Stability of consensus-based distributed estimation under denial of service

Giorgio Battistelli, Luigi Chisci, Daniela Selvi, and Pietro Tesi

***Abstract*—This paper aims to study the stability properties of consensus-based *distributed state estimation* (DSE) in the presence of *denial of service* (DoS) attacks. Specifically, we adopt a model which describes DoS in terms of its average frequency and duration. We focus on a family of DSE algorithms enjoying stability properties in the ideal case of no attacks, and prove that such properties are preserved under DoS provided that appropriate conditions are satisfied, with specific emphasis on the relation between transmission rate on one hand, and bounds on DoS frequency and duration on the other. Numerical simulation tests are shown concerning a target tracking case study.**

***Index Terms*—Distributed state estimation, consensus, sensor networks, denial of service**

I. INTRODUCTION

Modern control and monitoring systems have been highly influenced by the extraordinary recent breakthrough of wireless communication technology. In this respect, a lot of research efforts have been devoted to effectively utilize the available distributed sensing, computation and actuation resources so as to develop scalable multi-agent systems with improved performance without compromising the stability guarantees of their single-agent or centralized counterparts. Another key issue that is recently receiving great attention is the safe operation of such systems against cyber attacks of several types. In this context, this paper investigates the robustness of state-of-the-art *distributed state estimation* (DSE) algorithms under *Denial-of-Service* (DoS) attacks.

Recent works [1], [2], [3] have developed consensus-based DSE algorithms with guaranteed stability, in terms of boundedness of the state estimation error of all agents, under the fulfilment of minimal conditions on connectivity among agents and observability/detectability from the whole set of agents. In particular, we will consider the family of DSE algorithms known as *Hybrid Consensus on Measurements − Consensus on Information* (HCMCI) [1] which encompasses, as special cases, *Consensus on Information* [4] and *Information Weighted Consensus* [2]. In HCMCI, information is diffused through the network by performing two parallel consensus tasks, respectively on the prior information pair (associated with the predicted estimates and covariances) and on the likelihood information pair (associated with the measurements). The goal of this paper is to investigate whether such a family of algorithms is resilient to DoS attacks that temporarily prevent the agents from receiving consensus data by, e.g., injecting an interference/jamming signal into the communication channel. This investigation is motivated by the following main reasons: i) the robustness of networked systems under DoS attacks has received increasing attention in recent years for its inherent theoretical challenges and its practical relevance in system safety and cybersecurity, see for instance [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18] and the recent survey papers [19], [20], [21]; however most of the existing works deal with the centralized setting; ii) previous work on the stability of HCMCI under imperfect communication addresses the case of packet losses due to random link failures [22], however it is well known that communication failures due to DoS attacks typically exhibit a profile that is quite different from genuine packet losses, like the ones considered in [22]; specifically, failures induced by DoS need not follow a class of probability distributions [6], see for instance the DoS modeling framework introduced in [7] which characterizes DoS only in terms of its average frequency and duration, without relying on any assumption on the structure of the DoS attack signal; iii) from the theoretical point of view, considering deterministic bounds on the DoS frequency and duration [7] requires a different analysis than existing ones [22]. In particular, in this note the objective is to perform a worst-case analysis by providing deterministic error bounds that hold for all possible DoS patterns within the considered class. This is in contrast with existing probabilistic-type analysis like the one of [22] where error bounds hold in expectation.

The main contribution of this note is to show that the family of HCMCI DSE algorithms preserves its stability guarantees under the general classes of DoS signals modeled as in [7], provided that a sufficiently high transmission rate, related to the bounds on DoS frequency and duration, is ensured. For a fixed transmission frequency, our results provide a characterization of the robustness of HCMCI with respect to DoS attacks, which can be interpreted as the average percentage of transmission failures, or *jamming rate* [23], for which stability of the estimation error dynamics is still preserved. This investigation complements existing work on DSE with a robustness analysis which can be relevant for researchers and practitioners in the fields of networked systems and cybersecurity. A preliminary version of this work was presented in [24]. As compared to [24], this note includes more comprehensive simulation results and complete mathematical derivations. In particular, no proofs were given in [24], while here detailed proofs of all our robustness results are provided under the general case of *asynchronous* DoS that can affect any network link independently from one another.

II. DISTRIBUTED ESTIMATION FRAMEWORK

We consider a network $(\mathcal{N}, \mathcal{A})$, with the set of nodes denoted by $\mathcal{N}$ and the set of connections (arcs) denoted by $\mathcal{A} \subseteq \mathcal{N} \times \mathcal{N}$. All the nodes have processing and communication capabilities; a subset $\mathcal{S} \subseteq \mathcal{N}$ of the nodes, called *sensors*, can also sense data from the environment. For each node $i \in \mathcal{N}$, we define the set $\mathcal{N}^i$ of its *in-neighbors,* including i itself, as $\mathcal{N}^i \triangleq \{j : (j,i) \in \mathcal{A}\} \cup \{i\}$.

Each sensor node $i \in \mathcal{S}$ acquires measurements of the state $x(t)$ of a dynamical system

$$\dot{x}(t) = A_c x(t) + w(t) \tag{1}$$

at the sampling instants $t_k = k\,\Delta$, $k \in \mathbb{N} = \{0, 1, \dots\}$, with Δ the sampling interval, through the measurement equation

$$y_k^i \quad = \quad C^i x(t_k) + v_k^i\,, \qquad i \in \mathcal{S}, \tag{2}$$

where $w(t)$ is the process disturbance, and v_k^i is the measurement noise in node $i \in \mathcal{S}$. Then, the DSE problem over $(\mathcal{N}, \mathcal{A})$ can be expressed as follows. For each sampling time t_k, each node $i \in \mathcal{N}$ has to provide an estimate $\hat{x}_{k|k}^i$ of the state $x(t_k)$ of the

G. Battistelli, L. Chisci and P. Tesi are with Dipartimento di Ingegneria dell'Informazione (DINFO), Università di Firenze, Via Santa Marta 3, 50139 Firenze, Italy. e-mail: {giorgio.battistelli,luigi.chisci,pietro.tesi}@unifi.it

D. Selvi is with Dipartimento di Ingegneria dell'Informazione (DII), Università di Pisa, and with Centro di Ricerca "Enrico Piaggio", Università di Pisa, Largo Lucio Lazzarino 1, 56122 Pisa, Italy. e-mail: daniela.selvi@unipi.it

Published paper : https://ieeexplore.ieee.org/abstract/document/10255257
DOI : 10.1109/TAC.2023.3317306

dynamical system (1) given the local measurements (2) and data (e.g., estimates, associated covariances, etc.) received from all the in-neighbors $j \in \mathcal{N}^i$. For the sake of notational simplicity, we assume that all the sensor nodes collect measurements from process (1) at the same time instants t_k. This assumption could be removed, for example, by introducing a time stamp in the data exchanged by the nodes, and by aligning estimates and covariances to a common time through prediction before fusing them [25].

We first focus on the ideal case in which any transmission from each $j \in \mathcal{N}^i$ to i, $\forall i$, is successful, and recall that, in this situation, the family of DSE algorithms known as HCMCI [1] has been proved to ensure stability under appropriate hypotheses on collective observability and network connectivity. The remaining part of this section will provide a brief overview of the HCMCI family of algorithms as proposed in [1] in perfect communication conditions; then, in Section III-A, HCMCI will be analyzed when data transmission between network nodes can be unsuccessful.

