2024 Tenth Indian Control Conference (ICC)
9 - 11 December, 2024
IISER Bhopal, India

Quantifying Deviation in Average Consensus Equilibrium in a Multi-Agent System Subject to Periodic Denial-of-Service Attacks

Rajendra Prasad and Anoop Jain

***Abstract*— This paper investigates the problem of state consensus in multi-agent systems (MASs) under periodic denial-of-service (DoS) attacks affecting the inter-agent communication network. We introduce the so-called deviation matrix to quantify the impact of such DoS attacks on the consensus point of MAS with that of the average consensus point under no attack. It is demonstrated that the agents achieve asymptotic consensus at a perturbed location under DoS attacks of a finite period where the deviation between the average consensus and the perturbed consensus points is established analytically and found to be dependent on the DoS attack frequency and duration. Additionally, with an infinite attack period and communication link between any set of agents compromised, the MAS behaves as a decoupled set of agents, each achieving equilibrium at the origin. Illustrative examples and simulation results are provided to validate the theoretical developments in the paper.**

***Index Terms*— Multi-agent systems, deviation matrix, denial-of-service (DoS) attacks, consensus.**

I. Introduction

MASs involve multiple agents (or subsystems) working in cooperation to achieve shared goals, such as reaching an agreement on a state or executing coordinated tasks [1]–[3]. A fundamental aspect of MASs is the ability of the agents to communicate and share information, which is critical for the system's overall performance and stability. With the scalability and the wireless medium used for inter-agent communication, the MASs pose several challenges in their operation, including the issues of cyber security [4], [5], which is one of the critical issues in the present technical infrastructure.

Typically, cyber-attacks can be categorized in two ways. The first one is where an attacker directly influences an agent's dynamics/model; for instance, [6] and [7] show that an attack on a specific agent is equivalent to the removal of that agent from the network graph. The other type of attack targets the communication links between the agents, preventing information exchange among them [8]. Since the attacks directly influencing the system's dynamics are easily identifiable, the attacks affecting the communication links are more stealthy and require special attention in the secure operation of MASs. Such attacks can be further classified as [9]: (a) deception attacks, and (b) DoS attacks. The former refers to the data trustworthiness where the adversary manipulates data transmitted over communication networks to violate integrity [10]. At the same time, the latter is launched by external jammers, attempts to compromise the availability of transmitted data at their destinations [11].

The authors are with the Department of Electrical Engineering, Indian Institute of Technology Jodhpur, 342030, India (e-mail: m23eec011@iitj.ac.in; anoopj@iitj.ac.in).

For MASs subject to DoS attacks, several consensus control schemes have been proposed in the literature. Zhang *et al.* [12] investigated the sampled-data consensus for linear MASs. In [13], nonlinear MASs were considered, with the communication channels for observers and controllers under different attacks. Cetinkaya *et al.* [14], De Persis and Tesi [15], and Chen *et al.* [16] studied secure control against DoS attacks in a centralized setting. Consensus tracking protocols for linear stochastic MASs under two kinds of attacks were presented in [17]. In [18], event-triggered control schemes were proposed for MASs under DoS attacks. To the best of the authors' knowledge, no existing results on the consensus of MASs under DoS attacks have quantified the deviation in the consensus point from the average consensus point under periodic DoS jamming attacks.

This paper contributes in this direction and relates this deviation analytically with the given periodic DoS attack signal, affecting the communication network among agents. By quantifying the impact of these attacks on the consensus properties, our study provides valuable insights for developing resilient systems capable of maintaining performance and stability despite adverse conditions. The main contributions are summarized as follows:

(a) The concept of deviation matrix is introduced to characterize the deviation in the perturbed and average consensus points over one attack period. We further established that the eigenvalues of this matrix lie in the range $(-1, 1)$.
(b) An analytical expression is obtained relating to the deviation in the consensus point under the attack condition with that of the average consensus point in the no attack condition.
(c) We have shown that if the communication link between any set of agents is compromised and the DoS attack signal spans for a sufficiently long time, then the MAS will behave as a decoupled set of agents, each achieving equilibrium at the origin, unlike the situation where attack spans for a finite period.

The remaining paper is organized as follows. The system and attack models, along with the problem formulation are given in Section II. Section III presents the main results where we establish analytical relations pertaining to deviation in consensus points. An example with extensive simulation results is discussed in Section IV. Finally, Section V concludes the paper with some future remarks.

