Optimal Denial-of-Service Attack Scheduling in Cyber-Physical Systems*

Heng Zhang¹, Peng Cheng¹, Ling Shi² and Jiming Chen¹

Abstract

Security of Cyber-Physical Systems (CPS) has gained increasing attention in recent years. Most existing works mainly investigate the system performance given some attacking patterns. In this paper, we investigate how an attacker should schedule its Denial-of-Service (DoS) attacks to degrade the system performance. Specifically, we consider the scenario where a sensor sends its data to a remote estimator through a wireless channel, while an energy-constrained attacker decides whether to jam the channel at each sampling time. We construct optimal attack schedules to maximize the expected average estimation error at the remote estimator. We also provide the optimal attack schedules when a special intrusion detection system (IDS) at the estimator is given. We further discuss the optimal attack schedules when the sensor has energy constraint. Numerical examples are presented to demonstrate the effectiveness of the proposed optimal attack schedules.

Index Terms

State estimation, DoS attack, energy constraint.

I. INTRODUCTION

Recently, Cyber-Physical Systems (CPS), in which information and physical elements are closely integrated, have gained much research interest from various aspects [2], [3]. Applications of CPS have a wide spectrum, such as battle field, smart grid, smart building, intelligent transportation, etc. CPS are vulnerable to different types of malicious attacks which make the security a fundamental issue for reliable services [2]. A famous example is that in June 2010 a cyber worm named ‘stuxnet’ attacked an Iranian nuclear facility at Natanz, which resulted in 60% hosts damaged [4].

Researchers have investigated security issues in CPS from different perspectives recently [5], [6]. Teixeira et al. [6] summarized the characteristics of network attacks and defined an attack space with the adversary’s priori knowledge of the system model, its disclosure, and disruption resources. Typical attacks can be categorized into Denial-of-Service (DoS) attack, replay data attack, and false data injection attack [6]. DoS attack that blocks the communication between the system components has been well

¹H. Zhang, P. Cheng and J. Chen are with State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, China ezhangheng@gmail.com, pcheng@iipc.zju.edu.cn, jmchen@ieee.org
²L. Shi is with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong, China eesling@ust.hk
*Part of this work has been presented by IEEE CDC 2013 [1].
studied, since it is the most reachable attack pattern in the attack space [7]. Besides the theoretical research on DoS attack, some experiments were also conducted to demonstrate the effect of DoS attacks [8].

In practice, energy constraint is a natural concern for various types of attackers, which will affect their attack policies [9], [10]. Law et al. [9] pointed out that jammers may run out of energy very fast when their energy budget is limited. Kavitha et al. [10] introduced a random DoS attacker who randomly decides to jam the channel or sleep in order to save the energy.

Most existing works mainly investigate the system performance for given attack patterns. The study of the adversary’s optimal attack schedules and the corresponding consequences is an important aspect in CPS security as pointed out in [11]. Motivated by this, we aim to answer how to optimally schedule the attack so as to maximize the attacking effect on a CPS. Specifically, we consider a system where one sensor processes the measurements and sends the data to a remote estimator through a wireless channel. An attacker has a limited attacking energy budget, and decides at each sampling time whether or not to jam the channel in order to degrade the remote estimation quality. To the best of our knowledge, this is the first work on the DoS attack schedules against remote state estimation. The main contributions of this paper are summarized as follows:

1) We construct the optimal DoS attack schedules, which maximize the expected average estimation error.
2) We present the optimal attack schedules when a special IDS in the estimator is given.
3) We further present the optimal attack schedules when both the sensor and the attacker have energy constraints.

The remainder of the paper is organized as follows: In Section II, we formulate the attack schedule problems. In Section III, we construct the optimal DoS attack schedules for maximizing the expected average intrusion detection system. In Section IV, we study the optimal attack schedules when the sensor also has energy constraint. In Section V, numerical examples are shown to illustrate the results. Finally, Section VII concludes the paper.

