **Yinhe Wang** [1], **Xuexi Zhang** [1,*], **Peitao Gao** [1] and **Haoxiang Wen** [2]

[1] School of Automation, Guangdong University of Technology, Guangzhou 510006, China; luohuan@sgu.edu.cn (H.L.); yinhewang@sina.com (Y.W.); peitao_gao@sina.com (P.G.)

[2] School of Intelligent Engineering, Shaoguan University, Shaoguan 512026, China; xiangxiang_0@163.com

* Correspondence: zxxnet@gdut.edu.cn; Tel.: +86-020-3932-2961

Abstract: This paper focuses primarily on the mean square consensus problem of a class of nonlinear multi-agent systems suffering from stochastic impulsive deception attacks. The attacks here are modeled by completely stochastic destabilizing impulses, where their gains and instants satisfy all distributions and the Markovian process. Compared with existing methods, which assume that only gains are stochastic, it is difficult to deal with systems with different types of random variables. Thus, estimating the influence of these different types on the consensus problem is a key point of this paper. Based on the properties of stochastic processes, some sufficient conditions to solve the consensus problem are derived and some special cases are considered. Finally, a numerical example is given to illustrate the main results. Our results show that the consensus can be obtained if impulsive attacks do not occur too frequently, and it can promote system stability if the gains are below the defined threshold.

Keywords: consensus; multi-agent systems; impulsive attacks; deception attacks; stochastic process

1. Introduction

With the development of hardware equipment and communication technology, the collaborative control problem has recently become the focus of studies of complex systems [1–3]. The consensus of multi-agent systems (MASs) plays an important role in the field of collective behaviors, owing to its excellent model assumptions and extensive application scenarios such as control of the formation of unmanned aerial vehicles [4], restoration of a power system [5], intelligent and sustainable supplier selection of supply chains [6], etc.

In real-world application scenarios, communication among agents may be affected by the environment or various attacks, especially human-made malicious attacks, which is likely to cause the system to become unstable. For attack scenarios, generally speaking, they may be classified into two main categories: denial-of-service (DoS) attacks [7–10] and deception attacks [11–13] (for more details, refer to [14]). DoS attacks are attacks that make the data of sensors and controllers unavailable, resulting in packet time delays or packet drops in the signal transmission. In contrast, deception attacks are attacks that have the ability to obtain and tamper with the transmitting data and the commands from controllers. DoS attacks can destroy communication topologies and can damage the stability of the systems. Compared with DoS attacks, deception attacks are more moderate and difficult to detect, which quietly makes the system unstable. Thus, deception attacks have attracted a lot of interest and has become one of our main concerns. Much research on deception attacks has been conducted in recent years [15–19]. For instant, consider the existence of false data injection attacks; the authors in [16] investigated the security issue in the state estimation problem of a networked control system. Similarly, in the presence of deception attacks, the authors [19] studied secure synchronization of MASs by means of impulsive control. However, in the above research, the results were based on a linear or an additive assumption and assumptions on the attack model were made, resulting in narrow scopes of applications.

Taking this restriction into account, models with more simulation significance and practical application value were established by means of stochastic processes, especially the Bernoulli distribution [20–24], in which the gains of attacks were assumed to be a stochastic Bernoulli variable. For example, the authors in [21] investigated the consensus of linear MASs under deception attacks with stochastic Bernoulli variables. It is worth noting that the attacks mentioned above were described as discrete events. When the state of the system suffers instantaneous disturbances and experiences sudden changes at certain moments, the system may be attacked. This is a so-called impulsive attack. An impulsive attack is a form of attack that causes instantaneous changes to the state of the system. Models of impulsive attacks with stochastic gains seem to be sufficiently good at neglecting positions. However, in actuality, such a problem is also vital to the stability of systems as we do not know a priori when attacks are made. Suppose that both the gains and instants of the impulsive attacks are stochastic. The author in [25] first considered these two characteristics of an attack, and then, some sufficient conditions for almost stable general Lipschitz-type nonlinear systems were derived. However, the work in [25] still used restricted gains under the Bernoulli distribution and the influence of attacks was assumed to monotonically decrease, which become restrictive assumptions.

On the other hand, focused on the variability in an environment, a model relying on a Markovian chain is appropriate in general. Taking this into account, the consensus with Markovian switching topologies has become a hot issue regarding the performance of multi-agent systems with external disturbances. However, most existing methods such as the works in [26,27] for a consensus with attacks only considered cases where topologies or systems contained Markovian properties rather than attacks. Though some authors did assess attacks in a Markovian form such as the works in [9,28], most of these works were concerned with DoS attacks; the type of variable chosen, such as gains; or assumptions about the effects of a combination of attacks instead of deception attacks. As a result, the works above do not fully consider the characteristics of the attack, and thus, a general work on both gains and instants of deception attacks still has not yet been conducted.

With the discussion above, this paper aims to establish a more universal model for deception attacks and provides some sufficient conditions for the consensus of multi-agent systems. The contributions of this paper can be summed up as follows:

- Taking destabilizing impulse into account, and based on the Markovian properties, a general model for impulsive deception attacks is established, where the gains do not obey any specific distribution and instants are assumed to obey the Markovian chain.
- In addition, some special cases including both the characteristics of attacks and Markovian properties are considered.

The remainder of this paper is organized as follows. The main results about the consensus for system (1) are derived in Section 3 based on the novel model for the impulsive deception attacks introduced in Section 2, and a corresponding numerical example is provided in Section 4. The conclusion and some interesting topics of future work are given in Section 5.

Notation 1. *Let $\mathbb{R}$ be a set of real numbers and $\mathbb{N}$ be a set of positive integers. Let $\mathbb{R}^n$ be the n-dimensional Euclidean space; furthermore, I_n is the n-dimensional identity matrix and 1_n is the n-dimensional column vector with one element. Let M be a matrix or vector, for which the transposition is represented by M^T, and its deduced norm or norm is represented by $|M|$. Let $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$ denote the largest and nonzero smallest eigenvalue of the matrix A, respectively. A matrix B is said to be a symmetric positive definite matrix if $B = B^T$ and $x^T B x > 0$ for any nonzero vector x. For any function $h : \mathbb{R} \to \mathbb{R}$, we define $h(t^+) = \lim_{\Delta t \to 0^+} h(t + \Delta t), h(t^-) = \lim_{\Delta t \to 0^-} h(t + \Delta t)$. In addition, let $(\Omega, \mathcal{F}, \mathcal{F}_{t \geq 0}, \mathcal{P})$ be a complete probability space with respect to the filtration $\mathcal{F}_{t \geq 0}$, which satisfies the common conditions, i.e., right continuous and $\mathcal{F}_0$ contains all $\mathcal{P}$-null sets. Let $\mathbb{E}[\cdot]$ ($\mathbb{E}[\cdot|\cdot]$) denote the (conditional) expectation of a stochastic process.*

2. Preliminaries

Before presenting the system models and the problem statement, we first give some necessary knowledge about graph theory, which is used to describe the communication topology among MASs. In this paper, we consider the MASs with N agents and the topology can be represented by a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$, where $\mathcal{V}$ is the set of vertices, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of edges, and $\mathcal{A} = [a_{ij}]_{N \times N}$ is called the adjacency matrix. When the jth agent sends information to the ith agent, there exists an edge between them and $a_{ij} = 1$; otherwise, $a_{ij} = 0$. Let the diagonal matrix $D = diag\{\bar{d}_i\}$ be the in-degree matrix and $\bar{d}_i = \sum_{j=1}^{N} a_{ij}, i = 1, 2, \ldots, N$. Then, the Laplacian matrix $L = [l_{ij}]_{N \times N}$ can be defined as $L = D - \mathcal{A}$, where $l_{ij} = -a_{ij}, i \neq j$ and $l_{ii} = \sum_{j \neq i}^{N} a_{ij}$.

