Optimal State Estimation Synthesis over Unreliable Network in Presence of Denial-of-Service Attack: an Operator Framework Approach

Mohammad Naghnaeian

Abstract—In this paper, we consider the problem of state-estimation in the presence of Denial-of-Service (DoS) attack. We formulate this problem as an state estimation problem for a plant with switching measured outputs. In the absence of attack, the state-estimator has access to all measured outputs, however, in the presence of attack, only a subset of all measurements are made available to the state-estimator. We seek to find an state-estimator that results in the minimum estimation error for the worst-case attack strategy. First, we parameterize the set of all state-estimators that result in stable estimation error for the worst-case attack scenario. Then, we will show that any state-estimator in this set can be written as a generalized Luenberger observer with an appropriately defined observer-gain. This observer-gain, in general, can be an operator and possibly unbounded as opposed to the classical static observer-gain. Furthermore, we will show that finding the optimal state-estimator that results in the minimum estimation error can be cast as a convex program over the set of stable factors of the observer operator-gain. This optimization in, in fact, linear programming and tractable.

I. INTRODUCTION

Modern cyber-physical systems (CPS) typically consist of many smaller components that are spread over a large spatial domain. The performance of the system, in whole, depends on the synergistic integration of computational components such as control or estimation algorithm and physical components such as actuators or sensors. Connectivity to the outside world and the critical nature of CPS has made such systems hot targets for adversarial attacks, see e.g. [1] and [2]. Denial-of-Service attack is an adversarial attack in which the attacker disrupts the exchange of the information [3]. In the control theoretic context, the disrupted information could be sensor measurements or control inputs to the actuators. In this paper, we seek to design state-estimators that are resilient with respect to the DoS attacks on the measurement channels. Such a problem has been given some attention in the literature, e.g., in [4], [5], and [6]. Most of the existing results aims at optimizing a cost-function, which is a measure of estimation error, over a finite horizon in the stochastic/probabilistic framework where a distribution form for the attacker or transmitter is assumed. In this paper, however, we address this problem in the deterministic framework and infinite horizon objective.

Our perspective is to think of a DoS attack as a switch and model the system as a Linear Switching System (LSS). The attacker’s strategy is to choose the switching to maximize the estimation error and possibly destabilize that while having a complete knowledge about system. On the other hand, the state-estimator’s strategy is to minimize the estimation error based on the available sensor measurements as well as the current and past actions of the attacker. We first, parametrize the set of all state-estimators that result in bounded estimation error. We refer to such state-estimators as stable estimators. Then we will define a new class of state observers mimicking the conventional Luenberger observers. We will refer to this new class as generalized Luenberger observers. A generalized Luenberger observer, in form, is very similar to a classical Luenberger observer with a significant difference that its observer gain is an operator, and possibly an unstable one, as opposed to a static gain in the classical observer. By allowing the Luenberger observer to have an operator-gain, we will show that the set of generalized Luenberger observers capture all stable state-estimators. This, by itself, is a new result to the best of our knowledge. Then, in order to find the optimal observer resulting in the minimum estimation error, we formulate the problem as a convex optimization over the stable factors of the observer operator-gains. These factors, and the resulting observer operator-gain, are switching operators that causally depend on the switching sequence (attacker’s strategy). Finding the optimal state-estimator, in fact, can be cast as a linear program and hence is tractable.

Our approach relies on utilizing the operator framework which was first introduced and developed in [7] and [8]. This operator framework provides a powerful tool to study any type of linear system, time invariant, time varying, delayed, switching, etc., in a unified way. Recently, the author has used such a framework for the synthesis of decentralized controllers [9]. In what follows, we first review some results on the switching systems and then present our results on optimal state-estimator design subject to DoS.

II. PRELIMINARIES

A. Generic Notation

We use $\mathbb{R}^n$ for the set of vectors of real numbers of dimension $n$. Given $x = \{x(k)\}_{k=1}^n \in \mathbb{R}^n$, its $l_\infty$ norm is defined as $\|x\| = \max_{k \in \{0,1,\ldots,n-1\}} |x(k)|$. For a (infinite dimensional) sequence $x = \{x(k)\}_{k=0}^\infty$ with $x(k) \in \mathbb{R}^n$, the $l_\infty$ norm is defined by $\|x\| = \sup_k \|x(k)\|$ whenever finite. The space of
sequences with elements in $\mathbb{R}^n$ whose $l_\infty$ norm is bounded is denoted by $l^\infty$. Throughout this paper, we view linear systems as mapping on the space of $l^\infty$ for some positive integer $n$. In general, for two normed spaces $(X, \|\cdot\|_X)$ and $(Y, \|\cdot\|_Y)$ and a linear operator $R : X \to Y$, the induced norm of this operator is given by $\|R\|_{X \to Y} := \sup_{x \neq 0} \frac{\|Rx\|_Y}{\|x\|_X}$. The operator $R$ is said to be bounded if its induced norm is finite. In this paper, we typically have $X = l^\infty$ and $Y = l^\infty$, for some positive integers $n$ and $m$, and we simply write $\|R\|$ to denote the $l^\infty$ to $l^\infty$ induced norm of the operator $R$. Any linear causal operator $R$ can be thought of as an infinite dimensional lower triangular matrix,