**Notations:** $S^n_+$ stands for the set of $n \times n$ positive semi-definite matrices. $\mathbb{Z}^+$ stands for the set of positive integers. $\mathbb{E}[X]$ is the mean of random variable $X$, and $\mathbb{E}[X|Y]$ is the mean of random variable $X$ conditioned on $Y$, respectively. $\| \gamma \|_0$ is used to denote the zero norm of $\gamma$, which is the number of nonzero entries of the vector $\gamma$. $Tr(\cdot)$ represents the trace of matrix.

II. PROBLEM FORMULATION AND PRELIMINARIES

A. **Problem formulation**

Consider the following system (Fig. 1)

\[
\begin{align*}
x_{k+1} &= Ax_k + w_k, \\
y_k &= Cx_k + v_k,
\end{align*}
\]

(1)

where $x_k \in \mathbb{R}^{n_x}$ is the system state with $n_x \in \mathbb{Z}^+$, $y_k \in \mathbb{R}^{n_y}$ is the sensor measurement with $n_y \in \mathbb{Z}^+$, $w_k \in \mathbb{R}^{n_x}$ is the process noise, $v_k \in \mathbb{R}^{n_y}$ is the measurement noise, and $w_k$ and $v_k$ are uncorrelated
zero mean Gaussian noises with covariance $\Sigma_w$ and $\Sigma_v$, respectively. The pair $(A, C)$ is assumed to be observable and $(A, \Sigma_{\frac{1}{2}}w)$ is controllable.

After $y_k$ is obtained, the sensor pre-estimates the state $x_k$, and then sends its minimum mean squared error (MMSE) estimate $\hat{x}^*_{k} = \mathbb{E}[x_k|y_1, \ldots, y_k]$ to a remote estimator through a wireless channel.

We consider the scenario that there is an attacker which degrades the remote estimation quality by jamming the wireless channel. The attacker has a limited energy budget and has to determine whether to jam the channel or not at each sampling time. It is assumed that the packet will arrive at the remote estimator if there is no DoS attack during the transmission.

Denote $\gamma_k = 1$ or $0$ as the attacker’s decision variable at time $k$, and $\gamma$ as a schedule that defines $\gamma_k$ at each $k$. When the attacker launches an attack and jams the channel, the sensor data packet will be dropped with probability $\alpha$. Denote $\theta_k = 1$ or $0$ as the indicator function whether the data packet drops or not. We assume that $\theta_k$’s are i.i.d. Bernoulli random variables with $\mathbb{E} (\theta_k) = \alpha$.

Denote all the data packet received at the estimator until time $k$ as $D(\gamma_{1:k})$. The remote estimator then computes its own MMSE estimate $\hat{x}_k$ and its corresponding estimation error covariance $P_k$ based on $D(\gamma_{1:k})$, e.g.,

$$\hat{x}_k(\gamma_{1:k}) = \mathbb{E}[x_k|D(\gamma_{1:k})]$$

and

$$P_k(\gamma_{1:k}) = \mathbb{E}[(x_k - \hat{x}_k)(x_k - \hat{x}_k)']|D(\gamma_{1:k})].$$

For simplicity, we write $\hat{x}_k(\gamma_{1:k})$ as $\hat{x}_k$, etc., when the schedule $\gamma_{1:k}$ is given.

Consider a finite horizon $T$. Due to the finite energy constraint, assume the attacker can only launch $n$ attacks from $k = 1$ to $k = T$, i.e., $\|\gamma\|_0 = n$.

**Average Error:** For a given attack schedule $\gamma$, define $J_a(\gamma)$ as the average expected estimation error covariance matrix, i.e.,

$$J_a(\gamma) = \frac{1}{T} \sum_{k=1}^{T} \mathbb{E}[P_k(\gamma_k)].$$

In this paper, we aim to solve the following problem in the viewpoint of the attacker:

\[ Since the bit error rate (BER) is fixed in every attack time when the attacker exploits the same energy to jam the channel [12], we assume that the rate of successful attacks follows a Bernoulli probability distribution. \]
Problem 2.1:

$$\max_{\gamma \in \Gamma} Tr[J_a(\gamma)],$$

s.t. $\|\gamma\|_0 = n,$

where $\Gamma = \{0, 1\}^T$ is the set of all possible attack schedules.

