Resilient Event-triggered Average Consensus Under Denial of Service Attack and Uncertain Network

Amir Amini, Student Member, IEEE, Ali Azarbahram, Student Member, IEEE, Arash Mohammadi, Member, IEEE, Amir Asif, Senior Member, IEEE

Abstract—The paper investigates resilient conditions for the event-triggered average consensus problem under denial of service (DoS) attack and uncertainty in the network. To reach average consensus in the multi-agent system, each node communicates with its neighboring nodes only if an event-triggering condition is satisfied. In the presence of the DoS attack, no information can be communicated within the network. In addition to DoS, the information being transmitted through the communication channels is perturbed due to uncertainty in the nominally designed edge weights of the network. Using the Lyapunov theorem, we analytically determine the maximum allowable duration and frequency for the DoS attack and maximum network uncertainty for which the exponential event-triggered consensus convergence stays preserved. The performance of the implementation is quantified through simulations in different scenarios.

Index Terms— Cyber-physical systems, Event-triggered consensus, Resilient control, Denial of service attack.

I. INTRODUCTION

Distributed average consensus is a major step in many collaborative signal processing and network control implementations including multi-agent coordination [1], sensor calibration [2], and node counting in multi-agent systems [3, Section 3.3]. Related works in this area primarily consider constant inter-node transmission within the network. Continuous data transmission is a critical restriction in networks with limited energy resources. Periodic and event-triggering schemes are proposed to prolong the energy of multi-agent systems. It is widely known that the event-triggering strategies, in general, offer superior performance as they allow nodes to transmit information, irrespective of a fixed time interval, and only if a dynamic triggering condition is satisfied [4]. Numerous event-triggered average consensus schemes have recently been developed based on different objectives [5].

One of the main recent concerns in networked control systems is the security of implementation and its resilience to different types of cyber-attacks which can vastly impact the consensus performance. In general, these attacks can be classified into two categories, namely, deception attacks [6] and denial of service (DoS) [7]. In the DoS attacks, the attacker attempts to block the transmission and measurement channels while in a deception attack the communicated information is manipulated by the attacker. Some literatures concerning DoS on networked control systems consider a continuous-time transmission scheme between the participating nodes [8]–[10]. Using an event-triggering scheme, the authors in [11] investigate resilient conditions for consensus subject to DoS attack, where the maximum tolerable duration and frequency for DoS intervals are obtained.

An important issue that has received little attention (especially in event-triggered setups) is the robustness of the approach to uncertainty in the network. Consensus protocols are often designed based on a linear weighted disagreement between the neighboring nodes. These weights either model the physical interaction between two nodes, or are designed beforehand as network design parameters. In both cases, it is important to investigate the robustness of controller to possible uncertainties in the network edge weights. Additionally, another scenario used by the attacker is to adversely impact the communication channels between the neighbouring nodes, which leads to variation in the nominal values of the edge weights used to model the network [12]. Unlike [12]–[15] where such uncertain networks are studied for continuous-time communications, the paper focuses on networks with event-triggered transmission.

To the best of our knowledge, there exists no study on resilience of event-triggered average consensus that simultaneously considers the DoS attack and network uncertainty, two obstacles that may coexist in real networked systems. A mathematical characterization of the network uncertainty and DoS attacks along with determination of the event-triggering parameters is an important (and yet a disregarded challenge) that motivates the paper.

The remaining paper is organized as follows. Section 2 introduces required preliminary concepts along with an overview of the problem. In Section 3, we formulate the event-triggered consensus problem under attack and derive sufficient conditions for resilience of the proposed implementation. We provide simulation examples in Section 4. Finally, Section 5 concludes the paper.

II. PRELIMINARIES AND PROBLEM STATEMENT

We use bold alphabets to represent matrices and vectors while normal letters are used to specify scalars. Notations \(1_N\) and \(0_N\) are column vectors of order \(N\) with, respectively, one and zero entries. For matrix \(A = \{a_{i,j}\}_{m \times n}\), \(A^T\) denotes the transpose of \(A\). \(N\) denotes the set of
natural number with \( N_0 = \mathbb{N} \cup \{0\} \). For two sets \( A \) and \( B \), \( A \setminus B \) denotes the elements belonging to \( A \) but not to \( B \). For a network with \( N \) nodes, \( \mathcal{A} = \{a_{ij}\}_{N \times N} \) is the weighted adjacency matrix; \( L \) is the Laplacian matrix; \( \lambda_2 \) and \( \lambda_N \) are, respectively, the second smallest and the largest eigenvalues of \( L \); and \( N_i \) is the neighbouring set for node \( i \).