$$
R = \begin{bmatrix}
R_{0,0} & 0 & 0 & \cdots \\
R_{1,0} & R_{1,1} & 0 & \cdots \\
R_{2,0} & R_{2,1} & R_{2,2} & \cdots \\
\vdots & \vdots & \vdots & \ddots
\end{bmatrix}.
$$

**Definition 1:** A causal operator $R$ given by (1), is said to be bounded or stable (on the space of $l^\infty$ sequences) if

$$
\sup_k \left\| \begin{bmatrix} R_{0,0} & R_{1,0} & R_{2,0} & \cdots \\
R_{1,1} & R_{1,0} & \cdots \\
R_{2,2} & R_{2,1} & R_{2,0} & \cdots \\
\vdots & \vdots & \vdots & \ddots
\end{bmatrix} \right\| < \infty.
$$

Given a sequence $x = \{x(k)\}^\infty_{k=0}$, the delay or shift operator $\Lambda$ is defined by

$$
\Lambda^k x = \begin{cases}
0, & \text{if } k \neq 0 \\
x(0), x(1), \ldots, x(k) & \text{if } k = 0
\end{cases}.
$$

**Definition 2:** A linear causal map $R$ is called time-invariant if $\Lambda R = K \Lambda$.

A Linear Time-Invariant (LTI) operator $R$ is fully characterized by its impulse response denoted by $\{R(k)\}^\infty_{k=0}$ and its infinite dimensional matrix representation is given by

$$
R = \begin{bmatrix}
R(0) & 0 & 0 & \cdots \\
R(1) & R(0) & 0 & \cdots \\
R(2) & R(1) & R(0) & \cdots \\
\vdots & \vdots & \vdots & \ddots
\end{bmatrix}.
$$

A Linear Time-Varying (LTV) system $R$ can also be written in state-space representation as

$$
R : \begin{cases}
x(t+1) = A(t)x(t) + B(t)u(t) \\
y(t) = C(t)x(t) + D(t)u(t)
\end{cases},
$$

where $x(t) \in \mathbb{R}^m, y(t) \in \mathbb{R}^n, u(t) \in \mathbb{R}^p, x_0, y_0, u_0 \in \mathbb{R}^n$ are input, state, output, and the initial condition of the system and $A(\cdot), B(\cdot), C(\cdot),$ and $D(\cdot)$ are matrices with appropriate dimensions for all $t$. Throughout this paper, we think of linear systems as operators and hence we do not directly work with the state-space representation. We, rather, convert the state-space (2) to (1). To do so, given a sequence of matrices $\{A(k)\}^\infty_{k=0}$, we define $\tilde{A}$ to be the diagonal operator

$$
\tilde{A} = \begin{bmatrix}
A(0) & 0 & \cdots \\
0 & A(1) & \cdots \\
\vdots & \vdots & \ddots
\end{bmatrix}.
$$

Using this notation, we can define diagonal operators $\tilde{A}, \tilde{B}, \tilde{C},$ and $\tilde{D}$ and rewrite (2) as

$$
R : \begin{cases}
x(t+1) = \Lambda \tilde{A} x + \Lambda \tilde{B} w + \tilde{x}_0 \\
y(t) = \tilde{C} x + \tilde{D} w
\end{cases},
$$

where $\tilde{x}_0 = \{0,0,0,0,0,\ldots\}$, $x = \{x(t)\}_{t=0}^\infty$, $y = \{y(t)\}_{t=0}^\infty$, $w = \{w(t)\}_{t=0}^\infty$, and $\Lambda$ is the delay operator. The above representation of $R$ is referred to as the operator form.

**Definition 3:** System $R$ in (4) is said to be stable or bounded if it is a bounded operator from $\begin{pmatrix} \tilde{x}_0 \\ w \end{pmatrix}$ to $\begin{pmatrix} x \\ y \end{pmatrix}$. More precisely, $R$ is stable if there exists a non-negative real number $\gamma \geq 0$ such that $\max\{\|x\|, \|y\|\} \leq \gamma\max\{\|\tilde{x}_0\|, \|w\|\}$ for all $\tilde{x}_0, w \in l_\infty$.