Preliminaries: We denote the set of real numbers by $\mathbb{R}$, the set of natural numbers by $\mathbb{N}$, the set of non-negative integers by $\mathbb{W}$, and the set of complex numbers by $\mathbb{C}$. Further, we model a MAS using a connected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, \ldots, N\}$ represents the set of agents (nodes) and

979-8-3315-1721-2/24/$31.00 ©2024 IEEE

$\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denotes the set of communication links (edges) between the agents. The neighboring set of any node i is denoted by the set $\mathcal{N}_i$. In the absence of any DoS attack, we assume that the communication topology $\mathcal{G}$ is connected and contains a spanning tree [19]. Let $A = [a_{ij}] \in \mathbb{R}^{N\times N}$ be the adjacency matrix of $\mathcal{G}$ where $a_{ij} = 1$ if there is an edge between nodes i and j, else $a_{ij} = 0$. The degree matrix $D \in \mathbb{R}^{N\times N}$ is a diagonal matrix where the i-th diagonal element d_i represents the degree of node i, defined as $d_i = \sum_{j=1}^{N} a_{ij}$. By $\beta = \max_i(d_i)$, we denote the maximum degree of the graph $\mathcal{G}$. The Laplacian matrix $L \in \mathbb{R}^{N\times N}$ is defined as $L = D - A$. We further define a consensus matrix P (referred to as Perron matrix in [2]) as $P = I - \alpha L$, where I is the $N \times N$ identity matrix and $\alpha > 0$ is a constant. Also, we do not consider any self-loop for the agents in the MAS.

II. System Model and Problem Description

A. Model of MAS

We consider N agents modeled using discrete-time single integrator dynamics:

$$x_i[k+1] = x_i[k] + u_i[k], \tag{1}$$

where $i = 1, \ldots, N$ and $k \in \mathbb{W}$. Here each agent i at time step k is characterized by the state $x_i[k] \in \mathbb{R}$ with $u_i[k] \in \mathbb{R}$ being the control variable. To achieve the state consensus, the control $u_i[k]$ is proposed as follows [2]:

$$u_i[k] = \alpha \sum_{j\in\mathcal{N}_i} a_{ij}(x_j[k] - x_i[k]),\ k \in \mathbb{W}, \tag{2}$$

for all $i = 1, \ldots, N$, and is referred to as distributed in the sense that it solely depends on the information of the agent i and its neighbors $j \in \mathcal{N}_i$. Here, $\alpha \in (0, 1/\beta]$ with β being the maximum degree of the network [2]. Using (2), the update rule for the i-th agent in (1) is described as follows:

$$x_i[k+1] = x_i[k] + \alpha \sum_{j\in\mathcal{N}_i} a_{ij}(x_j[k] - x_i[k]). \tag{3}$$

The system (3) can be expressed in the vector-matrix form as:

$$x[k+1] = Px[k], \tag{4}$$

where $x[k] \in \mathbb{R}^N$ is the state vector of all agents and P is the consensus matrix of size $N \times N$. The solution of (4) is obtained using the chain rule as follows:

$$x[k] = P^k x[0], \tag{5}$$

where $x[0] \in \mathbb{R}^N$ is the initial state vector of the agents and P^k represents the k-th power of the consensus matrix P.

B. DoS Jamming Attacks

We consider a type of power-constraint, discrete-time periodic jammer signal as shown in Fig. 1, and blocking the digital communication channel as follows [20]:

$$\mathcal{I}_{\text{DoS}}[k] = \begin{cases} 0, & k \in \{(s-1)T, \ldots, (s-1)T + m - 1\} \\ 1, & k \in \{(s-1)T + m, \ldots, sT - 1\}, \end{cases} \tag{6}$$

where $k \in \mathbb{W}$ denotes the discrete time step, $\mathcal{I}_{\text{DoS}}[k]$ represents the indicator function of the jamming signal at

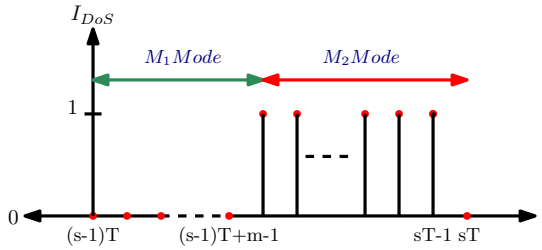


Fig. 1: DoS Jamming signal.

time step k, $s \in \mathbb{N}$ represents the period number, $T \in \mathbb{N}$ is the action period of the jammer, and $m \in \mathbb{W}$ $(m \leq T)$ indicates the number of time steps during which the jammer is inactive within the action period T. To facilitate the further analysis, we introduce the following concerning Fig. 1:

- Let $M_1 \triangleq \{(s-1)T, (s-1)T+1, \ldots, (s-1)T+m-1\}$ be the interval when the jamming signal is inactive, i.e., the communication edge is intact. We refer to this period as the inactive state or M_1 mode of the DoS jamming attacks.
- Let $M_2 \triangleq \{(s-1)T+m, (s-1)T+m+1, \ldots, sT-1\}$ be the interval when the jamming signal is active, i.e., there is no communication over the attacked edge. We refer to this period as the active state or M_2 mode of the DoS jamming attacks.