From the discretization of (1)-(2), the following discrete-time system is obtained:

$$x_{k+1} = Ax_k + w_k \tag{3}$$
$$y_k^i = C^i x_k + v_k^i, \qquad i \in \mathcal{S}, \tag{4}$$

where $x_k = x(t_k)$, $A = e^{A_c \Delta}$, $w_k = \int_{t_k}^{t_{k+1}} e^{A_c (t_{k+1}-\tau)} w(\tau) d\tau$.

In HCMCI, each node $i \in \mathcal{N}$ runs a local Kalman filter and consensus is employed in order to improve the local estimates. Specifically, in the following we will use the *information form* of the Kalman filter recursion which, instead of the estimate $\hat{x}^i_{k|k}$ and of the covariance matrix $P^i_{k|k}$, propagates the *information matrix* $\Omega^i_{k|k} = (P^i_{k|k})^{-1}$ and the *information vector* $q^i_{k|k} = \Omega^i_{k|k}\hat{x}^i_{k|k}$. For each $k \in \mathbb{N}$ and $i \in \mathcal{N}$, the HCMCI algorithm is carried out as in Table I, where we adopt the notation $A^{-\top} := (A^{-1})^\top$ (we underline that A is invertible by construction, since it is obtained by discretizing a continuous-time linear system).

In the HCMCI algorithm of Table I, two consensus tasks are performed in parallel in order to diffuse information through the sensor network: one on the predicted information pair $(q^i_{k|k-1}, \Omega^i_{k|k-1})$; the other on the likelihood information pair $(\delta q^i_k, \delta\Omega^i_k)$, related to the local correction term depending on the measurements. The consensus weights $\pi^{i,j}$ are strictly positive and such that

$$\sum_{j \in N^i} \pi^{i,j} = 1 \tag{5}$$

so that the resulting consensus matrix is row stochastic. A possible choice are uniform weights, i.e. $\pi^{i,j} = 1/|\mathcal{N}^i|$ for $j \in \mathcal{N}^i$, where $|\mathcal{N}^i|$ is the cardinality of $\mathcal{N}^i$ (recall that $\mathcal{N}^i$ includes i as well as its in-neighbors). Other possibilities include Metropolis weights as defined in [26] or Laplacian weights [27].

The outputs of the two consensus tasks are then combined in the correction step where the contribution of the likelihood information pair is weighted by a scalar ω^i_k. With this respect, Table I actually provides a family of distributed filters corresponding to different choices of the scalar weights ω^i_k. For instance, when $\omega^i_k = 1$, the *consensus on information* filter of [4] is retrieved. If instead ω^i_k is equal to the number $|\mathcal{N}|$ of network nodes, then the resulting algorithm coincides with the *information weighted consensus* [2]. Guidelines for the choice of the scalar weights ω^i_k are provided in [1].

Finally, each node carries out the usual Kalman filter prediction step to get the predicted information pair at time $k+1$. We refer the reader to [1] for a thorough discussion about the properties of the algorithm of Table I.

Notice that, in the algorithm of Table I, W and V^i, $i \in \mathcal{S}$, are given positive definite matrices. Typically, W is an estimate of the inverse covariance of the process disturbance w_k, while each V^i is an estimate of the inverse covariance of the measurement noise v^i_k affecting the i-th sensor. Further, the algorithm is initialised with arbitrary $q^i_{0|-1}$ and positive definite matrices $\Omega^i_{0|-1}$, $i \in \mathcal{N}$, which ensures $\Omega^i_{k|k} > 0$ for every $k \in \mathbb{N}$ and $i \in \mathcal{N}$. The specific choices of W, V^i, $q^i_{0|-1}$, and $\Omega^i_{0|-1}$ have no impact on the stability analysis of Section IV.

In the next sections, we will address the problem of determining the stability properties of HCMCI in non-perfect communication conditions. In particular, Section III will present the DoS model adopted within our analysis. Then, before exposing our theoretical results (Section IV), we will briefly discuss in Section III-A how the HCMCI algorithm is modified when the network links may be temporarily interrupted by DoS.

TABLE I: HCMCI algorithm [1]

Compute the local correction terms:
if $i \in \mathcal{S}$ **then**
  collect the measurement y^i_k
  $\delta q^i_k = \left(C^i\right)^T V^i\, y^i_k$
  $\delta\Omega^i_k = \left(C^i\right)^T V^i\, C^i$.
else
  $\delta q^i_k = 0$, and $\delta\Omega^i_k = 0$
end if
Consensus:
$\delta q^i_k(0) = \delta q^i_k$, $\delta\Omega^i_k(0) = \delta\Omega^i_k$,
$q^i_k(0) = q^i_{k|k-1}$, $\Omega^i_k(0) = \Omega^i_{k|k-1}$,
for $\ell = 0, 1, \ldots, L-1$ **do**
  fuse the quantities $\delta q^j_k(\ell)$ and $\delta\Omega^j_k(\ell)$ as
  $\delta q^i_k(\ell+1) = \sum_{j \in \mathcal{N}^i} \pi^{i,j}\ \delta q^j_k(\ell)$
  $\delta\Omega^i_k(\ell+1) = \sum_{j \in \mathcal{N}^i} \pi^{i,j}\ \delta\Omega^j_k(\ell)$
  and in parallel fuse the quantities $q^j_k(\ell)$ and $\Omega^j_k(\ell)$ as
  $q^i_k(\ell+1) = \sum_{j \in \mathcal{N}^i} \pi^{i,j}\ q^j_k(\ell)$
  $\Omega^i_k(\ell+1) = \sum_{j \in \mathcal{N}^i} \pi^{i,j}\ \Omega^j_k(\ell)$
end for
Correction:
$q^i_{k|k} = q^i_k(L) + \omega^i_k\, \delta q^i_k(L)$
$\Omega^i_{k|k} = \Omega^i_k(L) + \omega^i_k\, \delta\Omega^i_k(L)$
$\hat{x}^i_{k|k} = \left(\Omega^i_{k|k}\right)^{-1} q^i_{k|k}$
Prediction:
$q^i_{k+1|k} = A^{-\top}\left[I - \Omega^i_{k|k}(\Omega^i_{k|k} + A^\top W A)^{-1}\right] q^i_{k|k}$
$\Omega^i_{k+1|k} = A^{-\top}\Omega^i_{k|k}A^{-1} - A^{-\top}\Omega^i_{k|k}(\Omega^i_{k|k} + A^\top W A)^{-1}\Omega^i_{k|k}A^{-1}$

III. A DETERMINISTIC MODEL FOR DoS

We will refer to DoS as the phenomenon that prevents communication among the network nodes. Following [7], we consider a DoS model that characterizes communication failures in terms of average frequency and duration. Let $\{h^{i,j}_n\}_{n \in \mathbb{N}}$, with $h^{i,j}_0 \geq 0$, denote the sequence of DoS *off/on* transitions on the link $(i,j) \in \mathcal{A}$, *i.e.*, the sequence of time instants at which the link (i,j) enters a DoS status. Accordingly,

$$H^{i,j}_n := [h^{i,j}_n, h^{i,j}_n + \tau^{i,j}_n) \tag{6}$$

is the n-th time-interval of length $\tau^{i,j}_n > 0$ over which nodes i and j cannot exchange data. Given $\tau, t \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$, let $n^{i,j}(\tau, t)$ denote the number of DoS *off/on* transitions over $[\tau, t]$ on the link (i,j), and let

$$D^{i,j}(\tau, t) := \bigcup_{n \in \mathbb{N}} H^{i,j}_n \bigcap [\tau, t]\,, \tag{7}$$

be the subset of $[\tau, t]$ where the link (i, j) is in DoS status. Finally, let $|D^{i,j}(\tau, t)|$ denote the Lebesgue measure of $D^{i,j}(\tau, t)$.