We use the first-order multi-agent system given bellow to achieve distributed average consensus on an initially localized parameter \( x_i(0) \), [16],

\[
\dot{x}_i(t) = u_i(t), \quad i \in \mathcal{V},
\]

where \( \mathcal{V} = \{1, \ldots, N\} \) is the set of participating nodes and \( u_i(t) \in \mathbb{R} \) is the proposed distributed control law (to be introduced later), which forces average consensus, i.e., \( \lim_{t \to \infty} |x_i(t) - x_{\text{avg}}(0)| = 0 \), \( 1 \leq i \leq N \), where \( x_{\text{avg}}(t) = \frac{1}{N} \sum_{i=1}^{N} x_i(t) \).

**Assumption 1.** The multi-agent system (1) is configured as an undirected (symmetric) connected network.

To reach average consensus, node \( i \) shares its state value with its neighbours. In order to reduce the number of transmissions and preserve communication resources, a distributed event detector is incorporated with each agent. The event detector monitors an `event-triggering condition' (to be introduced later) to determine whether or not to transmit the agent’s state. If the event detector at node \( i \) detects an event, agent \( i \) transmits its current state to its neighbours. Upon receiving a new state value from node \( i \), node \( j \), \( j \in N_i \), updates its information and keeps using this value until another state value (i.e., the next event) is transmitted from node \( i \). Without loss of generality, let \( t_{k_i}^{[i]} \) denote the time instant at which the most recent event for node \( i \) is triggered. In the ideal operation (i.e., the attack free situation with ideal channels), the following distributed control law is proposed for node \( i \) to reach average consensus

\[
u_{i}^{[\text{ideal}]}(t) = -X_{i}^{[\text{ideal}]}(t),
\]

where \( X_{i}^{[\text{ideal}]}(t) = \sum_{j \in N_i} a_{ij} (x_j(t_{k_i}^{[i]}) - x_i(t_{k_i}^{[i]})) \) is the disagreement value for node \( i \). The disagreement value \( x_i(t) \) is used by the event detector to determine the next event instant. More precisely, given the most recent event instant \( t_{k_i}^{[i]} \), the next event for node \( i \) is triggered at \( t_{k_i+1}^{[i]} \) with \( t_{k_i+1}^{[i]} \) satisfying the following event-triggering condition

\[
t_{k_i+1}^{[i]} = \inf \{ t \mid t > t_{k_i}^{[i]}, |e_i(t)| - \phi |X_{i}^{[\text{ideal}]}(t)| \geq 0 \},
\]

where \( e_i(t) = x_i(t_{k_i}^{[i]}) - x_i(t) \) is the state error for node \( i \). Scalar \( \phi > 0 \) is the transmission threshold to be designed. Based on (3), if the transmission channels are never blocked by DoS attacks the following inequality always holds

\[ |e_i(t)| \leq \phi |X_{i}^{[\text{ideal}]}(t)|, \quad (1 \leq i \leq N). \]

\footnote{Superscript [i] in \( t_{k_i}^{[i]} \) is used to indicate node \( i \), and subscript \( k_i = 1, 2, \ldots \) denotes the sequence of events for node \( i \). Since the event detectors are asynchronous, the value of event counter \( k_i \) may be different from \( k_j \) at a certain time instant \( t \).}

As shown in Fig. 1, the multi-agent system considered in this paper faces the following obstacles during the consensus process:

- **Denial of Service Attack (DoS):** In presence of the DoS attacks, information can neither be received nor sent between the constituent nodes [7]. As a consequence of DoS, controller (2) cannot be updated and the agent state evolves in open-loop based on the last updated controller input before the DoS attack.
- **Uncertain Communication Channel:** Even when the information is transmitted in the absence of DoS, the nodes receive perturbed information due to uncertainties in the communication channels. As a consequence, the neighbouring states cannot be received precisely affecting the consensus convergence rate and system stability is engendered in the extreme case.

**A. Denial of Service Attack**

In this section, we model the DoS attacks based on the approach proposed in [7].