**B. Linear Switched Systems**

In this section, we need to review some standard results on Linear Switched Systems (LSS) presented in [7] and [8]. A Linear Switched System, $P_\sigma$, can be represented in state-space by

$$
P_\sigma : \begin{cases}
x(t+1) = A_{\sigma(t)} x(t) + B_{\sigma(t)} u(t) \\
y(t) = C_{\sigma(t)} x(t) + D_{\sigma(t)} u(t)
\end{cases},
$$

where $\sigma = \{\sigma_k\}^\infty_{k=0}$ is called the switching sequence that takes values a finite set. Sometimes, $\sigma$ is restricted to be in the set of admissible switching sequences $\Sigma$. In the operator framework, (5) can be written as

$$
P_\sigma : \begin{cases}
x(t+1) = \Lambda \tilde{A}_\sigma x + \Lambda \tilde{B}_\sigma u + \tilde{x}_0 \\
y(t) = \tilde{C}_\sigma x + \tilde{D}_\sigma u
\end{cases},
$$

where $\tilde{A}_\sigma = \text{diag}(A_{\sigma_0}, A_{\sigma_1}, A_{\sigma_2}, \ldots)$ and $\tilde{B}_\sigma, \tilde{C}_\sigma,$ and $\tilde{D}_\sigma$ are defined analogously.

There are important sub-classes of LSS that are of interest in this paper. These are the LSS whose state matrices, $A$-matrices, remain constant and are defined below:

**Definition 4:** We say a LSS $P_\sigma$ is an input-output LSS of degree $M$, for some positive integer $M$, if it can be written, in state-space, as follows

$$
P_\sigma : \begin{cases}
x(t+1) = A_{\sigma(t)} x(t) + B_{\sigma(t)} u(t) \\
y(t) = C_{\{\sigma(k)\}^M}[t=M+1] x(t) + D_{\{\sigma(k)\}^M}[t=M+1] u(t)
\end{cases},
$$

We will denote the class of such systems by $\mathcal{S}_{IO}^M$ and $\mathcal{S}_{IO} = \bigcup_{M=1}^\infty \mathcal{S}_{IO}^M$.

We are also interested in a subclass of input-output LSS, output-only switching, as follows:

**Definition 5:** A LSS $P_\sigma$ is said to be an output-only LSS of degree $M$ if it admits the realization

$$
P_\sigma : \begin{cases}
x(t+1) = A_{\sigma(t)} x(t) + B u(t) \\
y(t) = C_{\{\sigma(k)\}^M}[t=M+1] x(t) + D_{\{\sigma(k)\}^M}[t=M+1] u(t)
\end{cases}.
The class of such systems is denoted by $\mathcal{S}_O$ and $\mathcal{S}_O = \bigcup_{M=1}^{\infty} \mathcal{S}_O^M$.

The classes of input-output and output-only LSS are rich classes since any stable LSS can be approximated by elements of $\mathcal{S}_O$ and $\mathcal{S}_IO$ with arbitrary accuracy.

**Lemma 6:** Let $P_\sigma$ be a stable LSS and $\epsilon > 0$. Then, there exist an integer $M$, $P_\sigma \in \mathcal{S}_IO^M$, and $\tilde{P}_\sigma \in \mathcal{S}_O^M$ such that
\[
\|P_\sigma - \tilde{P}_\sigma\| < \epsilon,
\]

\[
\|P_\sigma - \bar{P}_\sigma\| < \epsilon,
\]

for any switching sequence $\sigma$. Moreover, $\tilde{P}_\sigma$ and $\bar{P}_\sigma$ can be made FIR (Finite-Impulse-Response).

Furthermore, there exist tractable and exact expressions to calculate the $l_\infty$ induced norm of LSS. In [8], it is proved that the gain computation can be cast as a Linear Program. We do not review those results here but rather refer the reader to [8].

### III. Problem Setup

Consider a linear plant given by
\[
\begin{align*}
    x &= \Lambda \dot{x} + \Lambda \dot{w} + \bar{x}_0, \\
    y_i &= \bar{C}_i x + \bar{D}_i w,
\end{align*}
\]

where $x$ and $w$ are the states and exogenous disturbances, respectively, and $y_i$, for $i = 1, 2, \ldots, N$ for some integer $N$, are the measurements/observations from this system. In this paper, we address the problem of remote state-estimation where some of the measurements, $y_i$, might not be available to the state-estimator due to intermittent communication network or Denial-of-Service type of attack.