III. OPTIMAL ATTACK SCHEDULE ANALYSIS

A. State estimation under DoS attack

In this section, we present some properties of the estimation error at the remote estimator under a DoS attack.

The MMSE estimate $\hat{x}_k^s$ is obtained from a standard Kalman filter. Let $P_k^s$ be the estimation error covariance matrix of $\hat{x}_k^s.$ Standard Kalman filtering analysis shows that $P_k^s$ converges exponentially to its steady-state value $\overline{P}.$ ² For brevity, we assume $\Pi_0 = \overline{P},$ then it can be easily obtained that $P_k^s = \overline{P}$ for all $k \in [1, T].$ Define $h, h^k : \mathbb{S}^n_+ \rightarrow \mathbb{S}^n_+$ as

$$h(X) \triangleq AXA' + \Sigma_w,$$

and

$$h^k(X) \triangleq h \circ h \circ \cdots \circ h(X).$$

From [14], the following result holds.

**Lemma 3.1:** The function $h$ has following property:

$$\overline{P} \leq h(\overline{P}) \leq h^2(\overline{P}) \leq \cdots \leq h^k(\overline{P}) \leq \cdots, \forall k \in \mathbb{Z}^+.$$

It is straightforward to show that at the remote estimator, $\hat{x}_k$ and $P_k$ are obtained as follows [15]:

$$(\hat{x}_k, P_k) = \begin{cases} (A\hat{x}_{k-1}, h(P_{k-1})), & \text{if } \gamma_k = 1 \text{ and } \theta_k = 1, \\ (\hat{x}_k^s, \overline{P}), & \text{otherwise.} \end{cases}$$

Assume the data packet is delivered to the remote estimator successfully at time $s$, and the attacker launches $m$ consecutive attacks from time $s + 1$ to $s + m.$ The state space of the error covariance matrix $P_k$ in this period is $\{\overline{P}, h(\overline{P}), \ldots, h^m(\overline{P})\}.$

We can see that the error covariance matrix $P_k$ during the consecutive attack period $[s + 1, s + m]$ is a stationary Markov chain, and the transition probability matrix $(p_{ij})$ is given by

$$p_{ij} = Pr\{P_k = h^j(\overline{P})|P_{k-1} = h^i(\overline{P})\} = \begin{cases} \alpha, & j = i + 1, \\ 1 - \alpha, & j = 0, \\ 0, & \text{others}, \end{cases}$$

$(2)$

$i, j = 0, 1, 2, \ldots, m.$ Moreover, we have the following properties for $P_k, k \in [s + 1, s + m].$

²Since the pair $(A, C)$ is observable and $(A, \Sigma_w)$ is controllable, $\overline{P}$ uniquely exists and can be obtained from the discrete algebraic Riccati equation. Even if the assumption on controllability and observability fails, there are other iterative algorithms that can ensure quick convergence to the stabilizing solution for the steady-state Kalman filtering [13]. Thus it is reasonable to assume that $\Pi_0 = \overline{P}.$
Property 3.1: During the consecutive attack period \([s + 1, s + m]\):

1) the distribution of the error covariance matrix \(P_{s+k}\) can be computed as

\[
Pr\{P_{s+k} = h^i(\mathcal{P})\} = \begin{cases} 
\alpha^i - \alpha^{i+1}, & i = 0, 1, \ldots, k - 1; \\
\alpha^k, & i = k.
\end{cases}
\]

2) the conditional probability can be computed as follows:

\[
Pr\{P_{s+k} = h^j(\mathcal{P})|P_s = h^i(\mathcal{P})\} = \begin{cases} 
\alpha^j - \alpha^{j+1}, & j = 0, 1, \ldots, k - 1; \\
\alpha^k, & j = i + k.
\end{cases}
\]

Proof: See the Appendix.

Property 3.2: 1) If the packet is not received at the remote estimator at time \(s\), then \(E[P_{s+m}|P_s \geq \mathcal{P}] \geq E[P_{s+m}|P_s = \mathcal{P}]\).

2) Consider two different consecutive attacking periods, \(n_1\) and \(n_2\), where \(n_1 \geq n_2\). Then \(E[P_{s+n_1}] \geq E[P_{s+n_2}]\).