Let us consider that generally nonlinear multi-agent systems (NMASs) consist of N agents and that each can be described as follows:

$$\dot{x}_i(t) = Ax_i(t) + Bf(x_i(t)) + Cu_i(t), \quad t \geq t_0. \tag{1}$$

where $x_i(t) \in \mathbb{R}^n$ and $u_i(t) \in \mathbb{R}^n$ are the system state and external input control, respectively. Function $f : \mathbb{N}^n \to \mathbb{N}^n$ denotes the nonlinear items satisfying the well-known Lipschitz condition. A, B, and C are constant matrices with approximate dimensions.

Before presenting the controller considered in this paper, we first provide some explanations about the impulsive deception attacks, so that readers can understand the design of the controller more clearly. The configuration of NMASs under impulsive deception attacks is shown in Figure 1. Generally, controllers generate control signals according to states measured by sensors and then send them to the actuators. For MASs, data transmissions are heavily dependent on topologies and wireless transmission technology. If attackers launch data modification or false data attacks to topologies in discrete-time manners or calls impulsive attacks, they result in instantaneous jumps in the transmitted signal.
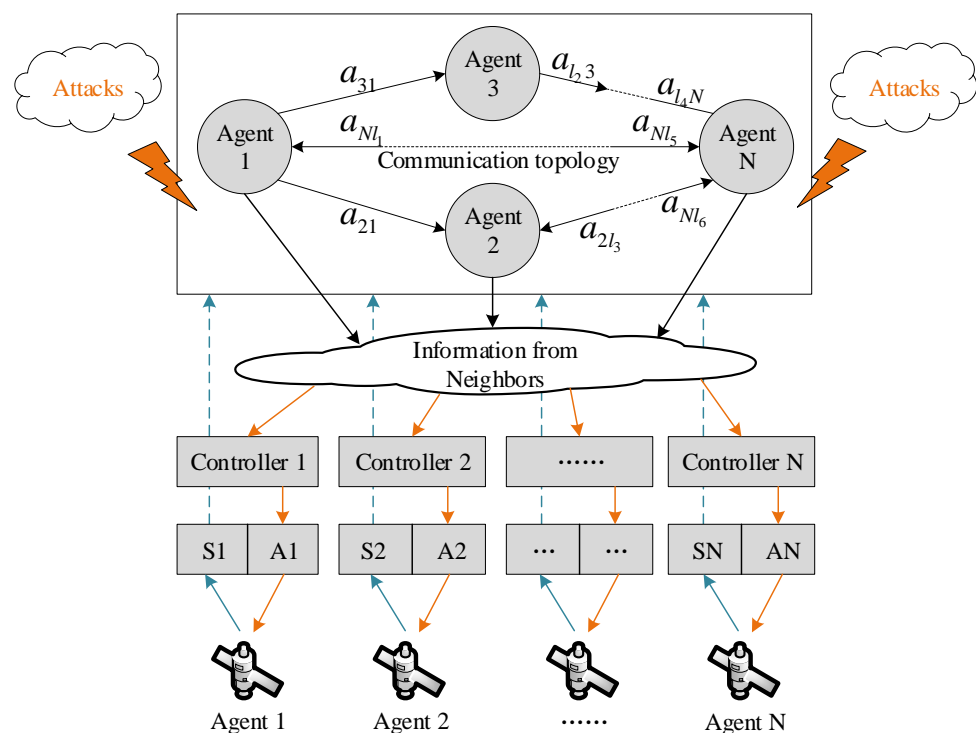

Figure 1. Configuration of NMASs under impulsive deception attacks (where Ai and Si denote the actuator and sensor of the ith agent, respectively, and l_i denotes the l_ith agent, $i = 1, 2, \ldots, N$).

Under the configuration reflected in Figure 1, in this paper, we consider the following common linear feedback controller under Markovian impulsive attacks:

$$u_i(t) = K \sum_{j=1}^{N} a_{ij}(x_j(t) - x_i(t)) + \sum_{k=1}^{+\infty} d_k x_i(t)\delta(t - t_k). \tag{2}$$

where $K \in \mathbb{R}$ is the feedback gain for designed controller. Let $\mathbb{I} := \{t_k\}_{k=1}^{+\infty}$ denote the impulsive sequence in Dirac form, i.e., the function δ, and d_k denotes the impulsive gains. In addition, we assume that $x_i(t)$ is right-hand continuous at $t = t_k$, meaning that $x_i(t_k^+) = x_i(t_k)$. Since the destabilizing impulse is adopted to model the impulsive attacks here, one can obtain the fact that $d_k > 0$ or $d_k < -2$. Note that $\sum_{k=1}^{+\infty} d_k x_i(t)\delta(t - t_k)$ here denotes impulsive attacks.

Remark 1. *Let $T_i(t, t_0)$ and $\bar{N}_i(t, t_0)$ denote the total impulsive intervals and the occurrence number for the ith modes of impulses over the interval $[t_0, t]$, respectively. Hence, we have $\bar{N}(t, t_0) = \sum_{i=1}^{p} \bar{N}_i(t, t_0)$, which denotes the total number of impulses over the interval $[t_0, t]$.*

Considering that the stabilization problem of an error system with ideal dynamics is a common method to tackle the consensus of multi-agent systems. Define the error state as $e_i(t) := x_i(t) - \bar{x}(t) = x_i(t) - \frac{1}{N}\sum_{i=1}^{N} x_i(t)$, which also can be written as $e(t) = [e_1^T(t), e_2^T(t), \ldots, e_N^T(t)]^T = Ex(t) = ((I_N - \frac{1}{N}1_N 1_N^T) \otimes I_n)x(t)$, and the vector of states $x(t) = [x_1^T(t), x_2^T(t), \ldots, x_N^T(t)]^T$. Then, we can rewrite system (1) with controller (2) in the error system in a compact form as follows:

$$\begin{cases} \dot{e}(t) = He(t) + \bar{B}F(e(t)), & t \neq t_k, t \geq t_0 \\ e(t_k) = \eta_k e(t_k^-), & t = t_k. \end{cases} \tag{3}$$

where $H = I_N \otimes A - KL \otimes C$. Define $\bar{B} = I_N \otimes B$ and function $F(e(t)) = Ef(x(t))$, where the vector function $f(x(t)) = [f^T(x_1(t)), f^T(x_2(t)), \ldots, f^T(x_N(t))]^T$. Moreover, $\eta_k = 1 + d_k$, and then, one has $|\eta_k| > 1$ according to the values of d_k.

Before ending this section, here, we present some assumptions and definitions used in this paper.

Assumption 1. *Suppose that there exists p types of impulses, and both the gains and instants of impulsive sequence are stochastic. The gains η_k take values from a finite set $\mathbb{G} = \{\mu_i\}_{i \in \Gamma}$ satisfying $\mathbb{E}[\mu_i^2] = v_i < +\infty$ and $\vartheta = \max_{i \in \Gamma}\{v_i\}$, and $\Gamma := \{1, 2, \ldots, p\}$. The impulsive sequence $\{t_k\}_{k=1}^{+\infty}$ is governed by a right-continuous homogeneous Markovian chain with p modes, i.e., for $t \in [t_k, t_{k+1})$, $r_k := r(t) = i \in \Gamma$ with the generator $\Lambda = [\lambda_{ij}]_{p \times p}, i, j \in \Gamma$ given by*

$$P(r_{t+h} = j | r_t = i) = \begin{cases} \lambda_{ij}h + o(h), & i \neq j, \\ 1 + \lambda_{ij}h + o(h), & i = j. \end{cases}$$

where $h > 0, \lim_{h \to 0} \frac{o(h)}{h} = 0$ and λ_{ij} denotes the transition rate from i to j, which satisfies that $\lambda_{ij} \geq 0$ for $i \neq j$ and $\lambda_{ii} = -\sum_{j \neq i} \lambda_{ij}$.