**Assumption 2.** The DoS attacks occur over disconnected intervals with finite durations, i.e., after an active period the attacker goes to the sleep mode to save on energy. The \( n^{th} \) DoS interval is given by the following expression

\[
D_n = [d_n, d_n + \tau_n), \quad n \in \mathbb{N}_0.
\]

We note that, due to the malicious nature of the attacker, the DoS intervals given in (5) do not necessarily follow any specific pattern nor a stochastic distribution. Next, we define \( n(t) \) which specifies the number of DoS attack intervals that have been occurred up to time \( t \), i.e.,

\[
n(t) = \begin{cases} 1, & \text{if } t < d_0, \\ \sup \{ n \in \mathbb{N} \mid d_n < t \}, & \text{otherwise}. \end{cases}
\]
From (5) and (6), we define the union of all DoS attack intervals up to time $t$ as follows

$$
D(t) = \bigcup_{n=0}^{n(t)-1} D_n \bigcup \left[ d_n(t), \min\{d_n(t)+\tau_n(t), t\} \right].
$$

Based on (7), notation $|D(t)|$ computes the total length of all attack intervals up to time $t$. The following assumption is considered for the duration and frequency of occurrence for the DoS intervals.

**Assumption 3.** There exist positive constants $\gamma$, $T$, $\kappa$, and $M$ such that the following upper-bounds hold [7],

$$
n(t) \leq \gamma + \frac{t}{T}, \quad |D(t)| \leq \kappa + \frac{t}{M}.
$$

(8)

**B. Uncertain Edge Weights**

In addition to the DoS attacks, multi-agent system (1) is subject to uncertainties in communication channels. More precisely, the edge weight $a_{i,j}$ is perturbed by an unknown but bounded parameter $\delta_{i,j}$. Therefore, the communication link from node $i$ to node $j$ is modeled by $a_{i,j} = a_{i,j} + \delta_{i,j}$, [12], [15], [17]. The Laplacian matrix under uncertainty can be viewed by the following perturbed Laplacian matrix

$$\tilde{L} = L + \Delta L.
$$

(9)

**Assumption 4.** The time-varying uncertainty $\delta_{i,j}$ satisfies $|\delta_{i,j}| \leq a_{i,j}$ for $t > 0$. Network connectivity is preserved for at all time instants. Moreover, $\|\Delta L\| \leq \delta_2$ for $t > 0$.

**Remark 1.** We note that the uncertain edge weight in the network configuration can also be translated to the following special cases: (i) The edge manipulation attack: Parameter $\delta_{i,j}$ can model another type of attack in which the attacker can access the transmission channel between nodes and manipulates the information being transmitted [12]. From the attacker perspective, these manipulations may be small due to energy constraints and detection avoidance. (ii) Packet dropout: The packet dropout from node $j$ to node $i$ can be modeled by (9) if $\delta_{i,j} = -a_{i,j}$ [18]. (iii) Actuator fault: The uncertain edge weight can represent a class of actuator fault known as the loss of actuator effectiveness. According to [19], such a faulty actuator is modeled by $u_{i,t} = \rho_{i}(t) u_{i,t}$, where $\rho_i$ is an unknown constant which belongs to a bounded set, e.g., $\rho_i \in [\hat{\rho}_i, \bar{\rho}_i]$. In a special case, the edge weights can model this class of actuator faults. (iv) Quantized state feedback: The quantized state feedback problem refers to the case where the actuators implement the quantized signals from the controller output [20]. It can be shown that a logarithmic quantized state feedback leads to an uncertain term in the closed-loop system which can be modeled as a special case of (9). In all cases, it is important to investigate the resilience of consensus algorithm to edge uncertainty, whether the source is from implementation constraints, faults, or security flaws.

In the next section, we will address these questions which are also our main design objectives: What is the operating region for transmission threshold $\phi$ to guarantee resilient average consensus in the presence of the DoS attacks and network uncertainty? What are the operating regions for $M$, $T$, and $\delta_L$ so that the average consensus is guaranteed? How is the rate of consensus convergence affected by different values of $\phi$, $M$, $T$, and $\delta_L$?