An attack scheme with given attacking number \(n\) can be divided into the following consecutive attacking sequences, \(k_1, k_2, \ldots, k_s\), i.e.,

\[
(0, \cdots, 0, 1, \cdots, 1, 0, \cdots, 0, 1, \cdots, 1, 0, \cdots, 0),
\]

where \(\sum_{i=1}^{s} k_i = n\). Note that each neighboring sequences are divided by at least one zero. Using Property 3.1, we have

\[
J_a(\gamma) = \frac{1}{T} \sum_{k=1}^{T} \mathbb{E}[P_k(\gamma_k)] = \frac{1}{T} \sum_{i=1}^{s} \sum_{n_i=1}^{k_i} \mathbb{E}[P_{s+i+n_i}] + \frac{T-n}{T} \mathcal{P}
\]

\[
= \frac{1}{T} \sum_{i=1}^{s} \sum_{n_i=1}^{k_i} (\sum_{m=0}^{n_i-1} h^m(\mathcal{P})(\alpha^m - \alpha^{m+1}) + \alpha^n h^n(\mathcal{P})) + \frac{T-n}{T} \mathcal{P}. \quad (3)
\]

Note that (3) is independent of the attack start sequence \(s_i, i = 1, 2, \ldots, s\), which means that any permutation of the \(k_i\)'s will lead to the same average expected estimation error. Thus, for the consecutive attack sequences \(k_1, k_2, \ldots, k_s\), we define \(\gamma_{k_1 \oplus k_2 \oplus \cdots \oplus k_s}\) as the set of attack schedules which have the same performance \(J_a(k_1 \oplus k_2 \oplus \cdots \oplus k_s)\). For simplicity, we write \(\gamma_{k_1 \oplus k_2 \oplus \cdots \oplus k_s}\) as \(\gamma_{k_1 \oplus k_2 \oplus \cdots \oplus k_s}\) and write \(J_a(k_1 \oplus k_2 \oplus \cdots \oplus k_s)\) as \(J_a(k_1 \oplus k_2 \oplus \cdots \oplus k_s)\), when the time horizon \([1, T]\) is given. In particular, let \(\gamma^n\) be the set of attack schedules with a consecutive attack sequence \(n\), which have the same performance \(J_a^{(n)}\).

Property 3.3: The following statements are true.

1) \(J_a^{(n_1)} \leq J_a^{(n_2)}\), where \(n_1 \leq n_2\).
2) \(J_a^{(n_1 \oplus n_2)} \leq J_a^{(n)}\), where \(n = n_1 + n_2\).
3) \(J_a^{(n_1 \oplus n_2 \oplus \cdots \oplus n_s)} \leq J_a^{(n)}\), where \(n = n_1 + n_2 + \cdots + n_s\).
4) \(J_a^{(m_1 \oplus m_2)} \leq J_a^{(m_1 \oplus m_2)}\), where \(m_1 + m_2 = n_1 + n_2\) and \(\max\{m_1, m_2, n_1, n_2\}\) is \(n_1\) or \(n_2\).

Proof: See the Appendix.

From statement 1) and 4) in Property 3.3, we can see that the more the attack times are grouped together, the larger the system cost becomes. Statement 2) and 3) demonstrate that consecutive attack is much better than scattered attack from the viewpoint of attacker.
B. Optimal attack schedule design

Now we are ready to present the optimal attack schedule for Problem 2.1.

**Theorem 3.1:** The optimal attack schedule that solves Problem 2.1 is anyone that belongs to $\gamma^n$, and the corresponding cost is given by

$$Tr(J_a)_{\text{max}} = \frac{1}{T} \sum_{i=1}^{n} Tr[h_i(\alpha, \overline{P})] + \frac{T - n\alpha}{T} Tr(\overline{P}),$$  \hspace{1cm} (4)

where $h_i(\alpha, \overline{P}) = [(n - i)(\alpha^i - \alpha^{i+1}) + \alpha^i]h_i(\overline{P})$.

**Proof:** A direct result from Property 3.3 2) and 3).

As a byproduct, we can obtain the worst attack strategy which minimizes the expected average error covariance.