According to properties of the Markovian chain, we know that the impulsive interval $\tau(k) = t_k - t_{k-1}$ satisfies the exponential distribution, i.e., $\tau(k) \sim Exp(\lambda_i)$, when $r_k = i$ and $\lambda_i = |\lambda_{ii}|$. Moreover, we obtain the transition probability that $p_{ij} = \frac{\lambda_{ij}}{\lambda_i}$ for $i \neq j$ and $p_{ij} = 0$ for $i = j$.

Based on Assumption 1, we further assume that η_k is a stochastic process on $(\Omega^1, \mathcal{F}^1, \mathcal{F}^1_{k \in \mathbb{N}}, \mathcal{P}^1)$, where $\mathcal{F}^1_{k \in \mathbb{N}} = \sigma(\eta_1, \eta_2, \ldots, \eta_k)$ is the filtration of $\mathcal{F}^1$. On the other hand, the impulsive instants satisfies the Markovian chain, meaning that $r_1, r_2, \ldots, r_k$ are independent random variables on a probability space $(\Omega^2, \mathcal{F}^2, \mathcal{F}^2_{k \in \mathbb{N}}, \mathcal{P}^2)$; similarly, $\mathcal{F}^2_{k \in \mathbb{N}} = \sigma(r_1, r_2, \ldots, r_k)$ is the filtration of $\mathcal{F}^2$. Hence, denote $\Omega := \Omega^1 \times \Omega^2, \mathcal{F} := \mathcal{F}^1 \times \mathcal{F}^2, \mathcal{P} := \mathcal{P}^1 \times \mathcal{P}^2$, and $\mathcal{F}_k := \sigma(\mathcal{F}^1_k \times \mathcal{F}^2_k)$. As a result, the jointly stochastic process $\{(r_k, \eta_k)\}_{k \in \mathbb{N}}$ can be defined on the probability space $(\Omega, \mathcal{F}, \mathcal{F}_k, \mathcal{P})$.

Assumption 2. *The nonlinear function $f : \mathbb{R} \to \mathbb{R}$ is said to be satisfied the Lipschitz condition if there exists a constant $\kappa > 0$ such that*

$$|f(x_1) - f(x_2)| \leq \kappa|x_1 - x_2|. \tag{4}$$

Definition 1. *System (1) is said to be mean square consensus under Markovian impulsive attacks for any given initial value of system states $x(t_0)$ if*

$$\lim_{t \to +\infty} \mathbb{E}\left[|e_i(t)|^2\right] = 0, \quad \forall i = 1, 2, \ldots, N. \tag{5}$$

3. Main Results

Theorem 1. *Under Assumptions 1 and 2, the mean square consensus of system (1) with controller (2) under the Markovian impulsive attacks can be reached if there exist symmetric positive definite matrix P and feedback gain K such that*

$$\sum_{j=1}^{p} \max_{i \in \Gamma}\{p_{ij}\} \frac{\lambda_j v_j}{\lambda_j - \gamma} < 1 \tag{6}$$

where $\gamma = \rho\beta < \min_{j \in \Gamma}\{\lambda_j\}$, $\rho = \frac{\lambda_{\max}(P)}{\lambda_{\min}(P)}$, $\beta = \lambda_{\max}(\Pi)$, and $\Pi = H^T + \kappa\bar{B}^T + PH + \kappa\bar{B}$.

Proof. Consider the following Lyapunov function candidate

$$V(t, e(t)) = e^T(t)Pe(t). \tag{7}$$

For $t \in [t_{k-1}, t_k)$, one can obtain the derivatives of $V(t, e(t))$:

$$\begin{aligned}
D^+ &V(t, e(t)) \\
&= \dot{e}^T(t)Pe(t) + e^T(t)P\dot{e}(t) \\
&\leq e^T(t)\left(H^T P + \kappa\bar{B}^T P + PH + \kappa P\bar{B}\right)e(t) \\
&\leq \gamma V(t, e(t)).
\end{aligned} \tag{8}$$

where $\gamma = \rho\beta$.

For $t = t_k$, caused by the impulsive attacks, we have

$$\begin{aligned}
V(t_k, e(t_k)) &= e^T(t_k)Pe(t_k) \\
&= \eta_k^2 e^T(t_k^-)Pe(t_k^-) \\
&\leq \eta_k^2 e^{\gamma\tau_k} V(t_{k-1}, e(t_{k-1})).
\end{aligned} \tag{9}$$

Since the items $e^{\gamma\tau_k}$ and $V(t_{k-1}, e(t_{k-1}))$ are nonnegative random variables, by taking the expectation and utilizing the properties of the conditional expectations, we obtain

$$\begin{aligned}
\mathbb{E}&[V(t_k, e(t_k))] \\
&\leq \mathbb{E}[\mathbb{E}[\eta_k^2 e^{\gamma\tau_k} V(t_{k-1}, e(t_{k-1}))|\mathcal{F}_{k-1}]] \\
&= \mathbb{E}[\mathbb{E}^2[\mathbb{E}^1[\eta_k^2 e^{\gamma\tau_k} V(t_{k-1}, e(t_{k-1}))|\mathcal{F}_{k-1}^1]|\mathcal{F}_{k-1}^2] \\
&= \mathbb{E}[V(t_{k-1}, e(t_{k-1}))]\mathbb{E}[\mathbb{E}[\eta_k^2 e^{\gamma\tau_k}|r_{k-1}]].
\end{aligned} \tag{10}$$

For $t \in [t_0, t_1)$, it follows from (8) that we have

$$\mathbb{E}[V(t, e(t))] \leq \mathbb{E}[\mathbb{E}[e^{\gamma\tau_1}|r_0]]\mathbb{E}[V(t_0, e(t_0))]$$

from which one can get that, for $t = t_1$,

$$\mathbb{E}[V(t_1, e(t_1))] \leq \mathbb{E}[\mathbb{E}[\eta_1^2 e^{\gamma \tau_1} | r_0]] \mathbb{E}[V(t_0, e(t_0))].$$

For $t \in [t_1, t_2)$, we obtain a similar result from (8) and (10):

$$\mathbb{E}[V(t, e(t))] \leq \mathbb{E}[\mathbb{E}[e^{\gamma \tau_2} | r_1]] \mathbb{E}[V(t_1, e(t_1))]$$

from which one can get that, for $t = t_2$,

$$\mathbb{E}[V(t_2, e(t_2))] \leq \prod_{l=1}^{2} \mathbb{E}[\eta_l^2 e^{\gamma \tau_l} | r_{l-1}] \mathbb{E}[V(t_0, e(t_0))].$$

By mathematical induction, one can finally obtain that, for $t = t_k$,

$$
\begin{aligned}
&\mathbb{E}[V(t_k, e(t_k))] \\
&\leq \mathbb{E}[V(t_0, e(t_0))] \prod_{l=1}^{k} \mathbb{E}[\mathbb{E}[\eta_k^2 e^{\gamma \tau_l} | r_{l-1}]] \\
&= \mathbb{E}[V(t_0, e(t_0))] \mathbb{E}[\prod_{l=1}^{k} \mathbb{E}^2[\mathbb{E}^1[\eta_k^2] e^{\gamma \tau_l} | r_{l-1}].
\end{aligned}
\tag{11}
$$