We consider the following assumption [7].

A1. The DoS signal satisfies the following conditions:

(i) (*DoS frequency*). There exist constants $\eta \geq 0$ and $\tau_D > 0$ such that

$$n^{i,j}(\tau, t) \leq \eta + \frac{t - \tau}{\tau_D} \tag{8}$$

for all τ, t with $t \geq \tau$, and $(i, j) \in \mathcal{A}$.

(ii) (*DoS duration*). There exist constants $\kappa \geq 0$ and $T > 1$ such that

$$|D^{i,j}(\tau, t)| \leq \kappa + \frac{t - \tau}{T} \tag{9}$$

for all τ, t with $t \geq \tau$, and $(i, j) \in \mathcal{A}$.

Assumption A1 characterizes DoS attacks in terms of their *average* frequency and duration. Specifically, $1/\tau_D$ gives an upper bound on the average frequency at which attacks may occur on any network link, while η is a regularization term that permits to have, on finite intervals, DoS attacks occurring at a frequency higher than $1/\tau_D$. Condition (9) expresses a similar requirement with respect to the DoS duration, i.e. the property that, on the average, the total duration over which communication is interrupted does not exceed a certain *fraction* of time, as specified by $1/T$. Like η, the constant κ plays the role of a regularization term. The requirements $\tau_D > 0$ and $T > 1$ imply that DoS cannot occur at an infinitely fast rate or be always active. The considered DoS model can describe many attack scenarios, ranging from *short-but-frequent* attacks to *long-but-infrequent* attacks. Examples in the latter category are the so-called *trivial* and *periodic* jamming attacks (the interested reader is referred to [7]), while examples in the former category are the so-called *protocol-aware* jamming attacks [28], [29].

Note that the network links can be affected by DoS independently of one another. In the sequel, we will refer to this general scenario as *asynchronous* DoS. We will instead refer to *synchronous* DoS when $H_n^{i,j} = H_n$ for every $n \in \mathbb{N}$ and i, j with $(i, j) \in \mathcal{A}$. This latter case occurs when DoS affects all the network links simultaneously and is of interest in networks operating through a single access point, in the so-called "infrastructure" mode.

We point out that (8) and (9), for any fixed parameters η, τ_D, κ, and T, do not identify a specific DoS pattern, but a class of DoS signals. The aim of our investigation is then to analyse stability and performance properties of HCMCI algorithms in the presence of *any* DoS signal satisfying Assumption A1. In this sense, our analysis can be regarded as a worst-case analysis, as we give stability conditions (and performance bounds) that hold *for all* the DoS signals within the class of interest.

We close this section with a technical lemma borrowed from [8] which quantifies the maximum number of consecutive transmission failures that can occur on any link in the presence of DoS modeled as in Assumption A1. Before stating such result (for its proof, the interested reader is referred to [8, Lemma 1]), we note that, in the HCMCI algorithm, L transmissions occur for each node in each sampling interval $[t_k, t_{k+1})$, where L is the number of consensus steps carried out at each time instant k. With this respect, in case of possible communication failures caused by DoS following the model of Assumption A1, it is important to introduce the following design condition on data transmission.

Design Condition (DC). Each network node transmits data periodically with period Δ/L, where both Δ and L are design parameters.

The following lemma can now be stated.

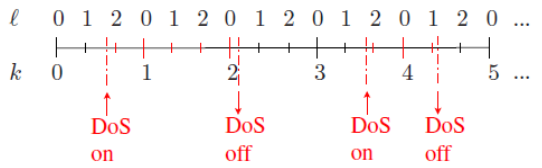

Fig. 1: Example of transmission failures (i.e., the transmission attempts occurring in the intervals highlighted in red between "DoS on" and "DoS off") in the HCMCI algorithm with $L = 3$ under DoS. In case of synchronous DoS, transmission failures occur over all the network links simultaneously. In case of asynchronous DoS, this example refers to any of the network links. We recall that transmission attempts occur at any ℓ, for each k.

Lemma 1: [8] Suppose that Assumption A1 and design condition DC are satisfied and that

$$\frac{1}{T} + \frac{\Delta}{\tau_D L} < 1. \tag{10}$$

Then, the maximum number of consecutive transmission failures on any link (i, j) is bounded from above by the constant

$$\bar{\Theta} := \left(\frac{\kappa L}{\Delta} + \eta\right)\left(1 - \frac{1}{T} - \frac{\Delta}{\tau_D L}\right)^{-1}. \tag{11}$$

■

Lemma 1 captures the intuition that DoS attacks that are very frequent (τ_D small) or sustained (T small) result in large values of $\bar{\Theta}$, i.e., can destroy a large number of tranmissions. As shown in [8], condition (10) is indeed *necessary* in the sense that DoS attacks with frequency and duration such that $1/T + \Delta/(\tau_D L) \geq 1$ can destroy all the transmissions. We note that (10) requires in particular that $\tau_D > \Delta/L$. This means that, on the average, DoS cannot occur at the same rate as (or faster than) L/Δ, which is the rate at which the network nodes exchange information. We also note that, when $\kappa = \eta = 0$, then DoS is absent and we obtain $\bar{\Theta} = 0$, meaning that all the transmissions succeed. We point out that the existence of an upper bound on the maximum number of consecutive transmission failures on any network link is essential for the stability of the HCMCI algorithm under DoS modeled as in Assumption A1, as it will be clarified in Section IV.

A. HCMCI under communication failures

In this section, we consider the HCMCI algorithm in the case in which the information transmitted by any node $j \in \mathcal{N}^i$ can fail to reach node i, for any $i \in \mathcal{N}$, due to DoS attacks following the model of Assumption A1. A schematic representation of such events is shown in Fig. 1. In this context, we denote the network by $(\mathcal{N}, \mathcal{A}_{k,\ell})$, where the set $\mathcal{N}$ of nodes is the same as before, and the set of arcs $\mathcal{A}_{k,\ell} \subseteq \mathcal{A}$ can vary at each time instant k and consensus step ℓ of the HCMCI algorithm of Table I. In accordance with such notation, we denote by $\mathcal{N}_{k,\ell}^i \subseteq \mathcal{N}^i$ the set of in-neighbors of node i that successfully transmit their local information to node i at time k and consensus step ℓ. We point out that the transmitted data $\delta q_k^j(\ell)$, $\delta\Omega_k^j(\ell)$, $q_k^j(\ell)$, and $\Omega_k^j(\ell)$ are assumed to be included in a single packet; this is a reasonable assumption, as the dimension of the transmitted data is $\dim(x)(\dim(x)+3)$, where $\dim(x)$ is the state dimension. Therefore, when transmission fails, all such data are lost. To address the DSE problem under communication failures, the HCMCI algorithm of Table I must include in the consensus steps, for any time instant k and consensus step ℓ, only the nodes belonging to $\mathcal{N}_{k,\ell}^i$, thus requiring that the consensus weights are re-computed

for each k and for each ℓ in order to satisfy condition (5). This can be achieved, for example, by simply rescaling the weights $\pi^{i,j}$ as follows

$$\pi^{i,j}_{k,\ell} = \begin{cases} \dfrac{\pi^{i,j}}{\sum_{j\in\mathcal{N}^i_{k,\ell}} \pi^{i,j}} & \text{if } j \in \mathcal{N}^i_{k,\ell} \\ 0 & \text{otherwise} \end{cases} . \tag{12}$$

Accordingly, we will refer in the following to $\Pi_{k,\ell}$ as the consensus matrix at time instant k and consensus step ℓ, whose elements are defined by (12).