**Problem 3.1:**

$$\min_{\gamma \in \Gamma} Tr[J_a(\gamma)],$$

s.t. $\| \gamma \|_0 = n,$

The solution of Problem 3.1 is given by the following theorem.

**Theorem 3.2:** 1) If $n \leq \frac{1}{2}T$, an optimal solution for Problem 3.1 is anyone in $\gamma^{1\oplus 1\oplus \cdots \oplus 1}$, and the corresponding cost is given by

$$Tr(J_a)_{\text{min}} = \frac{T - n\alpha}{T} Tr(\overline{P}) + \frac{n\alpha}{T} Tr[h(\overline{P})].$$  \hspace{1cm} (5)

2) If $n > \frac{1}{2}T$, an optimal solution for Problem 3.1 is

$$((1 \cdots 10) \cdots (1 \cdots 10)(1 \cdots 101 \cdots 1101 \cdots 110 \cdots 1)),$$

where $r_1 + r_2 = T - n - 1$, $z = \left\lfloor \frac{n}{T-n} \right\rfloor$, and $m_1 = m_2 = \frac{m}{2}$ if $m$ is even, $m_1 = \left\lfloor \frac{m}{2} \right\rfloor$, $m_2 = m - m_1$ or $m_1 = \left\lfloor \frac{m}{2} \right\rfloor + 1, m_2 = m - m_1$ if $m$ is odd, with $m = z + [n \mod (T - n)].$ The resulting cost is

$$Tr(J_a)_{\text{min}} = \frac{1}{T} Tr\{(T - n - 1) \sum_{i=1}^{z} h_i(\alpha, \overline{P}) + \sum_{i=1}^{m_1} h_i(\alpha, \overline{P}) + \sum_{i=1}^{m_2} h_i(\alpha, \overline{P}) + [(T - n) + m(1 - \alpha) + z(1 - \alpha)(T - n - 1)]\overline{P}\},$$  \hspace{1cm} (6)

where

$$h_i(\alpha, \overline{P}) = [(n - i)(\alpha^i - \alpha^{i+1}) + \alpha^i]h_i(\overline{P}).$$

**Proof:** A direct result from Property 3.3 3) and 4).

From the above two theorems, one can see that grouping the attacks together leads to maximal attacking effect, while separating the attacks as uniformly as possible leads to the minimal degradation. Thus the results can be viewed as the upper and lower bound of the damage an arbitrary attack schedule can make.

$^3 \lfloor x \rfloor$ is floor function, which is defined as the largest integer that is less than real number $x$.

$^4 \mod$ is defined as modulo operation, i.e., $n \mod m$ is the remainder in division $\frac{n}{m}$, where $n$ and $m$ are two positive integer.
IV. OPTIMAL ATTACK SCHEDULES AGAINST A GIVEN IDS

The aforementioned problems are discussed under the assumption that the channel is perfect and there is no defensive measure. In practical applications, when the estimator considers unknown factors from environment changes or adversary’s intrusion, which may lead to data drops, a detector is often designed at the receiver side as a first step to reduce the effectiveness of these factors. For example, packet reception rate ($P_{RR}$) at the receiver side is proposed as the criteria for intrusion detection in [16]. $P_{RR}$ is the rate of packets reception that are successfully delivered to the estimator compared to the number of packets that have been sent out by the sensor.

In practice, the $P_{RR}$ can be computed for a given length of a time window $\tau$, i.e., $P_{RR} = \frac{\sigma}{\tau}$, where $\sigma$ is the packet reception numbers in the time window. If the $P_{RR}$ is too small, the detector will deduce that there may exist an attacker, which triggers an alarm to alert the sensor. Then the sensor can use channel hopping technology to guarantee the packet can be received by the remote estimator [17]. In this paper, we assume that the alarm is triggered if $P_{RR} \leq P_{RR0}$, where $P_{RR0}$ is a given alarm bound.\(^5\)

![Fig. 2. Schematic of attack on the network against state estimation with an intrusion detector.](image)

Before introducing the attack schedule against the IDS mechanism, we present a property to help formulate the attack optimization problem.