Let $i_l \in \mathbb{I}, l \in \mathbb{N}$. Since the impulsive sequence $\{\eta_k, r_k, k \in \mathbb{N}^+\}$ with respect to t_k is a Markovian chain and the impulsive interval $\tau(k) \sim Exp(\lambda_i)$, then we have

$$
\begin{aligned}
&\mathbb{E}[\prod_{l=1}^{k} \mathbb{E}^2[\mathbb{E}^1[\eta_l^2] e^{\gamma \tau_l} | r_{l-1}]] \\
&= \sum_{i_1=1}^{p} \sum_{i_2=1}^{p} \cdots \sum_{i_k=1}^{p} \prod_{m=1}^{k} \mathbb{E}^2[\mathbb{E}^1[\eta_{i_m}^2] e^{\gamma \tau_{i_m}} | r_{i_{m-1}}] \\
&\quad \times P(r_{i_1} = i_1, r_{i_2} = i_2, \ldots, r_{i_k} = i_k) \\
&\leq \sum_{i_1=1}^{p} \sum_{i_2=1}^{p} \cdots \sum_{i_k=1}^{p} \prod_{m=1}^{k} \int_{0}^{+\infty} e^{\gamma s} \lambda_{i_m} e^{-\lambda_{i_m} s} ds \\
&\quad \times \prod_{m=1}^{k} \max_{i \in \Gamma} \{p_{i i_m}\} \mathbb{E}^1[\eta_{i_m}^2] \\
&\leq \sum_{i_1=1}^{p} \sum_{i_2=2}^{p} \cdots \sum_{i_k=1}^{p} \prod_{m=1}^{k} \frac{\lambda_{i_m} \mathbb{E}^1[\eta_{i_m}^2]}{\lambda_{i_m} - \gamma} \max_{i \in \Gamma} \{p_{i i_m}\} \\
&= \theta^k.
\end{aligned}
\tag{12}
$$

where $\theta = \sum_{j=1}^{p} \max_{i \in \Gamma} \{p_{ij}\} \frac{\lambda_j v_j}{\lambda_j - \gamma} < 1$.

Substituting (12) into (11), we get that

$$\mathbb{E}[V(t_k, e(t_k))] \leq \theta^k \mathbb{E}[V(t_0, e(t_0))].\tag{13}$$

from which we obtain that, with condition (6)

$$\lim_{k \to +\infty} \mathbb{E}[V(t_k, e(t_k))] = 0.\tag{14}$$

which indicates that $\lim_{k \to +\infty} \mathbb{E}[|e(t_k)|^2] = 0$. Hence, the consensus of system (1) can be achieved, and the proof of Theorem 1 is completed. □

Remark 2. *Note that the parameters γ and λ_j must satisfy $\gamma < \min_{j \in \Gamma}\{\lambda_j\}$. If we choose $\gamma \geq \min_{j \in \Gamma}\{\lambda_j\}$, we can easily know that $\int_0^{+\infty} e^{\gamma s} \lambda_{i_l} e^{-\lambda_{i_l} s} ds = +\infty$, so the condition that $\gamma < \min_{j \in \Gamma}\{\lambda_j\}$ is necessary. Moreover, from (6), we can find a fact that the nonlinear functions has a negative effect on the consensus of system (1), which cannot deal with a high-density impulsive attack. If the system considered is linear, then the condition (6) can be released to adapt more general cases.*

Corollary 1. *Under Assumptions 1 and 2, if $\kappa \equiv 0$, then the consensus of system (1) with controller (2) under Markovian impulsive attacks can be reached if there exist symmetric positive definite matrix P and feedback gain K such that*

$$\sum_{j=1}^{p} \max_{i \in \Gamma}\{p_{ij}\} \frac{\lambda_j v_j}{\lambda_j - \gamma} < 1. \tag{15}$$

where $\gamma = \rho\beta < \min_{j \in \Gamma}\{\lambda_j\}, \rho = \frac{\lambda_{\max}(P)}{\lambda_{\min}(P)}, \beta = \lambda_{\max}(\Pi)$, and $\Pi = H^T + H$.

Remark 3. *The impulsive attacks in this paper are assumed to be stochastic, and since we do not further restrict the distribution of impulsive gains, the explicit relations between the consensus (or system stability) and the impulsive gains are ambiguous, where $\mathbb{E}[\eta_k]$ is replaced by $\mathbb{E}[\eta_k^2]$. For the above reason, it may be hard to obtain $\mathbb{E}[\eta_k^2]$ as we do not know the distribution to which η_k subjected; we need a prior known $\mathbb{E}[\eta_k^2]$ when the clear distribution is unknown. On the other hand, it is common and suitable to assume that the gains from attacks satisfy the Bernoulli distribution such as that in the work of [25], representing the occurrence of attacks. Moreover, the condition (6) shows that a large feedback gain is needed if the strength of impulsive attacks is strong. If the gains are deterministic (i.e., $\eta_k = \eta > 1, k \in \mathbb{N}$), then we can get the following corollary, which is the direct result of model simplification, so the proof is also omitted here.*

Corollary 2. *Under Assumptions 1 and 2, then the consensus of system (1) with controller (2) under Markovian impulsive attacks can be reached if there exist symmetric positive definite matrix P and feedback gain K such that*

$$\sum_{j=1}^{p} \max_{i \in \Gamma}\{p_{ij}\} \frac{\lambda_j \eta^2}{\lambda_j - \gamma} < 1. \tag{16}$$

where $\gamma = \rho\beta < 0, \rho = \frac{\lambda_{\max}(P)}{\lambda_{\min}(P)}, \beta = \lambda_{\max}(\Pi)$, and $\Pi = H^T + H + \kappa \bar{B}^T + \kappa \bar{B}$.

Remark 4. *From the condition (16), one can observe that the dynamics of considered NMASs are stable without impulsive attacks. The reason for this restrictive condition is that the impulsive effects taken into account in this paper are destabilizing, which means that the parameter η always bigger than one. As a result, though the condition $\gamma < \min_{j \in \Gamma}\{\lambda_j\}$ is satisfied, one can find that the inequality (16) never holds when $\gamma \geq 0$. Therefore, the restrictive condition $\gamma < 0$ in (16) is required.*

In the following, we further assume that the Markovian chain obeyed by the impulsive sequence $\{t_k\}_{k=1}^{+\infty}$ is irreducible and that it adopts a stationary distribution $\bar{\varepsilon} = (\bar{\varepsilon}_1, \bar{\varepsilon}_2, \ldots, \bar{\varepsilon}_p)$.

Theorem 2. *Under Assumptions 1 and 2, then the consensus of system (1) with controller (2) under Markovian impulsive attacks can be reached almost surely (a.s.), if there exist symmetric positive definite matrix P and feedback gain K such that*

$$\sum_{i \in \Gamma} \lambda_i \bar{\varepsilon}_i \ln(\mathbb{E}[\eta_i^2]) + \gamma < 0. \tag{17}$$

where $\gamma = \rho\beta; \rho = \frac{\lambda_{\max}(P)}{\lambda_{\min}(P)}; and \beta = \lambda_{\max}(\Pi)$, where $\Pi = H^T + H + \kappa \bar{B}^T + \kappa \bar{B}$, and $\bar{\varepsilon}_i, i \in \Gamma$ is the element of the stationary distribution adotped by the impulsive sequence.

Proof. From (11), we get that for $\forall t \geq t_0$

$$V(t, e(t)) \leq \prod_{l=1}^{k} \eta_l^2 e^{\gamma(t-t_0)} V(t_0, e(t_0))$$

$$= \prod_{k=1}^{\bar{N}(t,t_0)} \eta_k^2 e^{\gamma(t-t_0)} V(t_0, e(t_0)). \tag{18}$$