Further, we define a communication availability indicator function $\delta[k]$ as:

$$\delta[k] = 1 - \mathcal{I}_{\text{DoS}}[k], \tag{7}$$

which indicates the availability of communication in compromised links of MAS at the time step k. We express $\delta[k]$ as follows:

$$\delta[k] = \begin{cases} 1, & k \in M_1 \\ 0, & k \in M_2 \end{cases}. \tag{8}$$

Remark 1. *Note that when $\delta[k]$ is zero, the communication link between the agents is compromised, that is, during this interval the agents do not receive state information from their neighbors. The absence of communication link refers to as receiving no new input, modeled as receiving a zero update.*

We consider the following assumption on the DoS signal:

Assumption 1. *The DoS jamming attack* (6) *is a finite-time periodic attack signal that spans over n periods, and after that, there is no attack, implying $s \leq n$.*

C. Problem Formulation

Let $\mathcal{K}_i \subseteq \mathcal{N}_i$ be the set of neighbors of agent i with compromised communication links, and $\mathcal{L}_i \subseteq \mathcal{N}_i$ be the set of neighbors of agent i with secure communication links. Using (7), the consensus protocol $\tilde{u}_i[k]$ in (2) can be expressed for the i-th agent in the presence of a DoS attack (6) as follows:

$$\tilde{u}_i[k] = \alpha[\sum_{j\in\mathcal{K}_i} a_{ij}(\delta[k]x_j[k] - x_i[k]) + \sum_{j\in\mathcal{L}_i} a_{ij}(x_j[k] - x_i[k])]. \tag{9}$$

In the absence of any attack, $\tilde{u}_i[k]$ will take the form of $u_i[k]$ as given in equation (2) as here $\mathcal{K}_i = \{\emptyset\}$. Hence, in

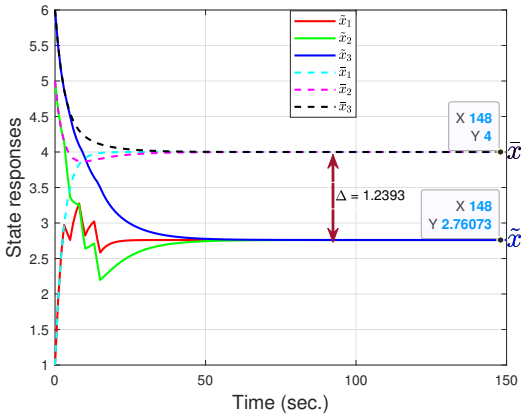


Fig. 2: Consensus with and without DoS attack and the deviation Δ.

this case the system (3) achieves average consensus in the sense that $\lim_{k\to\infty} \|x_j[k] - x_i[k]\| = 0, i, \ j = 1, \ldots, N$, and converges at the average value $\bar{x} = \lim_{k\to\infty} x_i[k] = \frac{1}{N}\sum_{i=1}^{N} x_i[0]$, where $x_i[0]$ denote the initial states [2].

In the presence of a DoS attack on the network when the DoS attack is in its active state, communication between certain sets of agents is denied, i.e. $\delta[k] = 0$ in equation (9). Hence, during this interval, $\tilde{u}_i[k]$ will take the form

$$\tilde{u}_i[k] = \alpha[\sum_{j\in\mathcal{K}_i} a_{ij}(0 - x_i[k]) + \sum_{j\in\mathcal{L}_i} a_{ij}(x_j[k] - x_i[k])], \quad (10)$$

that may cause issues such as deviation in the consensus point from the average value $\bar{x} \in \mathbb{R}$. We show that during this interval, the MAS behaves as a decoupled set of agents and eventually (after several such DoS attack periods) converges at an arbitrary point. When the DoS attack signal spans for a sufficiently large value of n and if $\mathcal{K}_i \neq \emptyset$ for any agent i, then the MAS following the consensus protocol $\tilde{u}_i[k]$ will behave as a decoupled system and converges at the origin (a detailed analysis is provided in part (ii) of the below Theorem 1), and in other situations, they achieve consensus at a perturbed value. Let the agents reach consensus at the point $\tilde{x}$ in the presence of DoS attacks (6). We define the deviation Δ as:

$$\Delta = |\tilde{x} - \bar{x}|, \quad (11)$$

the difference (in the absolute sense) between the consensus point under the presence and the absence of a DoS attack. One such scenario is depicted in Fig. 2 where the initial states of the agents are $x_1[0] = 1$, $x_2[0] = 5$, $x_3[0] = 6$ and the DoS attack spans three periods with sleeping state interval $m = 3$ and jammer action period $T = 5$. Hence, the DoS attack duration (d) is 2 and the DoS frequency (n) is 3 units. Please note that the DoS duration refers to the interval within the attack period T when the attack signal (6) is in M_2 mode, i.e., $d = T - m$ is the interval during which communication between the affected agents is denied. While the DoS frequency n refers to the number of periods the attack signal occurs, indicating how often the MAS has been under DoS attack. Our main objective in this paper is to investigate the impact of DoS attacks of different attack duration and frequency on the deviation Δ, analytically.

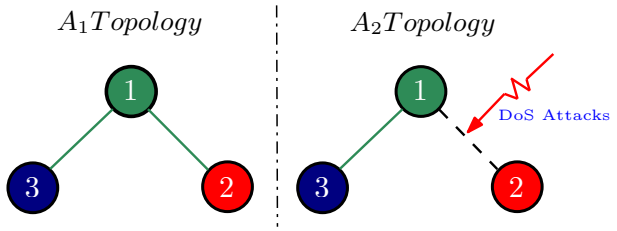


Fig. 3: Change in topology due to DoS attack.