IV. STABILITY ANALYSIS

In this section, we present the stability analysis of the HCMCI algorithm under communication failures characterized in terms of the DoS model following Assumption A1. Specifically, the result that we derive provides a relationship between the parameters τ_D and T (characterizing the adopted DoS model) on one hand, and L and Δ (especially, their ratio Δ/L, characterizing the frequency of data transmission among the network nodes) on the other one, so that, for any fixed τ_D and T, it is possible to determine the minimum transmission period Δ/L for which stability is still ensured.

The first part of the analysis is focused on highlighting some properties enjoyed by the consensus weights that will be useful for the subsequent derivations. Consider first the case in which no transmission failures occur, i.e., the network $(\mathcal{N}, \mathcal{A})$ is time-invariant. We denote by $\mathcal{N}^i(\gamma)$ the set of nodes from which node i can be reached following a directed path of length at most γ in $(\mathcal{N}, \mathcal{A})$. This means that, in absence of communication failures, the data transmitted by any node $j \in \mathcal{N}^i(\gamma)$ can reach node i in at most γ hops. In particular, by definition, $\mathcal{N}^i(0) = \{i\}$ and $\mathcal{N}^i(1) = \mathcal{N}^i$. Thanks to the results of Section III, we will show in the following that a similar characterization holds also for the time-varying network $(\mathcal{N}, \mathcal{A}_{k,\ell})$ subject to transmission failures. Consider a discrete-time window $[k-N, k]$ and let

$$\Pi|^k_{k-N} \triangleq \Pi_{k,L-1} \cdots \Pi_{k,0} \cdots \Pi_{k-N,L-1} \cdots \Pi_{k-N,0} \tag{13}$$

be the consensus matrix obtained from the ordered products of all the consensus matrices associated to the network $(\mathcal{N}, \mathcal{A}_{k,\ell})$ in $[k-N, k]$. Notice that, in the discrete-time window $[k-N, k]$, the total number of transmission attempts is $(N+1)L$. Recalling Lemma 1, and defining $\Theta := \lceil \bar{\Theta} \rceil + 1$ (with $\lceil \bar{\Theta} \rceil$ the smallest integer greater than or equal to $\bar{\Theta}$), we can assert that, when the transmission frequency is high enough, for every arc (j, i) in the network at least one every Θ transmissions is successful. This means that, when $L(N+1) \geq \Theta$, in the discrete-time window $[k-N, k]$, there is at least one successful communication between j and i for any $j \in \mathcal{N}^i$, so that the element $(\Pi|^k_{k-N})_{i,j}$ is ensured to be strictly positive. Generalizing, when $L(N+1) \geq \gamma\Theta$, the information transmitted by a node $j \in \mathcal{N}^i(\gamma)$ can reach node i along a path consisting of γ successful transmissions. Then, the following result holds.

Lemma 2: Let the same assumptions as in Lemma 1 hold. Then, for any N such that $L(N+1) \geq \gamma\Theta$, there exists a constant $\varepsilon > 0$ such that

$$(\Pi|^k_{k-N})_{i,j} > \varepsilon \tag{14}$$

for any $j \in \mathcal{N}^i(\gamma)$ and any $k \geq N$.

Proof: Consider a generic node $j \in \mathcal{N}^i(\gamma)$. Then, there exists a path of length at most γ from j to i, i.e., there exists a sequence of arcs $(i_0, i_1), \ldots, (i_{h-1}, i_h)$ belonging to $\mathcal{A}$ such that $i_0 = j$, $i_h = i$, and $h \leq \gamma$. Consider now the $(N+1)L$ transmission attempts (consensus steps) performed in the discrete-time window $[k-N, k]$. Clearly, in the first Θ consensus steps at least one transmission from i_0 to i_1 is successful. Then, in the consensus steps from $\Theta+1$ to 2Θ, at least one transmission from i_1 to i_2 is successful, and so on. Using the terminology of [3], this means that, in the discrete-time window $[k-N, k]$, there exists an *orderly appearing path* going from node j to node i. Further, as a result of the rescaling, the non-null elements of the matrix $\Pi_{k,\ell}$ are such that $\pi^{i,j}_{k,\ell} \geq \pi^{i,j}$. Hence, (14) directly follows from Lemma 15 of [3]. In particular, the lower bound in (14) can be taken as $\hat{\pi}^{L(N+1)}$ where $\hat{\pi} > 0$ is the smallest among the consensus weights $\pi^{i,j}$ with $i \in \mathcal{N}$ and $j \in \mathcal{N}^i$ (recall that all these weights are positive by hypothesis). ■

We point out that the lower bound in (14) is uniform in the sense that it depends on the length N of the discrete-time window but not on the discrete-time instant k.

The stability properties of the HCMCI algorithm under DoS will now be derived on the basis of the preliminary results reported above, and further relying on the following observability assumption.

A2. For any $i \in \mathcal{N}$, there exists γ^i such that the sensor nodes belonging to $\mathcal{N}^i(\gamma^i)$ ensure observability of the system state x_k, i.e., such that the pair $(A, C^i(\gamma^i))$ is observable, where $C^i(\gamma^i)$ is the matrix obtained by row-juxtaposition of the matrices C^j for $j \in \mathcal{N}^i(\gamma^i) \cap \mathcal{S}$.

We can now prove the following result.

Theorem 1: Let Assumptions A1-A2 and design condition DC hold, and let the HCMCI algorithm be adopted with weights as in (12). Further, for any $i \in \mathcal{N}$, let the algorithm be initialized with a positive definite information matrix $\Omega^i_{0|-1} > 0$ and the weights ω^i_k be chosen so that $0 < \underline{\omega} \leq \omega^i_k \leq \overline{\omega}$, $\forall k \in \mathbb{N}$, for some positive scalars $\underline{\omega}$ and $\overline{\omega}$. Then, there exist positive definite matrices $\underline{\Omega}$, $\overline{\Omega}$, $\underline{\Omega}^*$, $\overline{\Omega}^*$ and a discrete-time instant $\bar{k}$ such that, for any DoS signal satisfying (10), the following bounds hold for every $i \in \mathcal{N}$:

(i) $\Omega^i_{k|k} \leq \overline{\Omega}$ and $\Omega^i_{k+1|k} \leq \overline{\Omega}^*$, $\forall k \in \mathbb{N}$;
(ii) $\Omega^i_{k|k} \geq \underline{\Omega}$ and $\Omega^i_{k+1|k} \geq \underline{\Omega}^*$, $\forall k \geq \bar{k}$.

Proof: (i) For the proof of fact (i), it is convenient to resort to the following equivalent expression for the computation of the predicted information matrix $\Omega^i_{k+1|k}$:

$$\Omega^i_{k+1|k} = W - WA\left(\Omega^i_{k|k} + A^\top W A\right)^{-1} A^\top W . \tag{15}$$

Thus, if we define $\overline{\Omega}^* \triangleq W$, we can note that $\Omega^i_{k+1|k} \leq \overline{\Omega}^*$, $\forall k \in \mathbb{N}$. Further, we note that the explicit expression for $\Omega^i_{k|k}$ obtained from the consensus and correction steps of the HCMCI algorithm is as follows:

$$\begin{aligned} \Omega^i_{k|k} = & \sum_{j\in\mathcal{N}} (\Pi|^k_k)_{i,j} \Omega^j_{k|k-1} \\ & + \omega^i_k \sum_{j\in\mathcal{S}} (\Pi|^k_k)_{i,j} (C^j)^\top V^j C^j . \end{aligned} \tag{16}$$

Thus, recalling the choice of the consensus weights in (12) and the property (5), we have

$$\Omega^i_{k|k} \leq \overline{\Omega}^* + \overline{\omega} \sum_{j\in\mathcal{S}} (C^j)^\top V^j C^j . \tag{17}$$

Since the matrices C^j and V^j are time-invariant for any $j \in \mathcal{S}$, we can define $\overline{\Omega} \triangleq \overline{\Omega}^* + \overline{\omega} \sum_{j\in\mathcal{S}} (C^j)^\top V^j C^j$.