Note that the impulsive interval $\tau(k) \sim Exp(\lambda_i), i \in \Gamma$; then using the Ergodic theorem [29], the strong law of large number, and the properties of the homogeneous Markovian chain, for $i \in \Gamma$, we can obtain that

$$\lim_{t \to +\infty} \frac{\bar{N}_i(t, t_0)}{t - t_0} = \lim_{t \to +\infty} \frac{\bar{N}_i(t, t_0)}{T_i(t, t_0)} \frac{T_i(t, t_0)}{t - t_0}$$

$$= \lim_{t \to +\infty} \frac{\bar{N}_i(t, t_0)}{\sum_{k=1}^{\bar{N}_i(t,t_0)} \tau_k} \bar{\varepsilon}_i \tag{19}$$

$$= \lambda_i \bar{\varepsilon}_i, \quad a.s.$$

Then, it follows from (17) and (19) that

$$\mathbb{E}[V(t, e(t))]$$

$$\leq \prod_{k=1}^{\bar{N}(t,t_0)} \mathbb{E}[\eta_k^2] e^{\gamma(t-t_0)} \mathbb{E}[V(t_0, e(t_0))]$$

$$= \prod_{i=1}^{p} (\mathbb{E}[\eta_i^2])^{\bar{N}_i(t,t_0)} e^{\gamma(t-t_0)} \mathbb{E}[V(t_0, e(t_0))] \tag{20}$$

$$= e^{(\sum_{i \in \Gamma} \lambda_i \bar{\varepsilon}_i \ln(\mathbb{E}[\eta_i^2]) + \gamma)(t-t_0)} \mathbb{E}[V(t_0, e(t_0))]$$

$$= \bar{\omega}_1 (\mathbb{E}[V(t_0, e(t_0))], t - t_0) \quad a.s.$$

where the function $\bar{\omega}_1(r, s) := e^{(\sum_{i \in \Gamma} \lambda_i \bar{\varepsilon}_i \ln(\mathbb{E}[\eta_i^2]) + \gamma)s} r$. Define $\bar{\omega}_2(r, s) := \frac{\bar{\omega}_1(r,s)}{\epsilon}$ for an arbitrarily small $\epsilon \in (0, 1)$. By employing the Markov's inequality [[30], p. 111, (18.1)] to (20), we have for $t \geq t_0$

$$\mathcal{P}\{V(t, e(t)) \leq \bar{\omega}_2(\mathbb{E}[V(t_0, e(t_0))], t - t_0)\}$$

$$\geq 1 - \frac{\mathbb{E}[V(t, e(t))]}{\bar{\omega}_2(\mathbb{E}[V(t_0, e(t_0))], t - t_0)} \geq 1 - \epsilon. \tag{21}$$

From (20), we know that $\lim_{t \to +\infty} \mathbb{E}[V(t, e(t))] = 0$. Hence, the consensus of system (1) can be achieved almost surely, and the proof of Therorem 2 is completed. □

Remark 5. *Compared with the parameters in Theorem 1, from (17), one can observe that the condition $\gamma < \min_{j \in \Gamma}\{v\}$ is removed by employing the properties of stationary distribution of Markovian chain.*

4. Numerical Examples

In this section, a numerical example with four different cases corresponding to the results established in the previous section is presented, and the last one is given to illustrate the case when gains of attacks $|\eta_k| \leq 1, k \in \mathbb{N}$. Consider the NMASs with four agents, for which the communication topology is described as Figure 2. The dynamics of each agent can be described as follows:

$$\dot{x}_i(t) = Ax_i(t) + Bf(x_i(t)) + Cu_i(t). \tag{22}$$

where the system states $x_i(t) = [x_{i1}^T(t), x_{i2}^T(t)]^T \in \mathbb{R}^2$. $u_i(t)$ is shown in (2), and the non-linear function $f(x_i(t)) = (\tanh(x_{i1}(t)), \tanh(x_{i2}(t)))^T$. The constant matrices A, B, and C are given as follows:

$$A = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix}, B = \begin{bmatrix} 0.4 & -0.02 \\ -1 & 0.6 \end{bmatrix}, C = \begin{bmatrix} 0.2 & 0.1 \\ 0 & 0.2 \end{bmatrix}.$$
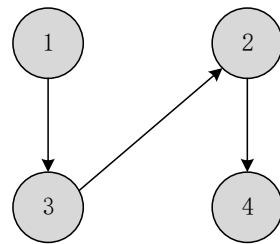
which implies $\kappa = 0.505$ and $\beta = 1.234$ with $K = 0.1$.

Figure 2. The communication topology of the NMASs (22).

Choose $P = I_2$; then $\rho = 1$ and $\gamma = \rho\beta = 1.234$. Suppose a generator of the considered Markovian chain is given as the matrix Λ

$$\Lambda = \begin{bmatrix} -4 & 2 & 1 & 1 \\ 1 & -5 & 2 & 2 \\ 2 & 1 & -4 & 1 \\ 2 & 2 & 1 & -5 \end{bmatrix},$$

from which we know that $\gamma = 1.234 < \min_{j\in\Gamma}\{\lambda_j\} = 4$, from which the transition probability matrix Q can also be derived as

$$Q = \begin{bmatrix} 0 & 0.5 & 0.25 & 0.25 \\ 0.2 & 0 & 0.4 & 0.4 \\ 0.5 & 0.25 & 0 & 0.25 \\ 0.4 & 0.4 & 0.2 & 0 \end{bmatrix},$$

and for which the Markovian chain is described in Figure 3, where we only present a local part of the whole Markovian chain.
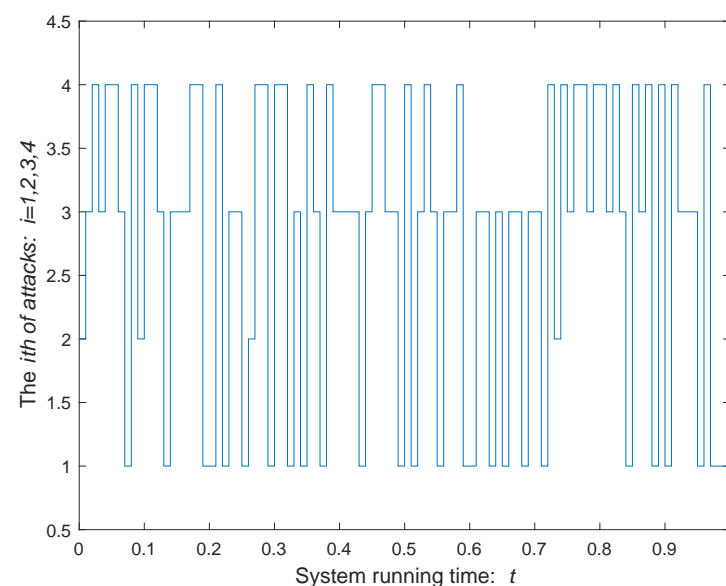

Figure 3. The Markovian chain generated by the probability transition matrix Q.

In addition, set the initial values of system state

$$x(t_0) = \left[x_1^T(t_0), x_2^T(t_0), x_3^T(t_0), x_4^T(t_0) \right]^T$$

$$= \begin{bmatrix} 1.5 & 0.6 & 0.5 & -1.2 & -1.5 & -0.6 & -0.5 & 1.2 \end{bmatrix}^T$$

which can also be randomly generated. Moreover, we can verify that the average values of $x(t_0)$ is $x_{ave} = 0$. Let the error state defined as $|e_i(t)| = \sqrt{x_{i1}^2(t) + x_{i2}^2(t)}$. As shown in Figure 4, the error trajectories of agents do not reach an agreement in the absence of a controller, in other words, system (22) is unstable without control.
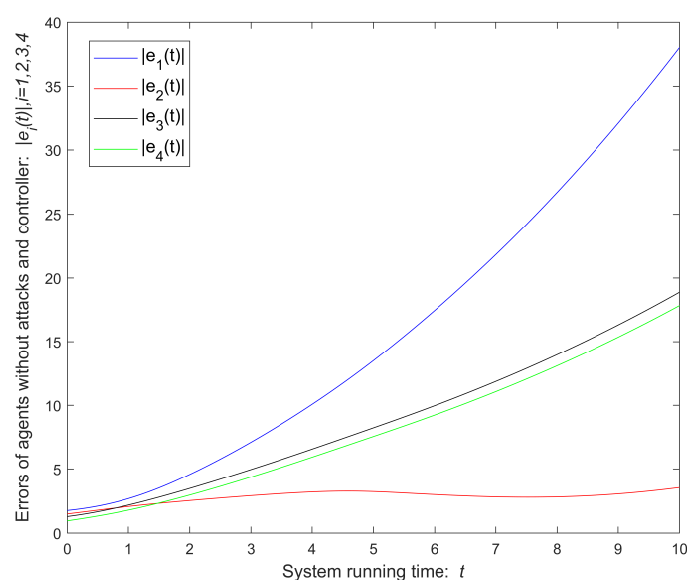
Figure 4. The error trajectories of agents in the absence of controller.