**Property 4.1:** The alarm triggering condition $P_{RR} \leq P_{RR0}$ is equivalent to $P_k \notin h^d(\bar{P}), k = 1, 2, \ldots, T$, where $d = \tau - \sigma_0$, $\sigma_0 = \max\{\sigma|\frac{\sigma}{\tau} \leq P_{RR0}\}$.

**Proof:** See the Appendix.

**Remark 4.1:** From Property 4.1, any attack schedule with at most $d$ times consecutive attack, i.e., $\sum_{i=k+1}^{k+\tau} \gamma_i \leq d, k = 0, 1, \ldots, T - \tau$, can guarantee that the attack action will not be detected by the estimator. In fact, time window $\tau$ and threshold $P_{RR0}$ can be evaluated by the attacker when he eavesdrops the transmission channels before taking attack actions.

In order not to be detected by IDS, we consider Problem 2.1 with an additional constraint, i.e.,

\(^5\)By utilizing the pseudo-random sequence, the sensor and estimator may implement channel hopping once the alarm is triggered [18]. However, the attacker can detect such channel switch by detecting the alarm signal, and search the new communication channel by scanning the wireless spectrum. In this way, the attacker can learn the alarm bound through statistical analysis, and follow the design against such IDS mechanism.
Problem 4.1:

\[
\max_{\gamma \in \Gamma} Tr[J_a(\gamma)],
\]
\[s.t. \| \gamma \|_0 = n,
\]
\[
\sum_{i=k+1}^{k+\tau} \gamma_i \leq d, k \in [0, T - \tau].
\] (7)

The following result presents the optimal solution to Problem 4.1.

Theorem 4.1: Consider Problem 4.1. Let \( d = \tau - \sigma_0 \), where \( \sigma_0 = \max\{\sigma | \frac{\sigma}{\tau} \leq PRR_0\} \).

1) If \( d \geq n \), any \( n \) times consecutive attack is optimal, and the corresponding cost is (4).

2) If \( d < n \), the optimal attack schedule has the structure as follows,

\[
\begin{array}{c}
\text{( 0 ... 0)(1 ... 0 ... 0) ... (1 ... 0 ... 0) (0 ... 0 1 0 ... 0) (0 ... 0 1 0 ... 0) ... (0 ... 0 1 0 ... 0) (0 ... 0 1 0 ... 0) (0 ... 0 1 0 ... 0)} \times \\
\text{z_0 times d times \sigma_0 times d times \sigma_0 times z_1 times r times z_2 times d times \sigma_0 times d times \sigma_0 times d times z_3 times s_1 times s_2 times}
\end{array}
\] (8)

where \( z_0 + z_1 + z_2 + z_3 + (s_1 + s_2)\sigma_0 = T - n \), and \( s_1 + s_2 = m \), where \( m \) is the quotient of \( n/d \) and \( r \) is the remainder. The corresponding cost is

\[
Tr(J_a)^{PRR}_{max} = \frac{1}{T} \left\{ m \sum_{i=1}^{d} Tr[h_i(\alpha, \mathcal{P})] + \sum_{i=1}^{r} Tr[h_i(\alpha, \mathcal{P})] \right\} + \frac{T - n\alpha}{T} Tr(\mathcal{P}).
\]

Proof: See the Appendix.

Remark 4.2: In Problem 4.1, the attacker can completely avoid the given IDS mechanism. However, this attack schedule seems too cautious from an adventurous attacker’s point of view. If the adventurous attacker still decides to use an attack schedule proposed in Theorem 3.1, the probability of being detected is \( \sum_{k>d} \binom{k}{\tau} \alpha^\tau (1 - \alpha)^k \) if \( n > \tau \), and is \( \sum_{k>d} \binom{n}{k} \alpha^{n-k} (1 - \alpha)^k \) if \( n \leq \tau \).

V. Optimal attack schedules with sensor’s energy constraint

The aforementioned problems are discussed under the assumption that the sensor has sufficient energy to transmit throughout the entire time horizon. When the sensor’s energy is also limited and cannot transmit all the time, the attacker needs to change the attacking schedule. Here we assume that the sensor and the estimator do not know the existence of the attacker.