(ii) Note that the computation of $\Omega^i_{k|k}$ in (16) can be equivalently written as

$$\begin{aligned} \Omega^i_{k|k} = & \sum_{j\in\mathcal{N}} (\Pi|^k_k)_{i,j} \Psi(\Omega^j_{k-1|k-1}) \\ & + \omega^i_k \sum_{j\in\mathcal{S}} (\Pi|^k_k)_{i,j} (C^j)^\top V^j C^j . \end{aligned} \tag{18}$$

where $\Psi(\Omega) \triangleq A^{-\top}\Omega A^{-1} - A^{-\top}\Omega(\Omega + A^{\top}WA)^{-1}\Omega A^{-1}$. Since we have proved (see fact (i) above) that the matrices $\Omega^i_{k|k}$ are uniformly upper-bounded by a constant matrix $\overline{\Omega}$, we can exploit Lemma 1, fact (ii) of [4] and obtain

$$\begin{aligned}\Omega^i_{k|k} \geq \quad & \sum_{j\in\mathcal{N}} (\Pi|^k_k)_{i,j}\, \check{\beta}\, A^{-\top}\Omega^j_{k-1|k-1}A^{-1} \\ & + \omega^i_k \sum_{j\in\mathcal{S}} (\Pi|^k_k)_{i,j} (C^j)^{\top} V^j C^j \,.\end{aligned} \tag{19}$$

for some $\check{\beta} > 0$.

Then, the proof proceeds as follows. Equation (18) can be iteratively applied and lower-bounded as in (19) for N times. By choosing N so that $L(N+1) \geq \bar{\gamma}\Theta$, where $\bar{\gamma} = \max_{i\in\mathcal{N}} \gamma^i$ (recall Assumption A2), we can exploit Lemma 2 and obtain the lower bound

$$\Omega^i_{k|k} \geq \check{\beta}^N (A^{-N})^{\top} \varepsilon \left(\sum_{j\in\mathcal{N}^i(\bar{\gamma})} \Omega^j_{k-N|k-N} \right) A^{-N} \,, \tag{20}$$

where we have used the fact that $\omega^i_k \geq 0$, $\forall i \in \mathcal{N}$, $\forall k \in \mathbb{N}$.

Let

$$\Xi^i_{k-N|k-N} \triangleq \left(\sum_{j\in\mathcal{N}^i(\bar{\gamma})} \Omega^j_{k-N|k-N} \right). \tag{21}$$

Note that each term in (21) can be expressed in the form given in (18); then, by applying the same recursion as above over the discrete-time interval $[k-N-n+1, \;\; k-N]$, where n is the dimension of the state x_k, and further considering only the information related to node j itself, it is possible to write

$$\begin{aligned}\Omega^j_{k-N|k-N} \quad & \geq \underline{\omega}\, \varepsilon \, \big[(C^j)^{\top} V^j C^j \\ & + \check{\beta}\, A^{-\top} (C^j)^{\top} V^j C^j A^{-1} + \cdots \\ & + \check{\beta}^{n-1} \, (A^{-n+1})^{\top} (C^j)^{\top} V^j C^j A^{-n+1} \big] \,.\end{aligned} \tag{22}$$

Since by Assumption A2 the nodes in $\mathcal{N}^i(\bar{\gamma}) \cap \mathcal{S}$ ensure observability, it follows that $\Xi^i_{k-N|k-N}$ is strictly positive definite, i.e. there exists a matrix $\Xi > 0$ such that $\Xi^i_{k-N|k-N} \geq \Xi$. In particular, for each node i one can compute a lower bound Ξ_i from (21) by replacing each matrix $\Omega^j_{k-N|k-N}$ with the corresponding lower bound in (22). Then Ξ can be simply taken as $\hat{\xi}\, I$, with $\hat{\xi}$ the minimum among the eigenvalues of the matrices Ξ_i, $i \in \mathcal{N}$. Thus, the proof of fact (ii) can be concluded by setting $\underline{\Omega} \triangleq \varepsilon\, \check{\beta}^N \, (A^{-N})^{\top} \Xi A^{-N}$ and $\bar{k} > n + N$ with N such that $L(N+1) \geq \bar{\gamma}\Theta$; further, we can set $\underline{\Omega}^* = \Psi(\underline{\Omega})$. ■

Notice that the information matrices $\Omega^i_{k|k}$ and $\Omega^i_{k+1|k}$ involved in the above theorem are fully deterministic, in the linear setting of this paper, since they do not depend on measurements. This is well known in the context of linear Kalman filtering and is not affected by the consensus among different local Kalman filters. Hence, the bounds on the information matrices in Theorem 1 hold deterministically and the subsequent stability analysis based on Lyapunov function arguments and exploiting such bounds is, unlike probabilistic-type analyses like that of [22], a deterministic (worst-case) one.

We can now prove that the HCMCI DSE algorithm preserves its stability properties even in the presence of DoS attacks provided that transmissions are performed periodically (recall design condition DC) and are frequent enough (recall condition (10) of Lemma 1). To this end, let $e^i_k = x_k - \hat{x}^i_{k|k-1}$ denote the estimation error in node i. Further, consider the collective estimation error $e_k = \mathrm{col}(e^i_k, i \in \mathcal{N})$ and the collective noise vector $v^i_k = \mathrm{col}(v^i_k, i \in \mathcal{S})$. Then, the following can be asserted.

Theorem 2: Let the same assumptions as in Theorem 1 hold. Then, the dynamics of the collective estimation error is exponentially input-to-state stable, i.e., there exists positive scalars $\beta < 1$, c_1, c_2, and c_3 such that, for $k \geq \bar{k}$,

$$\begin{aligned}\|e_k\| \leq \quad & c_1\, \beta^{(k-\bar{k})/2} \, \|e_0\| + c_2 \, \max_{0\leq\tau\leq k-1} \|w_\tau\| \\ & + c_3 \, \max_{0\leq\tau\leq k} \|v_\tau\| \,,\end{aligned} \tag{23}$$

where $\|\cdot\|$ denotes the Euclidean norm.

Proof: In [1] it is shown that, in the case of perfect communication, the collective estimation error dynamics can be written as a linear time-varying system (see Proposition 1 of [1]). It is an easy matter to see that the same result holds also in the the presence of DoS attacks (the only difference being that the consensus weights are time-varying). Specifically, we have

$$e_{k+1} = \Phi_k e_k + \Gamma_k v_k + w_k \tag{24}$$

for suitable matrices Φ_k and Γ_k (see [1] for details), which, in view of Theorem 1, are uniformly bounded over time.