In the following, we consider four cases of stochastic attacks, in which the first three examples are given to illustrate some results proposed in the previous section and the last example is given to illustrate the case in which gains of attacks are below the defined threshold, i.e., $|\eta_k| \leq 1, k \in \mathbb{N}$. Let the time step of all the simulations in this section be $step = 0.01$.

Remark 6. *As we know, the Markovian process can reflect the random jump phenomenon in the real world well and is widely used in many production activities. The cases given here are used to simulate different kinds of malicious human-made network attacks in reality as well as possible attack phenomena in engineering applications such as some transformers that suffer from cyber attacks and result in functional failure in the power grid.*

Case 1: Stochastic gains and instants.

In this case, based on the condition that $|\eta_k| > 1, k \in \mathbb{N}$, we assume that gains of the impulsive deception attacks $\mu_1 = 1.1\xi_1, \mu_2 = -1.2\xi_2, \mu_3 = -1.1\xi_3$, and $\mu_4 = 1.2\xi_4$, where $\xi_i, i = 1, 2, 3, 4$ satisfy the Bernoulli distribution with expectations $\mathbb{E}[\xi_1] = 0.5, \mathbb{E}[\xi_2] = 0.1, \mathbb{E}[\xi_3] = 0.2$, and $\mathbb{E}[\xi_4] = 0.1$, respectively. Then, we can verify that $v_1 = 0.605, v_2 = 0.144, v_3 = 0.242$, and $v_4 = 0.144$. In addition, instants of attacks obey the Markovian chain, for which the generator is presented as above.

Based on the given conditions, one can get that $\sum_{j=1}^{4} \max_{i \in \Gamma} \{p_{ij}\} \frac{\lambda_j v_j}{\lambda_j - \gamma} = 0.682 < 1$. Thus, by employing Theorem 1, the consensus of system (22) can be achieved as Figure 5 shown. Compared with Figure 4, we know that the error states of system (22) can converge to zero from Figure 5 with controller (2), and according to Definition 1, the consensus of system (22) can be achieved.
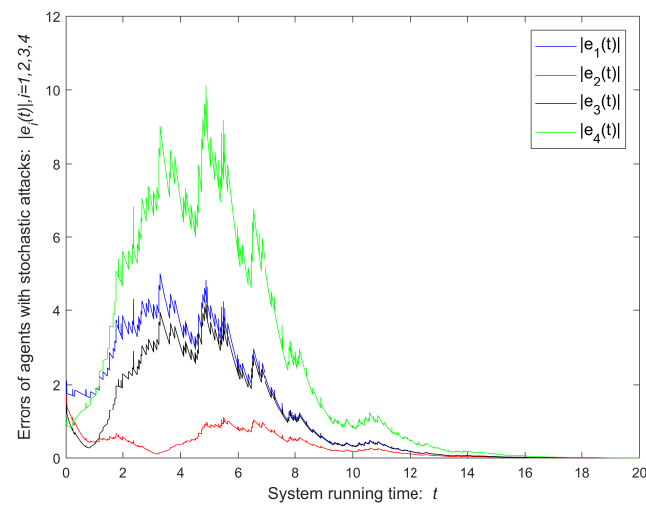
Figure 5. The error trajectories of agents in Case 1 with stochastic gains and Markovian instants.

Case 2: *The Markovian chain is a stationary distribution.*

From the given generator, the stationary distribution $\bar{\varepsilon} = (0.273, 0.227, 0.273, 0.227)$ can be obtained. In addition, we assume that gains of the impulsive deception attacks take values from the following random valuables such that $\mu_1 = -1.5\xi_1, \mu_2 = 2\xi_2, \mu_3 = -1.5\xi_3$, and $\mu_4 = 1.2\xi_4$, where ξ_1 and ξ_2 are the discrete variables obeying the following distribution:

ξ_1	0.7	-0.7	0.8	ξ_2	0.6	-0.6	0.8
Pr	0.5	0.4	0.1	Pr	0.6	0.2	0.2

In contrast, ξ_3 and ξ_4 satisfy the Bernoulli distribution with expectations $\mathbb{E}[\xi_3] = 0.5$ and $\mathbb{E}[\xi_4] = 0.1$, respectively. Thus, we know that $v_1 = 1.136, v_2 = 1.664, v_3 = 1.125$, and $v_4 = 0.144$; therefore the condition in Theorem 2 can be checked such that $\sum_{i \in \Gamma} \lambda_i \bar{\varepsilon}_i \ln(\mathbb{E}[\eta_i^2]) + \gamma = -0.117 < 0$ with $K = 0.1$ and $\beta = 1.234$. As a result, the consensus of system (22) can be achieved by employing Theorem 2, as shown in Figure 6. Similarly, we know that the error states of system (22) can converge to zero from Figure 5 with the controller (2), and and according to Definition 1, the consensus of system (22) can be achieved.
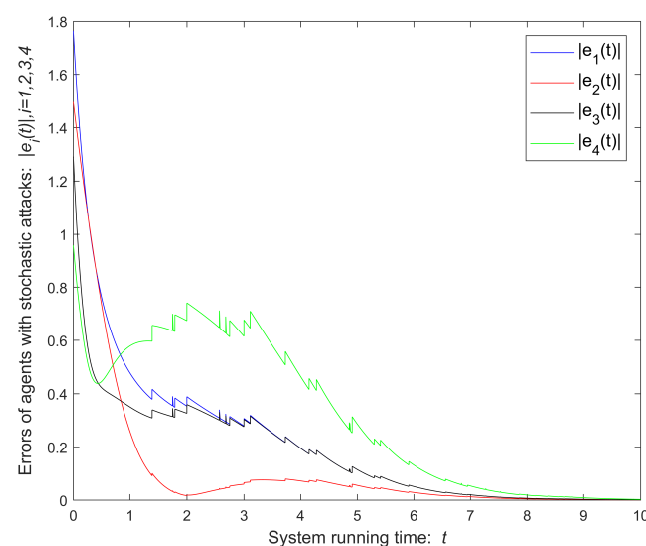

Figure 6. The error trajectories of agents in Case 2 with Markovian instants adopting a stationary distribution.

Case 3:   Determined gains and stochastic instants.

In this case, we further assume that gains of the impulsive deception attacks is a constant $\eta_k \equiv \eta = 1.2$ and that instants are assumed to be the same as that in Case 1. Note that the gains in this case are always bigger than one, and according to Remark 4, we know that system (22) must be stable without impulsive deception attacks. Thinking about the conditions (16), we reselect the system matrices A as

$$A = \begin{bmatrix} -4 & 0 \\ 0 & -4 \end{bmatrix}$$

With the parameters given or calculated above, one can obtain that $\gamma = \rho\beta = -7.479 < 0$ and $\sum_{j=1}^{4} \max_{i\in\Gamma}\{p_{ij}\}\frac{\lambda_j\eta^2}{\lambda_j-\gamma} = 0.978 < 1$. Therefore, the consensus of system (22) can be achieved by employing Corollary 2, and the result is shown as Figure 7. Note that, in this case, the parameter γ needs to be less than zero, the reason can be found in Remark 4. Similarly, from Figure 7 and Definition 1, we can obtain the consensus as error states converge to zero.
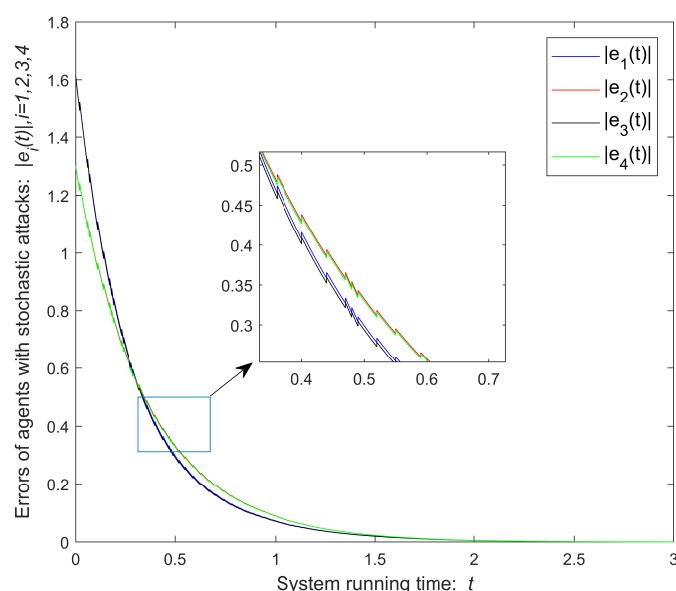