III. Main Results

In this section, we first obtain the point where the agents achieve consensus in the presence of periodic DoS attacks, followed by an analysis of the deviation Δ by introducing the concept of a deviation matrix. Due to periodic DoS attacks, the affected communication links are either active or inactive, implying that the communication topology varies accordingly. For instance, Fig. 3 shows a case of three agents where the edge connecting agents 1 and 2 is under DoS attack. Clearly, the network is connected under no attack, and the communication link between agent 1 and agent 2 is compromised in case of a DoS attack, as depicted by topology A_1 (under M_1 mode) and A_2 (under M_2 mode), respectively. Since the transition in topologies are of measure zero, the overall stability of the system remains intact. Let L_1 be the Laplacian matrix capturing the agents' communication pertaining to topology A_1. Let L_2 be a matrix obtained from L_1 by substituting $a_{ij} = 0 \ \forall \ j \in \mathcal{K}_i$, which essentially captures the communication topology pertaining to A_2. Note that L_2 does not share the properties of a Laplacian matrix. Further, let P_1 and P_2 be the consensus matrices corresponding to L_1 and L_2, respectively, defined as $P_1 = I - \alpha L_1$ and $P_2 = I - \alpha L_2$, where α is a positive constant. Based on these, we define the deviation matrix as follows:

Definition 1. *Define the deviation matrix $Z = [z_{ij}] \in \mathbb{R}^{N\times N}$ as:*

$$Z \triangleq P_2^{T-m} P_1^m, \quad (12)$$

where $m < T$ and m denote the number of time steps during which the jammer is inactive within the action period T.

Before proceeding further, we state some preliminary results as follows:

Lemma 1. *For any symmetric matrices $\mathcal{A} \in \mathbb{R}^{N\times N}$ and $\mathcal{B} \in \mathbb{R}^{N\times N}$, if their eigenvalues lies between $[-1, 1]$ and $(-1, 1)$ respectively, then the eigenvalues of their product ($\mathcal{AB}$ or $\mathcal{BA}$) lie in the range $(-1, 1)$.*

Proof. Please refer to Appendix. □

Lemma 2. *Given matrices L_1, L_2, and Z, the eigenvalues of L_1 are non-negative, the eigenvalues of L_2 are positive, and the eigenvalues of Z lie in the interval $(-1, 1)$ for $\alpha \in [0, 2/\gamma]$, where $\gamma = \max(\lambda_i, \mu_i)$, with λ_i and μ_i representing the eigenvalues of matrices L_1 and L_2, respectively.*

Proof. For the Laplacian $L = [\ell_{ij}] \in \mathbb{R}^{N\times N}$ of graph $\mathcal{G}$, the non-diagonal elements are $(\ell_{ij})_{i\neq j} = -a_{ij}$ and the diagonal elements are $(\ell_{ij})_{i=j} = d_i$. From Gershgorin's theorem, it is straightforward to observe that all the disks $|z - d_i| =$

$\sum_{j\neq i}|a_{ij}|$ (where $z \in \mathbb{C}$) corresponding to each row of the Laplacian L_1 lie in the right half of the complex plane and contain the origin. Therefore, the eigenvalues λ_i of L_1 satisfy $\lambda_i \geq 0$ (see [21]).

On the other hand, for matrix L_2, we consider the following two cases: (a) If any row satisfies the zero-sum row property, according to Gershgorin's theorem, the eigenvalues μ_i of L_2 satisfy $\mu_i \geq 0$. However, it is evident from the structure of L_2 that for $\mu_i = 0$, there exists no eigenvector v such that $L_2 v = \mu_i v$, due to rows of L_2 that do not satisfy the zero-sum row property under DoS attacks. Therefore, $\mu_i > 0$. (b) Suppose no row in L_2 satisfies the zero-sum row property (when there is a DoS attack on at least $N-1$ edges). Using Gershgorin's theorem, it can be concluded that all disks corresponding to the rows of L_2 lie in the right half of the complex plane and do not contain the origin. Hence, $\mu_i > 0$. Combining both cases, we can conclude that $\mu_i > 0$ for all $i \in N$.

Further, for achieving consensus, the eigenvalues of consensus matrices P_1 and P_2 must not lie outside the unit circle in the complex plane. Since P_1 has real eigenvalues $1-\alpha\lambda_i$, it must hold that $|1-\alpha\lambda_i| \leq 1$, implying that $0 \leq \alpha\lambda_i \leq 2$. Similarly, for P_2, it must be satisfied that $0 \leq \alpha\mu_i \leq 2$. Note that both P_1 and P_2 share the same α, the maximum allowable value of α is given by $\alpha \in [0, 2/\gamma]$, where $\gamma = \max(\lambda_i, \mu_i)$. Moreover, since $\lambda_i \geq 0$ and $\mu_i > 0$, the eigenvalues of P_1 and P_2 lie in the intervals $[-1, 1]$ and $(-1, 1)$, respectively. Consequently, the eigenvalues of P_1^m are $(1-\alpha\lambda_i)^m$ that lie in $[-1, 1]$, while the eigenvalues of P_2^{T-m} are $(1-\alpha\mu_i)^{T-m}$ that lie in $(-1, 1)$ (this follows from diagonalization). Now, exploiting Lemma 1, it can be concluded that the eigenvalues of Z lie in $(-1, 1)$ for $\alpha \in [0, 2/\gamma]$, where $\gamma = \max(\lambda_i, \mu_i)$. □