Some literatures have focused on sensor scheduling and optimal state estimation in a lossy network environment [15], [19]–[22]. Sinopoli et. al. studied the problem of state estimation using Kalman filtering in an i.i.d. packet-dropping network [19]. Reference [20] studied optimal state estimation and optimal LQG controller design over an intermittent packet-dropping network. Shi et al. [15] investigated sensor scheduling strategies to minimize the average estimation error under energy constraint. Mo et al. [21] provided a stochastic sensor selection scheme to minimize the asymptotic expected estimation error covariance due to the energy constraint. You et. al. [22] investigated the stability of the mean estimation error over a network subject to Markovian packet losses. More related works can be found in the reference therein. However, these literatures have not considered the state estimation quality when a DoS attacker jams the wireless channel and this shortage motivates us to study the subsequent problem.
Denote $\vartheta_k = 1$ or 0 as the sensor’s transmission decision variable at time $k$, and $\vartheta$ as a scheduling scheme that defines $\vartheta_k$ at each $k$. $\Theta$ is the set of the sensor’s transmission schedules. We assume that the sensor has energy constraint with $\| \vartheta \|_0 = N$ and we consider the following problem in this section.

**Problem 5.1:**

$$\max_{\gamma \in \Gamma} \min_{\vartheta \in \Theta} Tr[J_0(\vartheta, \gamma)],$$

s.t. $\| \vartheta \|_0 = N,$

$$\| \gamma \|_0 = n.$$  \hfill (9)

From [15], we have the following property:

**Property 5.1:** Let $q = \lfloor \frac{T}{N} \rfloor$.

1) If $N < \frac{1}{2} T$, the optimal sensor schedule $\vartheta^* \in \Theta$ that minimizes the $Tr(J_0)$ has following structure

$$(1 \cdots 0)(1 \cdots 0) \cdots (1 \cdots 0),$$  \hfill (12)

in which there are $T-qN$ times $\tau_i = q$ and $(q+1)N-T$ times $\tau_i = q-1$ in $\{\tau_i, i = 1, 2, \ldots, N\}$.

2) If $N \geq \frac{1}{2} T$, $\vartheta^*$ has structure (12) with $T-N$ times $\tau_1 = 1$ and $2N-T$ times $\tau_i = 0$ in $\{\tau_i, i = 1, 2, \ldots, N\}$.

Here we assume that the attacker obtains the sensor’s transmission strategy by eavesdropping the transmission channel over a long period before starting its attack action. We denote $t_{(i)}$, $i = 1, 2, \ldots, N$ as the sensor’s data transmission time. If $n \geq N$, it is obvious that optimal attack schedule is taking actions at full transmission time $t_{(i)}$, $i = 1, 2, \ldots, N$. Thus we only need to consider **Problem 5.1** for $n < N$ hereinafter.

**Theorem 5.1:** Consider **Problem 5.1** with $n < N$.

1) When $N < \frac{1}{2} T$ and the sensor’s schedule $\vartheta^*$ has the structure $$(1 \cdots 0)(1 \cdots 0) \cdots (1 \cdots 0),$$  \hfill (12)

the optimal attack schedules are given by

$$\gamma_{t(k)} = 1, k = i + 1, i + 2, \ldots, i + n,$$

and $\gamma_k = 0$ otherwise. The corresponding cost is given by

$$Tr(J_0)_{max} = \frac{1}{T} \sum_{i=1}^{n} Tr[\alpha_i(\Delta_\tau)] + \frac{N - n\alpha}{T} Tr(\Delta_\tau),$$

where $h_i(\alpha, \Delta_\tau) = [(n-i)(\alpha^{i-1} - \alpha^{i+1}) + \alpha^i h'(\Delta_\tau)].$

2) When $N \geq \frac{1}{2} T, \alpha = 1$ and the sensor’s schedule $\vartheta^*$ has the structure $$(1 \cdots 1 0)(1 \cdots 1 0) \cdots (1 \cdots 1 0),$$  \hfill (12)

the optimal attack schedules $\gamma^*$ are given by

$$\gamma_{t(k)} = 1, k = i + 1, i + 2, \ldots, i + n,$$

and $\gamma_k = 0$ otherwise. The corresponding cost is given by

$$Tr(J_0)_{max} = \frac{1}{T} Tr[(N-n)\mathcal{P} + (T-N-b)h(\mathcal{P}) + \sum_{i=1}^{n+b} h'(\mathcal{P})],$$  \hfill (13)
where \( n = \delta b + b_0 \) with \( 0 \leq b_0 < b \).