Figure 7. The error trajectories of agents in Case 3 with determined gains and Markovian instants.

Case 4:   Stochastic gains and instants with $d_k \in [-2, 0]$.

In this case, we further assume that $d_k \in [-2, 0], k \in \mathbb{N}$ and that gains of the impulsive deception attacks $\mu_i, i = 1, 2, 3, 4$ take values from $\mu_1 = 0.9\xi_1, \mu_2 = -0.9\xi_2, \mu_3 = 0.8\xi_3$, and $\mu_4 = -0.8\xi_4$, where $\xi_i, i = 1, 2, 3, 4$ satisfy the Bernoulli distribution with expectations $\mathbb{E}[\xi_1] = 0.1, \mathbb{E}[\xi_2] = 0.1, \mathbb{E}[\xi_3] = 0.1$, and $\mathbb{E}[\xi_4] = 0.1$, resceptively.

Then, we can verify that $v_1 = 0.081, v_2 = 0.081, v_3 = 0.064$, and $v_4 = 0.064$. In addition, instants of attacks obey the Markovian chain for which the generator is presented as above. Hence, based on the given conditions, one can get that $\sum_{j=1}^{4} \max_{i\in\Gamma}\{p_{ij}\}\frac{\lambda_j v_j}{\lambda_j-\gamma} = 0.180 < 1$. Thus, by employing Theorem 1, the consensus of system (22) can be achieved as shown in Figure 8.
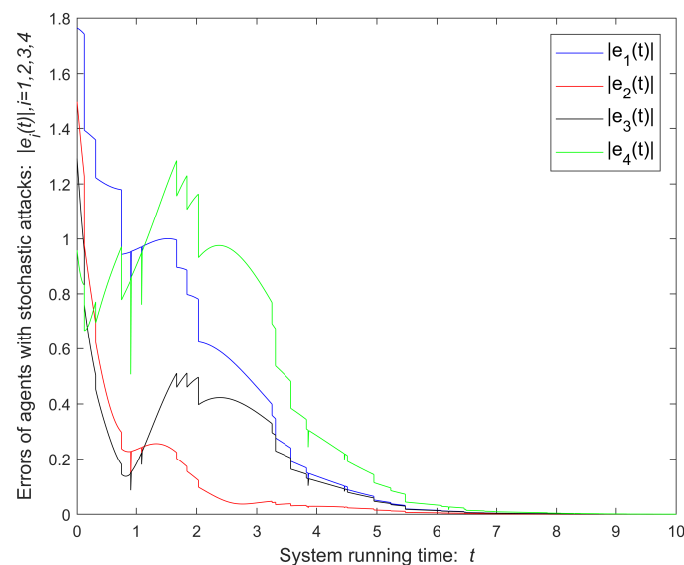
Figure 8. The error trajectories of agents in Case 4 with stochastic gains and Markovian instants.

Remark 7. *From Case 4, we can find that impulsive attacks can stabilize an unstable system when gains belong to* $[-2, 0]$. *In fact, we can find its theoretical support from the error system* (3). *When* $d_k \in [-2, 0]$, *one can get that* $|\eta_k| = |d_k + 1| \leq 1$. *The impulses can stabilize an unstable system, as we know, when the gains of impulses are less than one. Thus, the error system* (3) *can be stabilized with impulsive control.*

Remark 8. *In order to further compare the simulation results with the controller, we give the following simulations with attacks but without control and a system with control but without an attack. For a system* (3) *affected by the attack and no controller added, the error trajectories of the agents are depicted in Figure 9. From Figure 9, we can find that the error states of system* (3) *become bigger and bigger, meaning that consensus cannot be reached under attacks without the controller. In addition, for the system that is not attacked, the error trajectories of agents with control are depicted in Figure 10, from which we know that system* (22) *can achieve consensus under the common controller* $\hat{u}_i(t) = K \sum_{j=1}^{N} a_{ij}(x_j(t) - x_i(t))$ *and without the influence of attacks* $\sum_{k=1}^{+\infty} d_k x_i(t) \delta(t - t_k)$.
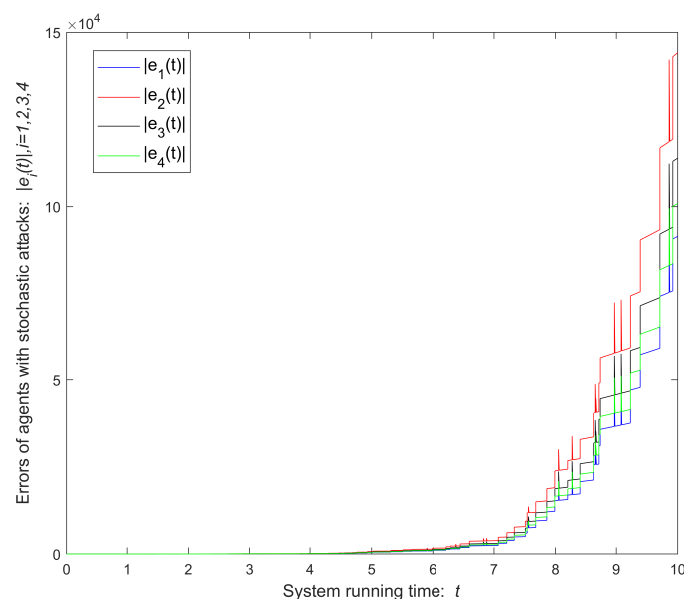

Figure 9. The error trajectories of agents affected by an attack without the controller.
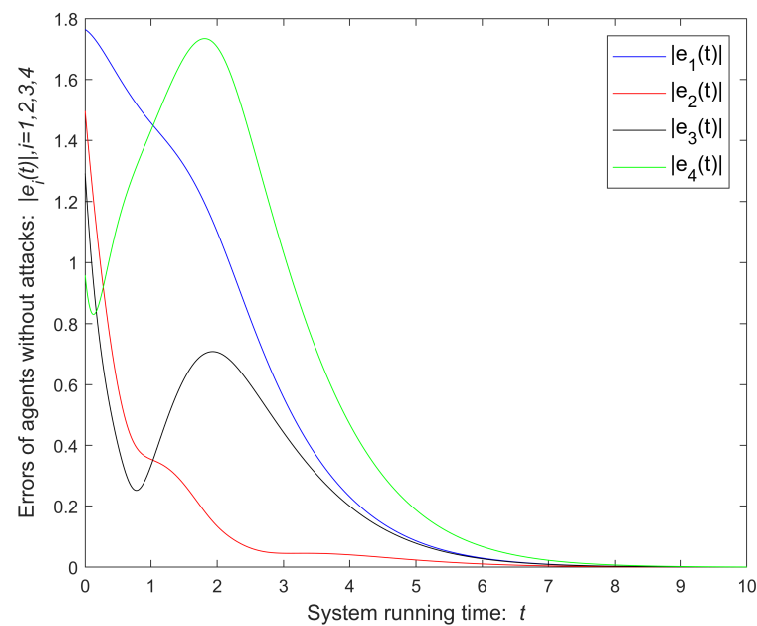
Figure 10. The error trajectories of agents with control but without an attack.