Lemma 3. *In case when the DoS attack spans infinitely with $m < T$, we have $\lim_{n\to\infty} Z^n = O_{N\times N}$, where $O_{N\times N}$ denotes the null matrix and n is the number of attack periods.*

Proof. Diagonalizing Z, we get $Z = QDQ^{-1}$, where D is the diagonal matrix with the eigenvalues of Z as its diagonal elements, and Q is a matrix whose columns are the eigenvectors of deviation matrix Z. Therefore, $Z^n = QD^nQ^{-1}$. From Lemma 2, since the eigenvalues of Z lie in $(-1, 1)$, therefore as n tends to infinity, D^n tends to a null matrix. Hence as $n \to \infty$, $Z^n = QD^nQ^{-1} = QO_{N\times N}Q^{-1} = O_{N\times N}$. □

We are now ready to state the main result:

Theorem 1. *Consider a multi-agent system consisting of N agents under the following distributed consensus algorithm:*

$$x_i[k+1] = x_i[k] + \tilde{u}_i[k], \tag{13}$$

which is subject to a periodic DoS attack spanning n periods with $m < T$. Suppose $\mathcal{G}$ is a connected graph and Z is the deviation matrix. Then,

(i) *When n is finite, a consensus is asymptotically reached at $\tilde{x} = \frac{1}{N}\sum_{i=1}^{N} Z_i^n x[0]$ for the given initial state vector $x[0] \in \mathbb{R}^N$, where Z_i denotes the i-th row of Z. When n is infinite, the MAS will behave as a decoupled set of agents and stabilize at the origin.*

(ii) *The deviation Δ in (11) is given by*

$$\Delta = \frac{1}{N}\left|\sum_{i=1}^{N}[Z^n - I]_i x[0]\right|, \tag{14}$$

where $[Z^n - I]_i$ denotes the i-th row of the matrix $Z^n - I$.

Proof. Consider a scenario where the attack spans for n periods. During these, the MAS operates under two distinct topologies A_1 and A_2. When the DoS signal is in the M_1 mode, the MAS operates according to the A_1 topology. Hence, if $\mathbf{x}[0]$ is the initial state vector of the agents, then using equation (5) we can write $\mathbf{x}[m] = P_1^m x[0]$. As the DoS signal transitions to the M_2 mode within this period, the MAS operates according to the A_2 topology. Taking $\mathbf{x}[m]$ as the initial state vector for the M_2 mode in the first period and using equation (5) we get $\mathbf{x}[T] = P_2^{T-m}\mathbf{x}[m] = P_2^{T-m}P_1^m\mathbf{x}[0]$. For the second attack period, the DoS signal transitions back to the M_1 mode, and MAS operates according to the A_1 topology. Taking $\mathbf{x}[T]$ as the initial state vector for the second DoS period, using equation (5) we get $\mathbf{x}[T+m] = P_1^m\mathbf{x}[T] = P_1^m P_2^{T-m} P_1^m\mathbf{x}[0]$. As the DoS signal transitions to the M_2 mode in the second DoS period, the MAS operates according to the A_2 topology. Taking $x[T+m]$ as the initial state vector for the M_2 mode in second period, then using equation (5) we get $x[2T] = P_2^{T-m}x[T+m] = P_2^{T-m}P_1^m P_2^{T-m}P_1^m x[0] = [P_2^{T-m}P_1^m]^2 x[0]$. Similarly, for the DoS attack spanning n periods, we can write $x[nT] = [P_2^{T-m}P_1^m]^n x[0]$. Since the DoS attack under consideration spans for n periods (Assumption 1), after these n attack periods, the MAS operates solely under the A_1 topology. Taking $x[nT]$ as the initial state vector, the system will achieve the average consensus at $\tilde{x} = (1/N)\sum_{i=1}^{N} x_i[nT] = (1/N)\sum_{i=1}^{N}[P_2^{T-m}P_1^m]_i^n x[0] = (1/N)\sum_{i=1}^{N} Z_i^n x[0]$ where Z_i denotes the i-th row of matrix Z. In case when $n \to \infty$, we have $\lim_{n\to\infty} Z^n = O_{N\times N}$ from Lemma 3. Using this, it follows that $\lim_{n\to\infty}\tilde{x} = \lim_{n\to\infty}\frac{1}{N}\sum_{i=1}^{N} Z_i^n x[0] = 0$. This implies that if the DoS attack spans for an infinite period, all the agents in the MAS will behave as decoupled agents and converge at the origin.