In the ideal nominal operating condition, when there is no DoS attack, the state-estimator receives all $y_i$. That is, available information to the state-estimator, $y_a$, is given by
\[
y_a^0 = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{bmatrix} = \begin{bmatrix} \bar{C}_1 \\ \bar{C}_2 \\ \vdots \\ \bar{C}_N \end{bmatrix} x + \begin{bmatrix} \bar{D}_1 \\ \bar{D}_2 \\ \vdots \\ \bar{D}_N \end{bmatrix} w. \tag{10}
\]

However, when a DoS attack occurs at the measurement channel, the state-estimator only receives a subset of measurements. In this case,
\[
y_a^\sigma(t) = E^{\sigma(t)} y_a^0(t), \tag{11}
\]

where $E^{\sigma(t)}$ is a block diagonal matrix with identity corresponding to $y_i$’s that are available to state-estimator and zero otherwise. In the above expression, $\sigma(.)$ is the switching signal orchestrating between modes of the system and take value in some finite set. We use the zeroth mode to denote the nominal mode. For a concrete example see below:

**Example 7:** Consider a system in Figure 1 where there are two measurements, $y_1$ and $y_2$. Suppose, the plant is unstable LTI given by
\[
\begin{align*}
    x(t+1) &= \begin{bmatrix} 1 & 0 & 1 \\ -1 & 1 & 1 \\ -1 & 0 & 2 \end{bmatrix} x(t), x(0) = \begin{bmatrix} 0.1 \\ 0.2 \\ -0.1 \end{bmatrix},
\end{align*}
\]

and the measurements are given by
\[
\begin{align*}
    y_1(t) &= \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} x(t) + w_1(t), \\
    y_2(t) &= \begin{bmatrix} 1 & -1 & -2 \end{bmatrix} x(t) + 0.01 w_2(t),
\end{align*}
\]

where $|w_i| \leq 1$, for $i = 1, 2$. In this example, $y_1$ is a reliable measurement but with higher level of disturbance and $y_2$ is an unreliable measurement with lower level of disturbance. The DoS type of attack may result in measurement $y_2$ to not reach the state-estimator. In this case, the available information, at each time instant, to the state-estimator, $y_a(t)$ is given by
\[
y_a^0(t) = \begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix},
\]

and
\[
E^{\sigma(t)} \in \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right\}.
\]

Therefore, $y_a^\sigma(t) = C^{\sigma(t)} x + D^{\sigma(t)} w$

\[
C^{\sigma(t)} \in \left\{ \begin{bmatrix} 0 & 1 & 0 \\ 1 & -1 & -2 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & -1 & -2 \end{bmatrix} \right\}, \tag{12}
\]

\[
D^{\sigma(t)} \in \left\{ \begin{bmatrix} 2 & 0 \\ 0 & 0.01 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} \right\}. \tag{13}
\]

Similarly to this example, we can rewrite (11) in the operator framework and combine with (9)-(10) to obtain the following plant and attack model:
\[
\begin{align*}
    x &= \Lambda \dot{x} + \Lambda \dot{w} + \bar{x}_0, \\
    y_a^\sigma &= \bar{C}^{\sigma} x + \bar{D}^{\sigma} w,
\end{align*}
\]

where the switching sequence $\sigma(.)$ is the attacker’s strategy; we use $\sigma(t) = 0$ to denote the nominal condition at time instant $t$. In this expression, $y_a^0$ is the sequence of available information to state-estimator and $\sigma$ belongs to the set of admissible sequences $\Sigma$. In the above example, $\Sigma$ is the set of binary sequences.
IV. MAIN RESULTS

A. Parametrization of State-Estimators

In this section, we are interested to parametrize the set of state-estimators. A state-estimator is a causal map, $T^\sigma$, from the available measurements, $y_a^\sigma$, to a signal $\hat{x}$ which is the estimation of state $x$. That is,

$$\hat{x} = T^\sigma y_a^\sigma. \quad (14)$$

In the above expression, the dependency of the state-estimator on $\sigma$ is made explicit. We emphasize that $\sigma(\cdot)$ is the attacker’s strategy which is causally known to the state-estimator. That is, the state-estimator, at any given time, does not know the attacker’s intention in future but know its current and past actions. Therefore, $T^\sigma$ only causally depends on $\sigma$. In fact, a generic LSS as given in (5) respects this causality. Henceforth, whenever an operator’s dependency on $\sigma$ is stated, causal dependency is assumed.

**Definition 8:** We say an state-estimator $\hat{x} = T^\sigma y_a^\sigma$ is stable if the estimation error $\tilde{x} := \hat{x} - x$ is a bounded signal.

In the sequel, we first parametrize the set of all stable state-estimators and then we will present our result on the synthesis of optimal state-estimator that is resilient to DoS attacks.