We show now that, in the noise-free case, the collective estimation error dynamics is exponentially stable. To this end, suppose that $w_k = 0$ and $v^i_k = 0$, $i \in \mathcal{S}$, for any $k \in \mathbb{N}$. Consider now the time-varying quadratic Lyapunov functions

$$\mathcal{L}^i_k(e^i_k) \triangleq (e^i_k)^{\top} \Omega^i_{k|k-1} e^i_k \,, \quad i \in \mathcal{N} \,, \tag{25}$$

and define the vector

$$\mathcal{L}_k(e_k) = \mathrm{col}\left(\mathcal{L}^i_k(e^i_k), i \in \mathcal{N} \right) . \tag{26}$$

Proceeding as in the proof of Theorem 5 of [4], it is possible to show that there exists a positive scalar $\beta < 1$ such that

$$\mathcal{L}_{k+1}(e_{k+1}) \leq \beta\, \Pi|^k_k \, \mathcal{L}_k(e_k) \tag{27}$$

for any $k \geq \bar{k}$ (with $\bar{k}$ the same as in Theorem 1). As a consequence, we have

$$\mathcal{L}_k(e_k) \leq \beta^N \, \Pi|^k_{k-N+1} \, \mathcal{L}_{k-N}(e_{k-N}) \tag{28}$$

for any $k - N \geq \bar{k}$ and any $N \geq 1$. Since $\Pi|^k_{k-N+1}$ is a row-stochastic matrix, it follows that its induced ∞-norm is equal to 1. This implies that the induced 2-norm of the matrix $\Pi|^k_{k-N+1}$ can be bounded as $\|\Pi|^k_{k-N+1}\|_2 \leq \sqrt{|\mathcal{N}|}\, \|\Pi|^k_{k-N+1}\|_\infty = \sqrt{|\mathcal{N}|}$. Therefore, from (28), we have

$$\|\mathcal{L}_k(e_k)\| \leq \beta^N \sqrt{|\mathcal{N}|}\, \|\mathcal{L}_{k-N}(e_{k-N})\| \,. \tag{29}$$

Notice now that, in view of Theorem 1, we have

$$\underline{\lambda}\, \|e^i_k\|^2 \leq |\mathcal{L}^i_k(e^i_k)| \leq \overline{\lambda}\, \|e^i_k\|^2 \tag{30}$$

where $\underline{\lambda} > 0$ is the minimum eigenvalue of $\underline{\Omega}^*$ and $\overline{\lambda} > 0$ the maximum eigenvalue of $\overline{\Omega}^*$. Focusing on the upper bound in (30), we obtain

$$\begin{aligned}\|\mathcal{L}_k(e_k)\| \quad & = \quad \sqrt{\sum_{i\in\mathcal{N}} \mathcal{L}^i_k(e^i_k)^2} \\ & \leq \quad \sqrt{\sum_{i\in\mathcal{N}} \overline{\lambda}^2 \|e^i_k\|^4} \leq \sum_{i\in\mathcal{N}} \overline{\lambda}\, \|e^i_k\|^2 = \overline{\lambda} \|e_k\|^2 \,.\end{aligned} \tag{31}$$

Considering instead the lower bound in (30), we obtain

$$\begin{aligned}\|\mathcal{L}_k(e_k)\| \quad & = \quad \sqrt{\sum_{i\in\mathcal{N}} \mathcal{L}^i_k(e^i_k)^2} \\ & \geq \quad \sqrt{\sum_{i\in\mathcal{N}} \underline{\lambda}^2 \|e^i_k\|^4} \geq \sqrt{\frac{\underline{\lambda}^2}{|\mathcal{N}|} \left(\sum_{i\in\mathcal{N}} \|e^i_k\|^2 \right)^2} \qquad (32) \\ & = \quad \sum_{i\in\mathcal{N}} \frac{\underline{\lambda}}{\sqrt{|\mathcal{N}|}} \|e^i_k\|^2 = \frac{\underline{\lambda}}{\sqrt{|\mathcal{N}|}} \|e_k\|^2 \,. \qquad (33)\end{aligned}$$

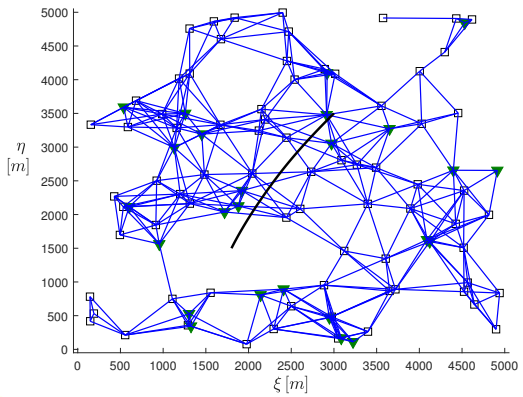

Fig. 2: Scenario 1. Network composed of 25 linear sensors (triangles) and 75 communication nodes (squares), and target trajectory (black line).

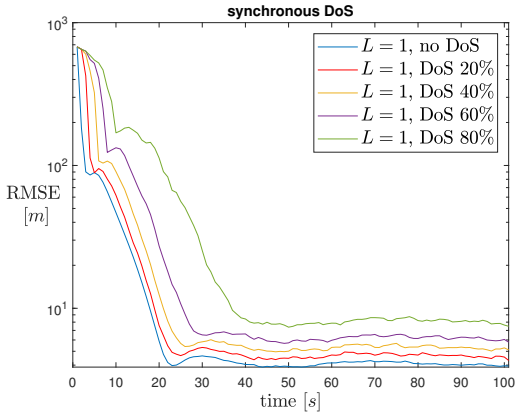

Fig. 3: Scenario 1. RMSE obtained with $L = 1$, in perfect communication conditions (no DoS) and under different percentage values of DoS occurrence (synchronous case).

Then, (29) implies

$$\|e_k\|^2 \leq \frac{\overline{\lambda}\,|\mathcal{N}|}{\underline{\lambda}}\beta^N \|e_{k-N}\|^2\,, \tag{34}$$

from which we obtain

$$\|e_k\| \leq \bar{c}_1\,\beta^{N/2}\,\|e_{k-N}\| \tag{35}$$

where $\bar{c}_1 = \sqrt{|\mathcal{N}|\,\overline{\lambda}/\underline{\lambda}}$. While the above bound holds only for $k - N \geq \bar{k}$, we can observe that, for a fixed $\bar{k}$, we can always write $\|e_{\bar{k}}\| \leq \tilde{c}_1\|e_0\|$ for some constant $\tilde{c}_1$. Hence, the noise-free collective estimation error dynamics is (uniformly) exponentially stable.

The proof can now be concluded by recalling that, for a discrete-time time-varying linear system with bounded matrices, uniform exponential stability in the absence of inputs implies input-to-state stability. ■

From Theorem 2 it is possible to assert that, under the considered assumptions, the estimation error is bounded in each network node if noises and disturbances are bounded, and goes to zero if noises and disturbances are zero. In the case of perfect communication, stability of the estimation error is ensured for any number of consensus steps (even $L = 1$). Conversely, in the presence of DoS attacks following the deterministic model of Assumption A1, stability is conditioned on the fact that the number of consensus steps is large enough so that condition (10) can be satisfied. As an alternative interpretation, condition (10) provides a measure of the robustness of the HCMCI DSE algorithms to DoS attacks. In fact, for a given number L of consensus steps, from condition (10) it is possible to know the maximum level of DoS, in terms of T and τ_D, for which stability of the estimation error is preserved.

V. SIMULATION RESULTS

The stability analysis of the previous section is validated through simulations carried out in a target-tracking framework. Specifically, the target motion is modeled by means of a white noise acceleration model of the form (3) with state transition matrix A as defined in [30]. The sampling interval Δ is $1\,s$. The elements of the unknown target state vector are the position and velocity components along the Cartesian coordinate axes ξ and η. The signal w_k is a white noise with zero mean and covariance matrix as defined in [30]. We address the DSE problem under the possible presence of DoS in two different scenarios.