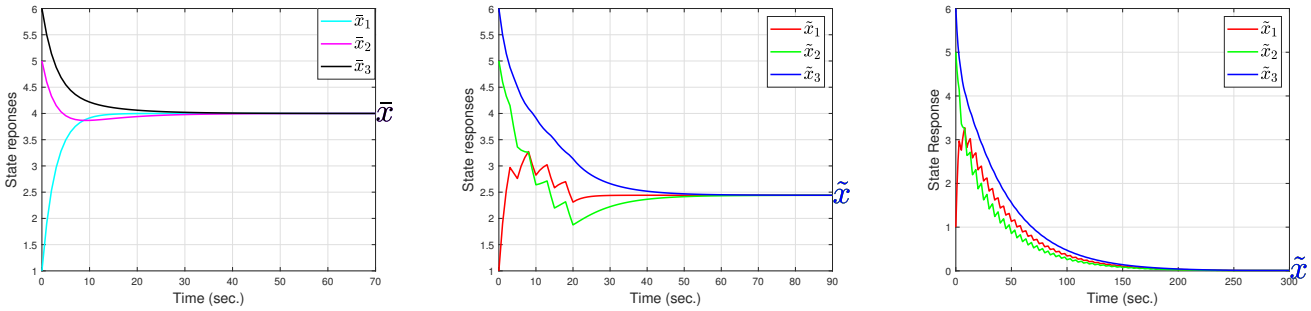
Following the above analysis and using (11), the deviation Δ is given by $\Delta = (1/N)|\sum_{i=1}^{N} Z_i^n x[0] - \sum_{i=1}^{N} x_i[0]| = (1/N)|\sum_{i=1}^{N}[Z^n - I]_i x[0]|$. Hence, proved. □

IV. An Example and Simulation Results

We illustrate the above theoretical developments through the below example, followed by simulation results.

A. An Example

Consider three agents ($N = 3$) as shown in Fig. 3 where the communication link between agent 1 and agent 2 is under a DoS attack. Let the initial state values of the agents be $x_1[0] = 1$, $x_2[0] = 5$, $x_3[0] = 6$. Clearly, the average consensus point in the absence of attack is $\bar{x} = (1/3)(1+5+6) = 4$. Let the attack (6) is characterized by $T = 5$, $m = 3$, and $n = 3$. Under control (9), agents are described as $x_1[k+1] = x_1[k] + \alpha[(\delta[k]x_2[k] - x_1[k]) + (x_3[k] - x_1[k])]$, $x_2[k+1] = x_2[k] + \alpha[\delta[k]x_1[k] - x_2[k]]$, $x_3[k+1] = x_3[k] + \alpha[x_1[k] -$



(a) No DoS Attack ($n = 0$) (b) Finite n (c) Sufficiently large n

Fig. 4: Agents' state response with DoS attack.

$x_3[k]]$. For the topologies A_1 and A_2 in Fig. 3, we can write the matrices corresponding to $\delta = \{0, 1\}$ as $L_1 = \begin{bmatrix} 2 & -1 & -1 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$ and $L_2 = \begin{bmatrix} 2 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$. The eigenvalues of L_1 are $\lambda_i = 0, 1, 3$ and L_2 are $\mu_i = 0.3820, 1, 2.6180$ for $i = 1, 2, 3$. According to Lemma 2, consider that $\alpha = 0.1$ since $0 \leq \alpha \leq 2/\gamma$ where $\gamma = \max(\lambda_i, \mu_i) = 3$, i.e., $0 \leq \alpha \leq 0.66$. The matrices P_1 and P_2 are given by $P_1 = I - 0.1 \begin{bmatrix} 2 & -1 & -1 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0.8 & 0.1 & 0.1 \\ 0.1 & 0.9 & 0 \\ 0.1 & 0 & 0.9 \end{bmatrix}$ and $P_2 = I - 0.1 \begin{bmatrix} 2 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0.8 & 0 & 0.1 \\ 0 & 0.9 & 0 \\ 0.1 & 0 & 0.9 \end{bmatrix}$. The deviation matrix in (12) is given by $Z = P_2^2 P_1^3$ where $P_1^3 = \begin{bmatrix} 0.562 & 0.219 & 0.219 \\ 0.219 & 0.755 & 0.026 \\ 0.219 & 0.026 & 0.755 \end{bmatrix}$ and $P_2^2 = \begin{bmatrix} 0.65 & 0 & 0.17 \\ 0 & 0.81 & 0 \\ 0.17 & 0 & 0.82 \end{bmatrix}$, and hence, $Z = \begin{bmatrix} 0.4025 & 0.1468 & 0.2707 \\ 0.1774 & 0.6116 & 0.0211 \\ 0.2751 & 0.0586 & 0.6563 \end{bmatrix}$. Since $n = 3$, $\tilde{x} = (1/3) \sum_{i=1}^{3} Z_i^3 x[0]$ where Z^3 is obtained as $Z^3 = \begin{bmatrix} 0.2146 & 0.1562 & 0.2647 \\ 0.1665 & 0.2770 & 0.1078 \\ 0.2811 & 0.1440 & 0.4165 \end{bmatrix}$. It can be obtained that $Z_1^3 x[0] = 2.5838$, $Z_2^3 x[0] = 2.1981$ and $Z_3^3 x[0] = 3.5003$, implying that $\tilde{x} = \frac{1}{3}(2.5838 + 2.1981 + 3.5003) = 2.7607$. Therefore, $\Delta = |2.7607 - 4| = 1.2393$.