**Lemma 9:** The set of all stable state-estimators $\hat{x} = T^\sigma y_a^\sigma$ that result in a bounded estimation error is parametrized by bounded operators $T^\sigma$ and $X^\sigma$ such that

$$\begin{bmatrix} T^\sigma & X^\sigma \end{bmatrix} \begin{bmatrix} \bar{C}^\sigma \\ \bar{A} - I \end{bmatrix} = I, \text{ for all } \sigma \in \mathbb{S}. \quad (15)$$

In this case, the state-estimator and estimation error are given by (14) and

$$\tilde{x} = X^\sigma (\bar{A} w + \bar{x}_0).$$

**Proof:** Let the state-estimator given by (14). Then, the error is given by

$$\tilde{x} = T^\sigma (\bar{C}^\sigma x + \bar{D}^\sigma w) - x = (T^\sigma \bar{C}^\sigma - I) x + T^\sigma \bar{D}^\sigma w$$

$$\frac{\bar{C}^\sigma}{\bar{A} - I} (I - \bar{A})^{-1} ABw$$

$$+ T^\sigma \bar{D}^\sigma w + (T^\sigma \bar{C}^\sigma - I) (I - \bar{A})^{-1} \bar{x}_0.$$

Notice that $\tilde{x}$ is a bounded signal for bounded $w$, $\bar{x}_0$, and $\sigma \in \mathbb{S}$ if and only if the mappings $T^\sigma$ and $(T^\sigma \bar{C}^\sigma - I) (I - \bar{A})^{-1}$ are bounded. Define

$$X^\sigma := (T^\sigma \bar{C}^\sigma - I) (I - \bar{A})^{-1}.$$

Post-multiplying both sides by $(I - \bar{A})$, we obtain

$$X^\sigma (I - \bar{A}) = (T^\sigma \bar{C}^\sigma - I),$$

which is equivalent to (15) and this completes the proof. \(\blacksquare\)

Traditionally, the state-estimation has been carried out utilizing Luenberger observers. Luenberger observers, in their conventional shape, form a strict subset of all stable state-estimators parametrized above. In what follows, we introduce the Generalized Luenberger Observers that differ from conventional ones in that their observer gains are (possibly unstable) operators as opposed to static. A generalized Luenberger is of the form

$$\dot{x} = \bar{A} \bar{x} + L^\sigma (\bar{C}^\sigma \bar{x} - \bar{y}_a^\sigma), \quad (16)$$

where $\bar{x}$ is the estimation of the state, $L$ is the observer (possibly unbounded) operator-gain, and $y_a^\sigma$ is the available information to state-estimator.

**Theorem 10:** Any stable state-estimator can be written as in (16) for an appropriate $L^\sigma$ in the form

$$L^\sigma = (I + Q^\sigma)^{-1} Z^\sigma, \quad (17)$$

where $Q^\sigma$ and $Z^\sigma$ are stable operators satisfying

$$\sup_{\sigma \in \mathbb{S}} \left\{ \bar{A} \bar{x} + [ Z^\sigma Q^\sigma ] \begin{bmatrix} \bar{C}^\sigma \\ \bar{A} - I \end{bmatrix} \right\} = 0. \quad (18)$$

Conversely, any generalized Luenberger observer (16) with observer operator-gain $L$ in (17) is a state-stable if

$$\sup_{\sigma \in \mathbb{S}} \left\| \bar{A} \bar{x} + [ Z^\sigma Q^\sigma ] \begin{bmatrix} \bar{C}^\sigma \\ \bar{A} - I \end{bmatrix} \right\| < 1. \quad (19)$$

**Proof:** Suppose

$$\dot{x} = T^\sigma y_a^\sigma,$$

is a stable state-estimator for all $\sigma \in \mathbb{S}$. By Lemma 2, $T^\sigma$ must be bounded and there exists a bounded operator $X^\sigma$ such that (15) holds. Now, define $Z^\sigma$ and $Q^\sigma$ as follows:

$$Z^\sigma := -T^\sigma,$$

$$Q^\sigma := -I - X^\sigma.$$

Then, direct calculation verifies

$$\bar{A} \bar{x} + [ Z^\sigma Q^\sigma ] \begin{bmatrix} \bar{C}^\sigma \\ \bar{A} - I \end{bmatrix}$$

$$= \bar{A} \bar{x} + [ -T^\sigma -I - X^\sigma ] \begin{bmatrix} \bar{C}^\sigma \\ \bar{A} - I \end{bmatrix}$$

$$= \bar{A} \bar{x} - T \bar{C}^\sigma + I - \bar{A} - X^\sigma \bar{A} + X^\sigma$$