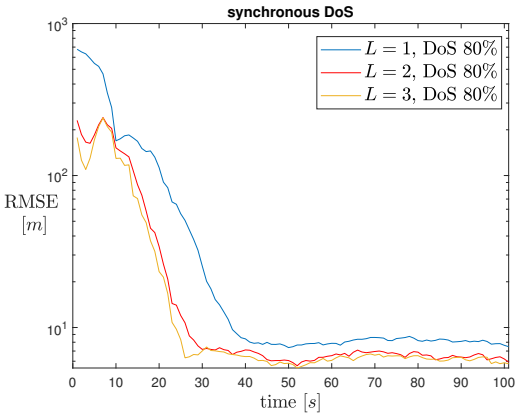

Fig. 4: Scenario 1. RMSE obtained with $L = 1$, $L = 2$, and $L = 3$, respectively, under 80% occurrence of synchronous DoS.

Scenario 1. We consider a network composed of 25 linear sensors and 75 communication nodes deployed in a square region having $5000\,m$ side length. Fig. 2 shows the considered network along with the target trajectory over the simulation time. For any node i, the set $\mathcal{N}^i$ is defined by all the nodes whose distance from i is less than a communication radius equal to $858\,m$. The sensor nodes provide measurements in Cartesian coordinates as

$$y_k^i = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} x_k + v_k^i\,, \tag{36}$$

with the measurement noise v_k^i having standard deviation of each component equal to $10\,m$. The HCMCI Algorithm is adopted with

DoS occurrence	$\tau_D\,[s]$	T
20%	5.9412	4.5909
40%	5.9412	2.5250
60%	5.9412	1.6833
80%	5.6111	1.2317

TABLE II: Scenario 1. DoS parameters τ_D and T corresponding to one of the Monte Carlo trials.

the weights used in the correction step set to $\omega_k^i = 1, \forall i \in \mathcal{N}$. The consensus weights $\pi^{i,j}$ are uniform and rescaled in accordance with (12). We perform Monte Carlo simulations with 150 runs

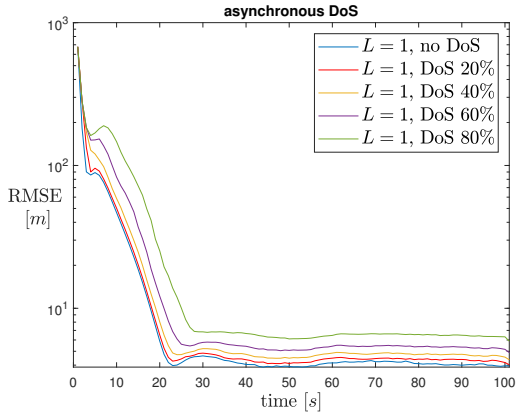

Fig. 5: Scenario 1. RMSE obtained with $L = 1$, in perfect communication conditions (no DoS) and under different percentage values of DoS acting independently on each link (asynchronous case).

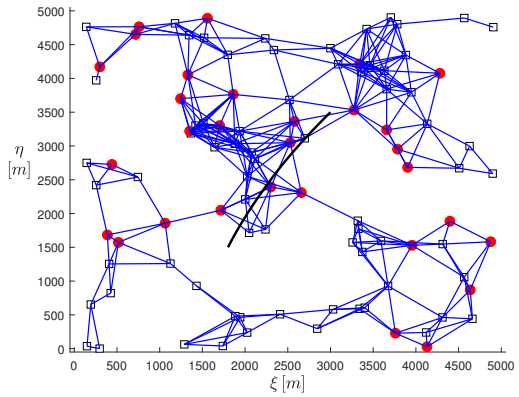

Fig. 7: Scenario 2. Network composed of 30 TOA sensors (circles) and 70 communication nodes (squares), and target trajectory (black line).

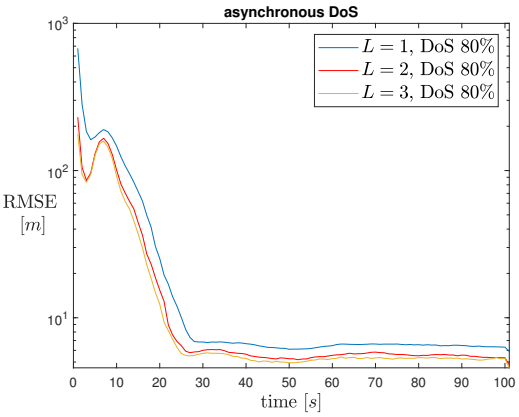

Fig. 6: Scenario 1. RMSE obtained with $L = 1$, $L = 2$, and $L = 3$, respectively, under 80% occurrence of asynchronous DoS.

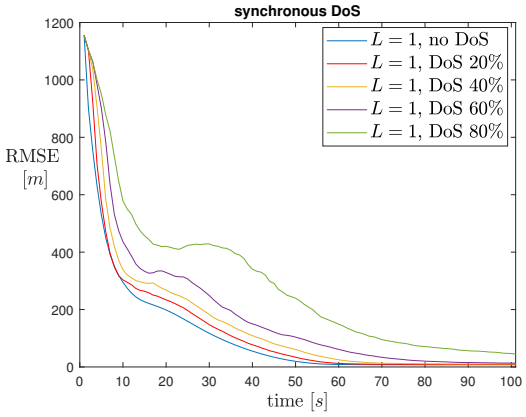

Fig. 8: Scenario 2. RMSE obtained with $L = 1$, in perfect communication conditions (no DoS) and under different percentage values of DoS occurrence (synchronous case).

obtained by varying the measurement noise realizations, as well as the DoS signal, and consider both synchronous and asynchronous DoS attacks. Fig. 3 shows the evolution of the Root Mean Square Error (RMSE) obtained with $L = 1$, both in perfect communication conditions and under different percentage values of DoS occurrence in the case of synchronous DoS. In particular, Table II reports the parameters τ_D and T corresponding to a Monte Carlo trial randomly selected from those considered in Fig. 3. The values of τ_D and T in Table II have been computed *a-posteriori* consistently with the actual DoS pattern affecting the network in the considered Monte Carlo trial. Note that these values are consistent with the fact that the quantity $\Delta/(\tau_D L) + 1/T$ is an upper bound for the average percentage of DoS occurrence (see [8, Section 2.3]). Fig. 4 shows the results obtained in correspondence to 80% of DoS occurrence under different values of L. As expected, we observe a performance improvement as the number L of consensus steps gets larger, which corresponds to more information exchanges among the network nodes. Figs. 5 and 6 report simulation results in the case of asynchronous DoS. The difference in the RMSE between the synchronous case and the asynchronous case can be appreciated in terms of speed of convergence and steady-state performance. Specifically, synchronous DoS is associated to lower performance as it affects all the network links simultaneously, whereas, under asynchronous DoS, communication failures involving some network links do not prevent other links from transmitting data. Further, as expected, such difference is more evident the larger the percentage of DoS occurrence.

Scenario 2. In order to further show the relevance of our study, we consider a network composed of 30 Time-of-Arrival (TOA) nonlinear sensors and 70 communication nodes, deployed in the same square region as in Scenario 1 (see Fig. 7). Each sensor measures the relative distance between itself and the target according to the equation

$$y_k^i = \sqrt{(\xi_k - \xi^i)^2 + (\eta_k - \eta^i)^2} + v_k^i\,, \tag{37}$$

where (ξ^i, η^i) represents the sensor position. The standard deviation of the measurement noise v_k^i is $10\,m$. The communication radius is $790\,m$. To deal with nonlinear sensors, within the HCMCI algorithm each local Kalman filter is replaced by an Unscented Kalman filter [31]. The results shown in Figs. 8 and 9 are in line with those obtained in the first scenario.