B. Simulation Result

To gain better clarity on how the average consensus point of the MAS in the previous example varies with changes in the nature of DoS jamming attacks, we present a simulation study in this subsection. As shown in 4(a), the agents achieve average consensus in the absence of any DoS attack. For a DoS attack of some certain frequency, agents deviate from their expected path and achieve consensus at a perturbed location, as shown in Fig. 4(b). When the DoS attack frequency becomes sufficiently large, the MAS behaves as a decoupled set of agents, each reaching equilibrium at the origin, as shown in Fig 4(c).

Fig. 5 illustrates how the average consensus point of the MAS varies with increasing DoS attack frequency. Here, we consider the DoS attack jamming action period $T = 5$ and $m = 3$. In Fig. 5(a), we observe that the average consensus point of the MAS deviates from the expected average location and moves toward the origin as the frequency of the DoS attack signal increases. Fig. 5(b) shows that as the DoS attack frequency becomes sufficiently large, all the agents stabilize at the origin. Furthermore, from Fig. 5(c), we infer that for a given DoS attack frequency, increasing the DoS attack duration from $d = 0$ to $d = 5$ results in a greater deviation in the average consensus from the expected location.

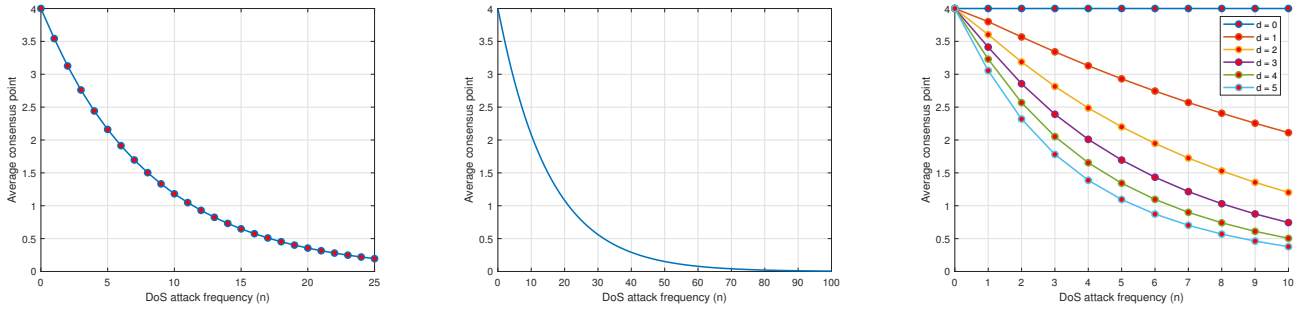
Fig. 6 depicts how the average consensus point of the MAS changes with increasing DoS attack duration (d). Here, we consider the DoS attack jamming action period $T = 5$. In Fig. 6(a), for a single DoS attack period ($n = 1$), increasing the DoS attack duration leads to a deviation of the average consensus point from the expected location towards the origin. Fig. 6(b) demonstrates that for a finite attack frequency ($n = 10$), increasing the DoS attack duration in each period causes the MAS to deviate further from the expected location towards the origin. Additionally, Fig. 6(c) shows that for a given DoS attack duration, increasing the attack frequency (n) from $n = 0$ to $n = 20$ results in a greater deviation in the average consensus from the expected location, leading the MAS towards the origin.

V. Conclusion

In this paper, we analyzed consensus in discrete MASs under periodic DoS attacks. We established that a DoS attack of a finite period results in state consensus other than the average value. An analytical expression for the deviation in the average consensus equilibrium was obtained, showing its dependence on DoS attack frequency and duration. Our findings demonstrate that when the attack period is finite, the system can asymptotically reach a consensus at a perturbed location. Conversely, if the attack period is infinite, the deviation matrix converges to the null matrix, and the system behaves as a decoupled set of agents, each achieving equilibrium at the origin. In the future, we would like to expand our analysis to consider the DoS of heterogeneous frequencies on the different communication links in the network.

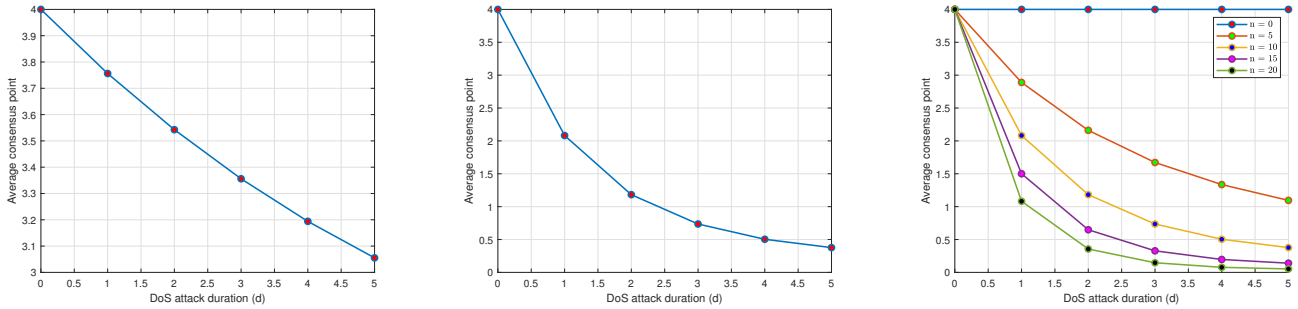
Appendix

Proof of Lemma 1. Let σ_i and ξ_i be the eigenvalues of $\mathcal{A}$ and $\mathcal{B}$, respectively, where $\sigma_i \in [-1, 1]$ and $\xi_i \in (-1, 1)$ for all $i = 1, \ldots, N$. Since $\mathcal{A}$ and $\mathcal{B}$ are symmetric matrices, the spectral norms of $\mathcal{A}$ and $\mathcal{B}$ are equal to their largest (absolute) eigenvalue, i.e., $\|\mathcal{A}\|_2 = \max_i |\sigma_i| \leq 1$ and