**III. Problem Formulation**

In this section, we analyze the closed-loop multi-agent system. Unlike the ideal scenario, in presence of the DoS attacks, the control law (2) can not always be updated in coordination with (3). Therefore, we define $k_i(t)$ as the index for the most recent event instant of node $i$, $(1 \leq i \leq N)$, that is successfully transmitted to node $j$, $(j \in \mathcal{N}_i)$, i.e.,

$$k_i(t) = \sup \left\{ k_i \in \mathbb{N}_0 \mid t_i^{[k_i]} < t, \quad t_i^{[k_i]} \notin \bigcup_{n=0}^{n(t)} D_n \right\}.
$$

(10)

Let $\mathcal{F}_i = \{ k_i \in \mathbb{N}_0 \mid t_i^{[k_i]} \in \bigcup_{n \in \mathbb{N}_0} D_n \}$ denote the set of unsuccessful transmission attempts for node $i$ which are denied by the DoS attacks. After a transmission attempt, if no acknowledgment is received a DoS interval is detected. Then, the transmission logic turns in to a different mode and periodically attempts to transmit an update so that an state can be transmitted as soon as the DoS interval is over. Let $\Delta_s > 0$ be the predefined period for these periodic update attempts. Based on the periodic attempts, we define $\tilde{D}_n = [d_n, d_n + \sigma_n + \Delta_s]$ as the $n$th ‘effective’ DoS interval during which (4) does not necessarily hold. Parameter $\sigma_n$ is defined as below

$$\sigma_n = \begin{cases} \tau_n & \text{if } \mathcal{F}_i = \emptyset, \forall i \in \mathcal{V} \\ \max\{t_i^{[k_i]} \mid k_i \in \mathcal{F}_i\} - d_n & \text{otherwise.} \end{cases}
$$

With such definition, two consecutive intervals for $\tilde{D}_n$ may overlap. To determine intervals (without intersection) where (4) does not necessarily hold, we define $\tilde{D}(t) = \bigcup_{m \in \mathbb{N}_0} Z_m \cap [0, t]$, with $Z_m = [\xi_m, \xi_m + \nu_m]$. Parameter $\xi_m$ is defined by $\xi_0 = t_0$ and $\xi_{m+1} = \inf\{d_n \mid d_n > \xi_m, d_n > d_{n-1} + \sigma_{n-1} + \Delta_s\}$. Parameter $\nu_m$ is as follows

$$\nu_m = \sum_{n \in \mathbb{N}_0, \xi_m \leq d_n < \xi_{m+1}} |\tilde{D}_n \setminus \tilde{D}_{n+1}|.
$$

On the other hand, notation $\tilde{R}(t) = \bigcup_{m \in \mathbb{N}_0} W_{m-1} \cap [0, t]$, with $W_{-1} = [0, \xi_0]$ and $W_m = [\xi_m, \nu_m, \xi_{m+1}]$, is the union of intervals with no intersection where (4) holds. Fig. 2 provides a schematic diagram to better illustrate different time notation used in the paper.

Based on (9) and (10), the disagreement value in the presence of DoS attacks and uncertainty in communication channels is modified to the following expression

$$X_i(t) = \sum_{j \in \mathcal{N}_i} a_{i,j} (x_j(t_i^{[k_i]})) - x_i(t_i^{[k_i]})).
$$

(11)
A. Stability Analysis

In the following theorem, we derive exponential stability conditions for system (16).

**Theorem 1.** Let the transmission threshold \( \phi \) satisfy the following upper-bound

\[
\phi < \frac{\lambda_2 - \delta_L}{(\lambda_N + \delta_L)(\lambda_2 + \lambda_N)}.
\]

For any DoS sequence satisfying Assumption 3 with arbitrary values for \( \gamma, T, K, M, \) and \( \Delta_* \), such that

\[
\frac{1}{M} + \frac{\Delta_*}{T} < \frac{\alpha_1}{\alpha_1 + \alpha_2},
\]

where \( \alpha_1 = \frac{\lambda_2}{\lambda_N + \delta_L} + \delta_L \) and \( \alpha_2 = \frac{\lambda_N + \delta_L}{1 - \frac{\phi(\lambda_N + \delta_L)}{(\lambda_N + \delta_L)(\lambda_2 + \lambda_N)}} \), system (16) is exponentially stable in the form of

\[
\|r(t)\| \leq \sqrt{\zeta} e^{-\frac{\zeta}{2}t}\|r(0)\|
\]

with the following parameters

\[
\zeta = \alpha_1 - \alpha_2 \left(\frac{1}{M} + \frac{\Delta_*}{T}\right),
\]

\[
\eta = e^{\left(\alpha_1 + \alpha_2\right)}.
\]