$$= -T \bar{C}^\sigma + I + X^\sigma (I - \bar{A}),$$

which implies (18) is satisfied. Therefore, any stable state-estimator can be written as a generalized Luenberger observer. It remains to show the converse. That is, any generalized Luenberger observer (16) with observer operator-gain (17) results in a stable state-estimator. Given a generalized Luenberger observer (16), its estimation error is given by

$$e = \dot{x} - x = \bar{A} \bar{x} + L^\sigma (\bar{C}^\sigma \bar{x} - \bar{y}_a^\sigma) - \bar{A} \bar{x} - \bar{A} \bar{B} \bar{w} - \bar{x}_0$$

$$= (\bar{A} \bar{A} + L^\sigma \bar{C}^\sigma) e - L^\sigma \bar{D}^\sigma \bar{w} - \bar{A} \bar{B} \bar{w} - \bar{x}_0. \quad (20)$$
Assuming (17)-(18), there exists a bounded operator \( \mathcal{E}^\sigma \) with \( \| \mathcal{E}^\sigma \| < 1 \) such that
\[
\mathcal{E}^\sigma = \Lambda \bar{\Lambda} + \begin{bmatrix} \begin{array}{c} \mathcal{C}^\sigma \\ \Lambda \bar{\Lambda} - I \end{array} \end{bmatrix} = (I + Q^\sigma) \Lambda \bar{\Lambda} + Z^\sigma - Q^\sigma.
\]
Using this expression in (20), we obtain
\[
e = -\{I - (\Lambda \bar{\Lambda} + L^\sigma \mathcal{C}^\sigma)\}^{-1} \{LD^\sigma w + \Lambda Bw + \bar{x}_0\} = -\{I - \mathcal{E}^\sigma\}^{-1} \{Z^\sigma D^\sigma w + (I + Q^\sigma) \Lambda Bw + (I + Q^\sigma) \bar{x}_0\}.
\]
Notice that, since \( \| \mathcal{E}^\sigma \| < 1 \), we have that
\[
\|e\| < 1 - \| \mathcal{E}^\sigma \| \times \|e\|,
\]
and hence the error, \( e \), in the above expression is a bounded signal. In fact,
\[
\|e\| \leq \frac{1}{1 - \| \mathcal{E}^\sigma \|} \times \|e\|.
\]
This implies that any generalized Luenberger observer, with (16) and (17)-(18), is a stable state-estimator and completes the proof.

**B. Optimal State-Estimator**

In this part, we present a resilient state-estimation design based on Theorem 10. We are interested to find the optimal state-estimator such that the estimation error is minimized. According to Theorem 10, any stable state-estimator can be written as
\[
\dot{x} = \Lambda \bar{\Lambda} \dot{x} + L^\sigma \left( \mathcal{C}^\sigma \dot{x} - y^\sigma \right),
\]
where, given \( \epsilon \in [0,1) \), there exist stable \( Q^\sigma \) and \( Z^\sigma \) such that
\[
L^\sigma = (I + Q^\sigma)^{-1} Z^\sigma,
\]
\[
\sup_{\sigma \in \mathcal{E}} \| \Lambda \bar{\Lambda} + \begin{bmatrix} \begin{array}{c} \mathcal{C}^\sigma \\ \Lambda \bar{\Lambda} - I \end{array} \end{bmatrix} \| < \epsilon.
\]
In above expression, the dependency of \( L^\sigma, Q^\sigma, \) and \( Z^\sigma \) on the switching signal is made explicit. The underlying assumption here is that the state-estimator knows the strategy of the attacker causally. That is, at each given time \( t \), the state-estimator has the knowledge \( \{\sigma(0), \sigma(1), \ldots, \sigma(t)\} \), but does not know the attacker’s strategy in future. We want to find \( Q^\sigma \) and \( Z^\sigma \) such that while (23) is satisfied the estimation error is minimized. The error estimation is derived in the proof of Theorem 10 given by
\[
e = -\{I - \mathcal{E}^\sigma\}^{-1} \{Z^\sigma D^\sigma w + (I + Q^\sigma) \Lambda Bw + (I + Q^\sigma) \bar{x}_0\}.
\]

\[\begin{aligned}
\mathcal{E}^\sigma &= \Lambda \bar{\Lambda} + \begin{bmatrix} \begin{array}{c} \mathcal{C}^\sigma \\ \Lambda \bar{\Lambda} - I \end{array} \end{bmatrix} \\
\{\begin{array}{c} \Lambda \bar{\Lambda} + \begin{bmatrix} \begin{array}{c} \mathcal{C}^\sigma \\ \Lambda \bar{\Lambda} - I \end{array} \end{bmatrix} \end{array} \end{bmatrix} &= (I + Q^\sigma) \Lambda \bar{\Lambda} + Z^\sigma - Q^\sigma.
\end{aligned}\]