5. Conclusions

In this paper, a more general model for impulsive deception attacks where both gains and instants are stochastic was established, and the consensus problem of the nonlinear multi-agent system under stochastic impulsive attacks was considered. The sufficient conditions were derived with the help of some properties of the stochastic process, and some special cases with more or fewer assumptions were also considered, including the determined, linear, and stationary processes. It can be found that the convergence rate of the NMASs and the transition rates were crucial for stabilization of the considered systems. Moreover, we find that the consensus under impulsive attacks can be maintained if the frequency of attacks is small, i.e., the probability of the random variables cannot be too large. Finally, a numerical example with four cases was provided to verify the effectiveness of the obtained results. Further works will attempt to generalize the Markovian assumption to the semi-Markovian process and will take continuous disturbances into account, as the impulsive intervals with semi-Markov assumption can be used to satisfy any distributions instead of only the exponential distribution while the continuous disturbances are likely to exist in many cases.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

MASs   Multi-agent systems
NMASs   Nonlinear multi-agent systems
DoS   The denial-of-service

References

1. Boccaletti, S.; Latora, V.; Moreno, Y.; Chavez, M.; Hwang, D.U. Complex networks: Structure and dynamics. *Phys. Rep.* **2006**, *424*, 175–308. [CrossRef]
2. Ge, X.; Yang, F.; Han, Q.L. Distributed networked control systems: A brief overview. *Inf. Sci.* **2017**, *380*, 117–131. [CrossRef]
3. Ren, Y.; Wang, A.; Wang, H. Fault diagnosis and tolerant control for discrete stochastic distribution collaborative control systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2014**, *45*, 462–471. [CrossRef]
4. Oh, K.K.; Park, M.C.; Ahn, H.S. A survey of multi-agent formation control. *Automatica* **2015**, *53*, 424–440. [CrossRef]
5. González-Briones, A.; Chamoso, P.; Prieto, J.; Corchado, J.M.; Yoe, H. Reuse of wasted thermal energy in power plants for agricultural crops by means of multi-agent approach. In Proceedings of the 2018 International Conference on Smart Energy Systems and Technologies (SEST), Seville, Spain, 10–12 September 2018; pp. 1–6.
6. Ghadimi, P.; Wang, C.; Lim, M.K.; Heavey, C. Intelligent sustainable supplier selection using multi-agent technology: Theory and application for Industry 4.0 supply chains. *Comput. Ind. Eng.* **2019**, *127*, 588–600. [CrossRef]
7. Xu, Y.; Fang, M.; Wu, Z.G.; Pan, Y.J.; Chadli, M.; Huang, T. Input-based event-triggering consensus of multiagent systems under denial-of-service attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *50*, 1455–1464. [CrossRef]
8. Lu, A.Y.; Yang, G.H. Distributed consensus control for multi-agent systems under denial-of-service. *Inf. Sci.* **2018**, *439*, 95–107. [CrossRef]
9. Xu, W.; Ho, D.W.; Zhong, J.; Chen, B. Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks. *IEEE Trans. Neural Netw. Learn. Syst.* **2019**, *30*, 3137–3149. [CrossRef] [PubMed]
10. Wu, X.; Tang, Y.; Zhang, W. Stability analysis of stochastic delayed systems with an application to multi-agent systems. *IEEE Trans. Autom. Control* **2016**, *61*, 4143–4149. [CrossRef]
11. Yang, W.; Lei, L.; Yang, C. Event-based distributed state estimation under deception attack. *Neurocomputing* **2017**, *270*, 145–151. [CrossRef]
12. Li, X.M.; Zhou, Q.; Li, P.; Li, H.; Lu, R. Event-triggered consensus control for multi-agent systems against false data-injection attacks. *IEEE Trans. Cybern.* **2019**, *50*, 1856–1866. [CrossRef]
13. Liu, H.; Niu, B.; Li, Y. False-Data-Injection Attacks on Remote Distributed Consensus Estimation. *IEEE Trans. Cybern.* **2020**, 1–11. [CrossRef]
14. Ding, D.; Han, Q.L.; Xiang, Y.; Ge, X.; Zhang, X.M. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* **2018**, *275*, 1674–1683. [CrossRef]
15. Guo, Z.; Shi, D.; Johansson, K.H.; Shi, L. Optimal linear cyber-attack on remote state estimation. *IEEE Trans. Control. Netw. Syst.* **2016**, *4*, 4–13. [CrossRef]
16. Hu, L.; Wang, Z.; Han, Q.L.; Liu, X. State estimation under false data injection attacks: Security analysis and system protection. *Automatica* **2018**, *87*, 176–183. [CrossRef]
17. Jin, X.; Haddad, W.M.; Yucelen, T. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. *IEEE Trans. Autom. Control* **2017**, *62*, 6058–6064. [CrossRef]
18. An, L.; Yang, G.H. Improved adaptive resilient control against sensor and actuator attacks. *Inf. Sci.* **2018**, *423*, 145–156. [CrossRef]
19. He, W.; Gao, X.; Zhong, W.; Qian, F. Secure impulsive synchronization control of multi-agent systems under deception attacks. *Inf. Sci.* **2018**, *459*, 354–368. [CrossRef]
20. Zhang, D.; Liu, L.; Feng, G. Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack. *IEEE Trans. Cybern.* **2018**, *49*, 1501–1511. [CrossRef] [PubMed]
21. Ding, D.; Wang, Z.; Ho, D.W.; Wei, G. Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks. *IEEE Trans. Cybern.* **2016**, *47*, 1936–1947. [CrossRef] [PubMed]
22. He, W.; Mo, Z.; Han, Q.L.; Qian, F. Secure impulsive synchronization in Lipschitz-type multi-agent systems subject to deception attacks. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 1326–1334.
23. Liu, J.; Yin, T.; Yue, D.; Karimi, H.R.; Cao, J. Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks. *IEEE Trans. Cybern.* **2020**, *51*, 162–173. [CrossRef] [PubMed]
24. Wen, G.; Zhai, X.; Peng, Z.; Rahmani, A. Fault-tolerant secure consensus tracking of delayed nonlinear multi-agent systems with deception attacks and uncertain parameters via impulsive control. *Commun. Nonlinear Sci. Numer. Simul.* **2020**, *82*, 105043. [CrossRef]
25. He, W.; Qian, F.; Han, Q.L.; Chen, G. Almost sure stability of nonlinear systems under random and impulsive sequential attacks. *IEEE Trans. Autom. Control* **2020**, *65*, 3879–3886. [CrossRef]
26. Sun, H.; Peng, C.; Yang, T.; Zhang, H.; He, W. Resilient control of networked control systems with stochastic denial of service attacks. *Neurocomputing* **2017**, *270*, 170–177. [CrossRef]

27. Xu, Z.; Ni, H.; Reza Karimi, H.; Zhang, D. A Markovian jump system approach to consensus of heterogeneous multiagent systems with partially unknown and uncertain attack strategies. *Int. J. Robust Nonlinear Control* **2020**, *30*, 3039–3053. [CrossRef]

28. Befekadu, G.K.; Gupta, V.; Antsaklis, P.J. Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies. *IEEE Trans. Autom. Control* **2015**, *60*, 3299–3304. [CrossRef]

29. Norris, J.R. *Markov Chains*; Number 2; Cambridge University Press: Cambridge, UK, 1998.

30. Rogers, L.C.G.; Williams, D. *Diffusions, Markov Processes and Martingales: Foundations*; Cambridge University Press: Cambridge, UK, 2000; Volume 1.