**Proof.** To use the Lyapunov stability theorem, we consider \( V(t) = \frac{1}{2}x^T(t)r(t) \) as the Lyapunov candidate. In what follows, the time derivative of \( V(t) \) is given along with (16)

\[
\dot{V}(t) = \left(-(L + \Delta_L)e(t) + r(t)\right)^T r(t)
\]

\[
= -e^T(t)(L + \Delta_L)^T r(t) - r^T(t)(L + \Delta_L)^T r(t).
\]

Using the second smallest and the largest eigenvalues of \( L \), we obtain the following inequality based on Assumption 4 and (21)

\[
\dot{V}(t) \leq -\lambda_2\|e(t)\|^2 + \lambda_N\|e(t)\|^2 \|r(t)\|^2 + \delta_L\|r(t)\|^2 + \delta_L\|e(t)\|^2 \|r(t)\|^2.
\]

Based on (12), inequality \( \|e(t)\|^2 \leq \phi(\|L + \Delta_L\| \|e(t)\| + \|r(t)\|) \) holds in a collective fashion if \( t \in W_m \), which leads to

\[
\|e(t)\| < \frac{\phi(\lambda_N + \delta_L)}{1 - \phi(\lambda_N + \delta_L)}\|r(t)\|.
\]

Incorporating (23) in (22) results in the following inequality

\[
\dot{V}(t) \leq -\alpha_1 V(t), \quad t \in W_m,
\]

where \( \alpha_1 \) is given in (18). On the other hand, if \( t \in Z_m \), we have

\[
\dot{V}(t) = - (L + \Delta_L)\hat{r}(\xi_m)^T r(t)
\]

\[
\leq (\lambda_N + \delta_L)\|r(t)\|\|\hat{r}(\xi_m)\|.
\]

In the beginning of the \( m \)th effective DoS interval, it holds that

\[
\|e(\xi_m)\| \leq \phi(\|L + \Delta_L\| \|\hat{r}(\xi_m)\|)
\]

which is equivalent to

\[
\|e(\xi_m)\| \leq \phi(\lambda_N + \delta_L)\|\hat{r}(\xi_m)\|.
\]

Based on the former inequality, the following condition is obtained

\[
\|\hat{r}(\xi_m)\| \leq \frac{1}{1 - \phi(\lambda_N + \delta_L)}\|r(\xi_m)\|.
\]
From (25) and (26), it holds that \( \dot{V}(t) \leq \alpha_2 \| r(t) \| \| r(\xi_m) \| \). If \( \| r(\xi_m) \| \leq \| r(t) \| \), then we have
\[
\dot{V}(t) \leq \alpha_2 V(t),
\] (27)
where \( \alpha_2 \) is given in (18). On the other hand, if \( \| r(t) \| \leq \| r(\xi_m) \| \) the following inequality is satisfied
\[
\dot{V}(t) \leq \alpha_2 V(\xi_m).
\] (28)
Combining (27) and (28), we obtain the following expression
\[
V(t) \leq e^{\alpha_2 (t-\xi_m)} V(\xi_m), \quad t \in Z_m.
\] (29)
Using some simple iterations [22], the two expressions derived for \( t \in W_m \), (i.e., (24)) and \( t \in Z_m \), (i.e., (29)) are included in the following condition
\[
V(t) \leq e^{\alpha_2 |\bar{D}(t)|} e^{-\alpha_1 |\bar{R}(t)|} V(0), \quad t \geq 0.
\] (30)
It is easy to verify that \( |\bar{D}(t)| \leq \frac{\bar{D}(t)}{1 + n(t) \Delta_k} \). Then, from Assumption 3 it holds that, \( |\bar{D}(t)| \leq \kappa_\delta + \frac{\delta}{M} \), where \( \kappa_\delta = \kappa + (1 + \gamma) \Delta_k \), and \( M = \frac{MT}{\kappa + \Delta_k} \). With \( |\bar{R}(t)| = 1 - |\bar{D}(t)| \), (30) gives way to the following expression
\[
\| r(t) \|^2 \leq e^{\kappa_\delta \alpha_2} e^{-t(\alpha_1 - \alpha_2)} \| r(0) \|^2, \quad t \geq 0,
\] (31)
which is equivalent to \( \| r(t) \| \leq \sqrt{\eta e^{-\zeta t}} \| r(0) \| \) with the given values of \( \eta \) and \( \zeta \) in (19). The operating region for \( \phi \) depends on \( \alpha_2 > 0 \) and that completes the proof.