(a) Finite n (b) Sufficiently large n (c) Affect of varying d

Fig. 5: Average consensus point vs DoS attack frequency (n).



(a) Single attack period ($n = 1$) (b) Finite attack frequency ($n = 10$) (c) Affect of varying n

Fig. 6: Average consensus point vs DoS attack duration (d).

$\|\mathcal{B}\|_2 = \max_i |\xi_i| < 1$. The sub-multiplicative property of the spectral norm implies that $\|\mathcal{AB}\|_2 \leq \|\mathcal{A}\|_2\|\mathcal{B}\|_2$ (resp., $\|\mathcal{BA}\|_2 \leq \|\mathcal{B}\|_2\|\mathcal{A}\|_2$). Now using the prior bounds, it can be concluded that $\|\mathcal{AB}\|_2 < 1$ (resp., $\|\mathcal{BA}\|_2 < 1$). Since the spectral radius $\rho(\mathcal{M}) = \max_i |\lambda_i(\mathcal{M})|$ of any matrix of $\mathcal{M} \in \mathbb{R}^{N\times N}$ is its largest eigenvalue (in the absolute sense) and satisfies $\rho(M) \leq \|\mathcal{M}\|_2$, it follows that $\rho(\mathcal{AB}) \leq \|\mathcal{AB}\|_2 < 1$ (resp., $\rho(\mathcal{BA}) \leq \|\mathcal{BA}\|_2 < 1$). Therefore, the eigenvalues of $\mathcal{AB}$ (resp., $\mathcal{BA}$) lie in $(-1, 1)$. □

REFERENCES

[1] R. Olfati-Saber and R. Murray, "Consensus problems in networks of agents with switching topology and time-delays." *IEEE Transactions on Automatic Control*, vol. 49, no. 0, pp. 1520–1533, 2004.

[2] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[3] Y. Su and J. Huang, "Cooperative output regulation of linear multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 4, pp. 1062–1066, 2011.

[4] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control: 12th International Conference, HSCC 2009, San Francisco, CA, USA, April 13-15, 2009. Proceedings 12*. Springer, 2009, pp. 31–45.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Multi-agent systems: A survey," *Ieee Access*, vol. 6, pp. 28 573–28 593, 2018.

[6] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol. 47, no. 12, pp. 2757–2764, 2011.

[7] W. Zeng and M.-Y. Chow, "Resilient distributed control in the presence of misbehaving agents in networked control systems," *IEEE transactions on cybernetics*, vol. 44, no. 11, pp. 2038–2049, 2014.

[8] Y. Xu, M. Fang, P. Shi, and Z.-G. Wu, "Event-based secure consensus of mutiagent systems against dos attacks," *IEEE transactions on cybernetics*, vol. 50, no. 8, pp. 3468–3476, 2019.

[9] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under dos attacks," *IEEE Transactions on Control Systems Technology*, vol. 28, no. 3, pp. 741–752, 2019.

[10] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 5, pp. 779–789, 2016.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, 2005, pp. 46–57.

[12] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and dos attack," *IEEE transactions on cybernetics*, vol. 49, no. 4, pp. 1501–1511, 2018.

[13] Y. Wan, J. Cao, G. Chen, and W. Huang, "Distributed observer-based cyber-security control of complex dynamical networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 11, pp. 2966–2975, 2017.

[14] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Event-triggered control over unreliable networks subject to jamming attacks," in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 4818–4823.

[15] C. De Persis and P. Tesi, "Resilient control under denial-of-service," *IFAC proceedings Volumes*, vol. 47, no. 3, pp. 134–139, 2014.

[16] B. Chen, D. W. Ho, W.-A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under dos attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 2, pp. 455–468, 2017.

[17] Z. Feng, G. Hu, and G. Wen, "Distributed consensus tracking for multi-agent systems under two types of attacks," *International Journal of Robust and Nonlinear Control*, vol. 26, no. 5, pp. 896–918, 2016.

[18] Y. Xu, M. Fang, Z.-G. Wu, Y.-J. Pan, M. Chadli, and T. Huang, "Input-based event-triggering consensus of multiagent systems under denial-of-service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 4, pp. 1455–1464, 2018.

[19] C.-Q. Ma and J.-F. Zhang, "Necessary and sufficient conditions for consensusability of linear multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 5, pp. 1263–1268, 2010.

[20] S. Hu, Q.-L. Han, X. Xie, and C. Dou, "Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks," *IEEE Trans. on Cybernetics*, vol. 50, no. 5, May 2020.

[21] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.