VI. CONCLUSIONS

The stability properties of state-of-the-art DSE algorithms based on consensus have been analyzed when DoS attacks can compromise communication between the network nodes. In particular, a quantification of the robustness of such algorithms to DoS attacks has been provided, specifically in terms of DoS frequency and duration for

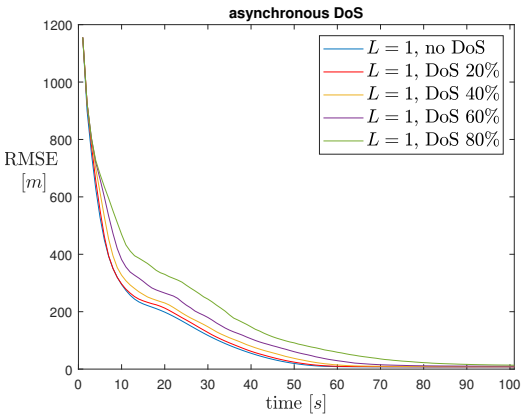

Fig. 9: Scenario 2. RMSE obtained with $L = 1$, in perfect communication conditions (no DoS) and under different percentage values of DoS occurrence (asynchronous case).

which it is ensured that stability of the estimation error dynamics is not destroyed. Simulations carried out on a target tracking case study have confirmed the theoretical analysis. The topic addressed in this paper could pave the way for interesting future investigations. For example, nonlinear settings like the one considered in [1] could be explored under DoS. Another research direction could consist in extending the analysis to the case of data-driven (event-triggered) communication [32]. This latter direction is particularly challenging, as the interaction between DoS and stability is more complex when communication is non-periodic than in the periodic case [33].

REFERENCES

[1] G. Battistelli, L. Chisci, G. Mugnai, A. Farina, and A. Graziano, "Consensus-based linear and nonlinear filtering," *IEEE Transactions on Automatic Control*, vol. 60, no. 5, pp. 1410–1415, 2015.

[2] A.T. Kamal, J.A. Farrell and A.K. Roy-Chowdhury, "Information weighted consensus filters and their application in distributed camera networks", *IEEE Transactions on Automatic Control*, vol. 58, no. 12, pp. 3112–3125, 2013.

[3] S. Wang, W. Ren, "On the convergence conditions of distributed dynamic state estimation using sensor networks: a unified framework," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 4, pp. 1300–1316, 2018.

[4] G. Battistelli and L. Chisci, "Kullback-Leibler average, consensus on probability densities, and distributed state estimation with guaranteed stability", *Automatica*, vol. 50, no. 3, pp. 707–718, 2014.

[5] D. Senejohnny, P. Tesi, and C. De Persis, "A jamming-resilient algorithm for self-triggered network coordination," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 981-990, 2018.

[6] S. Amin, A.A. Cárdenas, and S.S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in Majumdar, R., and Tabuada, P. (Eds.), *Hybrid systems: computation and control*, Lecture Notes in Computer Science, Springer, pp. 31–45, 2009.

[7] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[8] S. Feng and P. Tesi, "Resilient control under denial-of-service: robust design," *Automatica*, vol. 79, pp. 42–51, 2017.

[9] N. Zhao, P. Shi, and W. Xing, "Dynamic event-triggered approach for networked control systems under denial of service attacks," *International Journal of Robust and Nonlinear Control*, vol. 31, no. 5, pp. 1774-1795, 2021.

[10] H. Liu, and Z. Wang, "Sampled-data-based consensus of multi-agent systems under asynchronous denial-of-service attacks," *Nonlinear Analysis: Hybrid Systems*, vol. 39, 100969, 2021.

[11] C. Deng, and C. Wen, "Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and DoS attacks," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 3, pp. 1308-1318, 2020.

[12] C. Peng, and H. Sun, "Switching-like event-triggered control for networked control systems under malicious denial of service attacks," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3943–3949, 2020.

[13] R. Kato, A. Cetinkaya, and H. Ishii, "Stabilization of nonlinear networked control systems under denial-of-service attacks: a linearization approach," *2019 American Control Conference*, Philadelphia, PA, USA, 2019.

[14] H. Yang, Y. Li, L. Dai, and Y. Xia, "MPC-based defense strategy for distributed networked control systems under DoS attacks," *Systems & Control Letters*, vol. 128, pp. 9-18, 2019.

[15] Y.-C. Sun, and G.-H. Yang, "Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks," *International Journal of Robust and Nonlinear Control*, vol. 29, no. 14, pp. 4797-4811, 2019.

[16] A. Cetinkaya, H. Ishii, and T. Hayakawa, "A probabilistic characterization of random and malicious communication failures in multi-hop networked control," *SIAM Journal on Control and Optimization*, vol. 56, no. 5, pp. 3320-3350, 2018.

[17] A Cetinkaya, H Ishii, and T Hayakawa, "Networked control under random and malicious packet losses," *IEEE Transactions on Automatic Control* vol. 62, no. 5, pp. 2434-2449, 2017.

[18] 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, 2020.

[19] Y. Zacchia Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: an automatic control perspective," *Journal of Systems and Software*, vol. 149, pp. 174-216, 2019.

[20] A Cetinkaya, H Ishii, and T Hayakawa, "An overview on denial-of-service attacks in control systems: attack models and security analyses," *Entropy*, vol. 21, no. 2, 2019.

[21] C. De Persis and P. Tesi, "Resilient control under denial-of-service: results and research directions," in R.M.G. Ferrari, and A.M.H. Teixeira Eds., *Safety, Security and Privacy for Cyber-Physical Systems*, Lecture Notes in Control and Information Sciences, Springer International Publishing, 2021.

[22] Q. Liu, Z. Wang, X. He, and D.H. Zhou, "On Kalman-consensus filtering with random link failures over sensor networks," *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2701–2708, 2018.

[23] L. Anantharamu, B.S. Chlebus, D.R. Kowalski, and M.A. Rokicki, "Medium access control for adversarial channels with jamming," *Proc. 18th International Colloquium on Structural Information and Communication Complexity (SIROCCO)*, 2011.

[24] G. Battistelli, L. Chisci, D. Selvi, and P. Tesi, "Distributed state estimation under denial of service," *Proceedings of the 2019 IEEE 58th Conference on Decision and Control (CDC)*, Nice, France, 2019.

[25] G. Li, W. Yi, S. Li, B. Wang, and L. Kong, "Asynchronous multi-rate multi-sensor fusion based on random finite set," *Signal Processing*, vol. 160, pp. 113-126, 2019.

[26] L. Xiao, S. Boyd and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus", *Proc. 4th Int. Symposium on Information Processing in Sensor Networks*, pp. 63–70, 2005.

[27] 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.

[28] D.J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," *Proceedings of the 2006 IEEE Conference on Military Communications*, Washington, DC, USA, 2006.

[29] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2005.

[30] Y. Bar-Shalom, X. Rong Li, T. Kirubarajan, "Estimation with applications to tracking and navigation," *John Wiley & Sons,*, 2001.

[31] S.J. Julier and J.K. Uhlmann, "Unscented filtering and nonlinear estimation," *Proceedings of the IEEE*, vol. 92, no. 3, pp. 401-422, 2004.

[32] G. Battistelli, L. Chisci, and D. Selvi, "A distributed Kalman filter with event-triggered communication and guaranteed stability," *Automatica*, vol. 93, pp. 75-82, 2018.

[33] V.S. Dolk, P. Tesi, C. De Persis, and W.P.M.H. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93-105, 2017.