**Remark 2.** (Design trade-offs) The following observations are made from (17), (18), and (19): (i) The maximum channel uncertainty \( \delta_k \) must be smaller than \( \lambda_2 \), otherwise, the transmission threshold \( \phi \) will be negative which is not acceptable. (ii) With larger values for \( \phi \), the right hand side of (18) in decreased, implying that a lower duration for DoS attack with less frequency is tolerable. Therefore, there is a trade-off between the transmission savings and maximum allowable DoS attacks in terms of duration and frequency. (iii) The convergence rate \( \zeta \) is decreased with larger values for \( \delta_L \) and smaller values for \( M \) and \( T \). (iv) As expected, with larger \( \delta_k \), the operating region for \( \phi \) is reduced. In addition, the lower-bound for \( M \) becomes larger which is translated to less tolerance to DoS attacks.

### B. Zeno-behaviour

In an event-triggered scheme, there must be a finite number of events within a finite time interval. Otherwise, the scheme exhibits a phenomenon known as the Zeno behavior. In what follows, we analyze the interval between two consecutive events and rule out the Zeno behaviour.

**Theorem 2.** Considering the event-triggering condition (12) and control law (13), the inter-event interval for node \( i \), \( 1 \leq i \leq N \), is strictly positive and satisfies
\[
\phi \int_{t_{k_i}(t)}^{t_{k_i}(t)+1} |X_i(\tau)| d\tau, \quad t \in W_m.
\] (32)

**Proof.** Consider \( t_{k_i}^{[i]}(t) \), \( t_{k_i}^{[i]}(t)+1 \in W_m \). According to (12), \( e_i(t_{k_i}^{[i]}(t)) = 0 \). Then, \( e_i(t_{k_i}^{[i]}(t)) \) evolves from zero until the next event instant \( t_{k_i}^{[i]}(t)+1 \) is determined by (12). From \( e_i(t) = x_i(t_{k_i}^{[i]}(t)) - x_i(t) \), we obtain \( \dot{e}_i(t) = -\dot{x}_i(t) \), which leads to \( \dot{e}_i(t) = X_i(t) \). The former equality results in \( e_i(t) = \int_{t_{k_i}^{[i]}}^{t} X_i(\tau) d\tau \). Based on (12) the next event is triggered when \( |e_i(t_{k_i}^{[i]}(t)+1)| = \phi |X_i(t_{k_i}^{[i]}(t)+1)| \). The next event is triggered at \( t = t_{k_i}^{[i]}(t)+1 \) which satisfies (32). Before consensus is achieved, it holds that \( |X_i(t)| \neq 0 \), which implies that \( t_{k_i}^{[i]}(t)+1 \) is strictly larger than \( t_{k_i}^{[i]}(t) \). We note that if \( t \in Z_m \), no event can be triggered. Therefore, the first event instant transmitted after a DoS interval is strictly larger than the last successful event.

### IV. Simulations

In this section, we validate our theoretical results through simulation experiments. First, we select a network with six nodes, i.e., \( N = 6 \), which is represented by the following Laplacian matrix
\[
L = \begin{bmatrix}
3 & -1 & -1 & 0 & 0 & -1 \\
-1 & 4 & 0 & -1 & -1 & 0 \\
-1 & 0 & 2 & 0 & -1 & 0 \\
0 & -1 & 0 & 2 & -1 & 0 \\
0 & -1 & -1 & 4 & -1 & 0 \\
-1 & 0 & 0 & 0 & -1 & 3
\end{bmatrix}.
\] (33)

It can be verified that \( \lambda_2 = 1.6072 \) and \( \lambda_0 = 5.5869 \) for this network. We assume that \( \delta_{ij} = \rho \) for all \( a_{ij} \neq 0 \), where \( \rho \) is a random variable identically distributed in \( (0, 0.01) \). With this uncertainty in the adjacency matrix, it holds that \( \|\Delta_L\| \leq 0.01\|L\| \). Therefore, \( \delta_L = 0.0872 \). Using the values of \( \lambda_2 \), \( \lambda_0 \), and \( \delta_L = 0.0872 \), the maximum allowable value for transmission threshold \( \phi \) is calculated from (17) as \( \phi_{\text{max}} = 0.0372 \). We select \( \phi = 0.5\phi_{\text{max}} = 0.0186 \) as the operating value for \( \phi \). Let \( \psi = \frac{1}{M} + \frac{\Delta}{\phi} \). With