**Theorem 11:** There exists a stable state-estimator such that the induced norm from \( w \) to the estimation error \( e \) is less than some positive real number \( \gamma \) if and only if there exist stable operators \( Q^\sigma \) and \( Z^\sigma \) such that
\[
\left[ \begin{array}{c} \Lambda \bar{\Lambda} + \begin{bmatrix} \begin{array}{c} \mathcal{C}^\sigma \\ \Lambda \bar{\Lambda} - I \end{array} \end{bmatrix} \end{array} \end{bmatrix} \left[ \begin{array}{c} \Lambda \bar{\Lambda} + \begin{bmatrix} \begin{array}{c} \mathcal{C}^\sigma \\ \Lambda \bar{\Lambda} - I \end{array} \end{bmatrix} \end{array} \end{bmatrix} \right] \leq \gamma.
\]

**Proof:** From Theorem 10, the set of all stable state-estimator is parametrized by \( (Q^\sigma, Z^\sigma) \) such that (17) and (18) hold. We notice that (18) is the same as (28) and, from (22), the induced norm from \( w \) to \( e \), when (28) is satisfied is given by
\[
\left[ \begin{array}{c} \begin{array}{c} \Lambda \bar{\Lambda} + \begin{bmatrix} \begin{array}{c} \mathcal{C}^\sigma \\ \Lambda \bar{\Lambda} - I \end{array} \end{bmatrix} \end{array} \end{array} \end{bmatrix} \left[ \begin{array}{c} \begin{array}{c} \Lambda \bar{\Lambda} + \begin{bmatrix} \begin{array}{c} \mathcal{C}^\sigma \\ \Lambda \bar{\Lambda} - I \end{array} \end{bmatrix} \end{array} \end{array} \end{bmatrix} \right] \leq \gamma.
\]

Therefore, the induced norm from \( w \) to the estimation error \( e \) is less than \( \gamma \) if (28) holds.

We note that searching over stable systems \( Q^\sigma \) and \( Z^\sigma \) such that (27)-(28) hold is a convex optimization but infinite dimensional optimization. In what follows, we will reduce (27)-(28) to finite dimensional convex optimization at the cost of finding sub-optimal (but arbitrarily close to optimal) solutions. To this end, according to Lemma 6 since \( (Q^\sigma, Z^\sigma) \) is stable, one can approximate them by FIR input-output switching systems. In doing so, in general, it becomes challenging to satisfy (28) exactly and hence we need to relax (28). The result is summarized in the following:

**Theorem 12:** Suppose there exist \( 0 \leq \bar{\epsilon} < 1 \) and FIR input-output switching systems \( Q^\sigma, Z^\sigma \in \mathcal{H}_\infty^{M} \) of some degree \( M \) such that
\[
\leq \bar{\gamma}.
\]

Then the optimal cost \( \gamma^* \) satisfies
\[
\gamma^* \leq \gamma + \bar{\epsilon} \bar{\gamma}.
\]

**Proof:** Immediate from the error dynamics given in (25).

We emphasize that (30)-(31) are in the so-called model-matching form and they can be solved using the methods developed in [8] with arbitrary accuracy.
V. ILLUSTRATIVE EXAMPLE

In this section, we derive the optimal state-estimator for problem outlined in Example 7. We use Theorem 12 as basis of our computations. The parameter values are given in Example 7 and the attackers strategy can cause switches in the C- and D-matrices as given by (12)-(13). First, we will find the optimal state-estimator for the nominal case, i.e., when $\sigma(\cdot)$ is constant and identically equal to 0. In this case, the optimal cost is $\gamma^* = 5.0275$ and the state-estimator is given by

$$\dot{x} = T y^0,$$

where the impulse response of $T = \{T(k)\}_{k=0}^{\infty}$ is given by

$$T(0) = \begin{bmatrix} 0 & 0.75 \\ 0.74 & -0.065 \\ -1.126 & -0.031 \end{bmatrix},$$

$$T(1) = \begin{bmatrix} -1.25 & -2 \\ 0.195 & 0 \\ -0.906 & -1 \end{bmatrix},$$

$$T(k) = 0, \text{ for } k \geq 2.$$

This state-estimator, however, does not result in a stable approximation error in the presence of DoS attack. One can use the method developed in this paper to find a stable state-estimator that is resilient to DoS attack strategy. In this example, we apply Theorem 12 and search for input-output switching ($Q^\sigma, Z^\sigma$) of degree 1. Furthermore, we let $\Xi$ to be the set of all binary sequences. For this case, we manage to find a stable state-estimator with optimal cost of $\gamma^* = 32.5$. The optimal state-estimator is given by $\dot{x} = T^\sigma y^0$ where $T^\sigma$ is an output-only switching system of degree one. At each time instant $t$,

$$\dot{x}(t) = \sum_{\tau=t-4}^{t} T^\sigma(i)(t-\tau) y^{\sigma(\tau)}(\tau),$$

where

$$T^i = \{T^i(k)\}_{k=0}^{4}, \text{ for } i = 1, 2,$$

is the FIR impulse response of $T^i$. The numerical values for the impulse response terms of $T^1$ are

$$T^1(0) = \begin{bmatrix} 0.24 & 0.44 \\ 0.37 & -0.17 \\ 0.06 & -0.17 \end{bmatrix}, T^1(1) = \begin{bmatrix} 0.25 & 0 \\ 0.39 & 0 \\ 0.94 & 0 \end{bmatrix},$$

$$T^1(2) = \begin{bmatrix} 0.02 & 0 \\ 0.14 & 0 \\ 0.07 & 0 \end{bmatrix}, T^1(3) = \begin{bmatrix} -0.21 & 0 \\ 0.01 & 0 \\ -0.3 & 0 \end{bmatrix},$$

$$T^1(4) = \begin{bmatrix} -2.1 & 0 \\ -0.06 & 0 \\ -0.93 & 0 \end{bmatrix},$$

And the impulse response of $T^2$ is given by

$$T^2(0) = \begin{bmatrix} -1.5 & 0 \\ 0.98 & 0 \\ 0.66 & 0 \end{bmatrix}, T^2(1) = \begin{bmatrix} 3.75 & 0 \\ 0.07 & 0 \\ 0.61 & 0 \end{bmatrix},$$

$$T^2(2) = \begin{bmatrix} 0 & 0 \\ -0.06 & 0 \\ -0.05 & 0 \end{bmatrix}, T^2(3) = \begin{bmatrix} 0 & 0 \\ -0.03 & 0 \\ -0.45 & 0 \end{bmatrix},$$

$$T^2(4) = \begin{bmatrix} -2.25 & 0 \\ 0.05 & 0 \\ -0.77 & 0 \end{bmatrix}.$$

VI. CONCLUSION

In this paper, utilizing the operator framework, we first parametrized the set of all stable state-estimators resilient to DoS attack. This was carried out by converting the problem to a state estimation problem for linear switched systems where the attacker's strategy prescribes the switching law. Furthermore, we showed that the set of generalized Luenberger observers captures all stable state-estimators. Then, we cast the problem of finding the optimal estimator as a convex optimization over the set of stable factors of the observer operator-gain. This optimization, for the $L_1$ induced norm, can be rewritten as a linear program which can be solved efficiently.

REFERENCES

[1] D. Powner and K. Rhodes, “Critical infrastructure protection: Multiple efforts to secure control systems are under way, but challenges remain,” 2007.

[2] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O’Brien, “Roadmap to secure control systems in the energy sector,” Energetics Incorporated. Sponsored by the US Department of Energy and the US Department of Homeland Security, 2006.

[3] A. A. Cárdenas, S. Amin, and S. Sastry, “Secure control: Towards survivable cyber-physical systems,” in 2008 The 28th International Conference on Distributed Computing Systems Workshops. IEEE, 2008, pp. 495–500.

[4] S. Amin, A. A. Cárdenas, and S. S. Sastry, “Safe and secure networked control systems under denial-of-service attacks,” in International Workshop on Hybrid Systems: Computation and Control. Springer, 2009, pp. 31–45.

[5] A. Gupta, C. Langbort, and T. Başar, “Optimal control in the presence of an intelligent jammer with limited actions,” in 49th IEEE Conference on Decision and Control (CDC). IEEE, 2010, pp. 1096–1101.

[6] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, “Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach,” IEEE Transactions on Automatic Control, vol. 60, no. 10, pp. 2831–2836, 2015.

[7] M. Naghnaeian and P. G. Voulgaris, “Characterization and optimization of $L_1$ gains of linear switched systems,” IEEE Transactions on Automatic Control, vol. 61, no. 8, pp. 2203–2218, 2016.

[8] M. Naghnaeian, P. G. Voulgaris, and G. E. Dullerud, “LP analysis and synthesis of linear switched systems: A unified input-output and state-space approach,” SIAM Journal on Control and Optimization, vol. 56, no. 2, pp. 1181–1205, 2018.

[9] M. Naghnaeian, P. G. Voulgaris, and N. Elia, “A unified framework for decentralized control synthesis,” in 2018 European Control Conference (ECC). IEEE, 2018, pp. 2482–2487.