| TABLE I: Consensus performance for different \{ \phi, \delta_L \} with fixed \psi = 0.1263. |
|---|---|---|---|
| \( \delta_L \) | \( \phi / \phi_{\text{max}} \) | \( \zeta \) | \( T^* \) | \( \Delta \Sigma \) |
| 0.0436 | 0.5 | 0.2455 | 2.5150 | 93.6 |
| 0.1744 | 0.5 | 0.2256 | 2.5120 | 99.0 |
| 0.2615 | 0.5 | 0.2122 | 2.5089 | 110.5 |
| 0.0872 | 0.1 | 0.6399 | 2.5510 | 491.5 |
| 0.0872 | 0.3 | 0.1307 | 2.5329 | 165.6 |
| 0.0872 | 0.5 | 0.2389 | 2.5120 | 96.0 |
the given values, $\psi$ should satisfy $\psi < 0.1799$ from (18). Let $\Delta_1 = 0.01$, $M = 8$, and $T = 8$ which leads to $\psi = 0.1263$. Using (19), the guaranteed rate for average consensus is obtained as $\zeta = 0.2075$. Two DoS attack intervals are assumed in this setting with $d_1 = 0.2$, $\tau_1 = 0.05$, $d_2 = 1$, and $\tau_2 = 0.05$. Starting from initial values $x_i(0) = i$, $(1 \leq i \leq 6)$, we run the consensus process until $t = t^*$, where $t^* = \min \{ t \mid \|r(t)\| \leq 0.02 \}$ provides an acceptable threshold for the average consensus. For this setting, $t^* = 2.5122$ s. The evolution of the states $x_i(t)$ and $u_i(t)$ for the six nodes are shown, respectively, in Figs. 3(a) and (b). The six nodes, respectively, trigger 103, 76, 106, 111, 81, and 58 events (as shown in Fig. 3(c)), leading to an average event (\$AE\$) of 89 per node. In Fig. 3(d), we compare the guaranteed rate $e^{-0.41505\|r(0)\|}$ with the actual rate $\|r(t)\|$, which satisfies the exponential convergence.

Next, we study the effect of varying parameters $\delta_L$ and $\phi/\phi_{\text{max}}$ with fixed $\psi = 0.1263$ on average consensus for (33). For given values of $\delta_L$ and $\phi/\phi_{\text{max}}$ in each row of Table 1, we run average consensus. The results for $\zeta$, $t^*$, and \$AE\$ are listed in Table 1, based on which we observe that: (i) For fixed $\phi/\phi_{\text{max}}$, increasing $\delta_L$ leads to smaller values for $\zeta$ (which accordingly affects $t^*$); (ii) For fixed $\delta_L$, increasing $\phi/\phi_{\text{max}}$ decreases the \$AE\$. However, the maximum tolerable DoS attack in terms of duration and frequency is also decreased.

Finally, we investigate the resilience of a random network with $N = 20$ ($\lambda_2 = 3.4324$ and $\lambda_3 = 14.5802$) against various selections for $\delta_L$ and two DoS intervals with different durations until $t = 2$. Let $\delta_L \in \{0.21, 0.42, 0.63, 0.84\}$ and $|D(2)| \in \{0.025, 0.050, 0.075, 0.1\}$. For each pair $(\delta_L, |D(2)|)$, we run event-triggered average consensus with $\phi/\phi_{\text{max}} = 0.5$. Corresponding values for $t^*$ and \$AE\$ are shown in Figs. 4(a) and (b) with respect to $\delta_L$ and $|D(2)|$, which corroborate the expected relations discussed in Remark 2.

**V. Conclusion**

The paper studies resilient conditions for an event-triggered average consensus implementation under the denial of service (DoS) attacks and uncertainty in communication channels. The DoS attacks occur in disconnected intervals due to the energy constraints from the attackers perspective. The Lyapunov stability theorem is used to compute the maximum tolerable DoS attacks (in terms of duration and frequency) and maximum network uncertainty under which the closed-loop stability is preserved. The relations between eigenvalues of the Laplacian matrix, upper-bounds for network uncertainty and DoS intervals, and transmission threshold are derived analytically.

**References**