**Proof:** 1) The proof is similar to that of Theorem 3.1. The only difference is that we replace \( \overline{P} \) by \( \Delta_t \).

2) One can easily obtain that the resulting cost under the attack schedule \( \gamma^* \) is (13). For an arbitrary attack schedule \( \gamma \), we have

\[
Tr(J_a(\gamma)) = \frac{1}{T} Tr\left[ (N - n) \overline{P} + m_1 h(\overline{P}) + \sum_{i=1}^{m_2} \sum_{j=1}^{s_i} h^j(\overline{P}) \right],
\]

where \( t_i \) is the length of \( i \)-th \( (i = 1, 2, \ldots, m_2) \) attack period \([s_i + 1, s_i + t_i]\) which satisfies \( \vartheta_{s_i} = 1, \gamma_{s_i} = 0, \vartheta_{s_i + t_i} = 1, \gamma_{s_i + t_i} = 0 \), and \( \vartheta_k = 1, \gamma_k = 1 \) or \( \vartheta_k = 0, \gamma_k = 0 \) for \( k = s_i + 2, \ldots, s_i + t_i - 1 \), and \( (N - n) + m_1 + \sum_{i=1}^{m_2} t_i = T \) and \( \sum_{i=1}^{m_2} t_i \leq n + b \). Then we have

\[
Tr(J_a(\gamma^*)) - Tr(J_a(\gamma)) = \frac{1}{T} Tr\left[ \sum_{i=1}^{n+b} h_i^i(\overline{P}) - \sum_{i=1}^{m_2} \sum_{j=1}^{s_i} h^j(\overline{P}) - [m_1 - (T - N - b)]h(\overline{P}) \right] > 0,
\]

which completes the proof.

**Example 5.1:** (1) Consider the Problem 5.1 for \( N < \frac{1}{2}T \) with \( T = 12, N = 4, n = 2, \tau = 2 \). From Property 5.1, one notes that the optimal sensor transmission schedule is \( \vartheta^* = (100)(100)(100)(100) \). Then we can obtain three optimal attack schedules \((100)(100)(000)(000), (000)(100)(100)(000), (000)(000)(100)(100)\).

(2) For \( N \geq \frac{1}{2}T \), consider \( T = 12, N = 9, n = 6, \delta = 3 \). From Property 5.1, the optimal sensor transmission schedule is \( \vartheta^* = (1110)(1110)(1110) \). Then we obtain four optimal attack schedules \((1110)(1110)(0000), (0110)(1110)(1000), (0010)(1110)(1100), (0000)(1110)(1110)\).

**Remark 5.1:** In Theorem 5.1 we study some special cases of Problem 5.1, and obtain the optimal attack schedules. Note that these schedules only depend on the sensor transmission schedule \( \vartheta^* \) rather than on the system parameters. Thus the attacker can run his optimal attack schedules when he obtains the sensor’s transmission schedule \( \vartheta^* \). The general cases of Problem 5.1, however, are complicated since the optimal attack schedules depend on sensor transmission schedule \( \vartheta \), the system parameters, and the attack successful probability. An example is given in Section VI (Fig. 5) to illustrate this.

**Remark 5.2:** In many situations, the expected terminal estimation error, i.e., \( J_T = \mathbb{E}[P_T] \) is considered as another important system performance index [23]. When the attacker tries to maximize the trace of expected terminal estimation error covariance, one can see that the optimal attack schedule is to consecutively attack at time \( k = T - n + 1, T - n + 2, \ldots, T \). If the detector with (7) is embedded in estimator, any feasible attack schedule with \( \gamma_{T-d} = 0, \gamma_k = 1, k = T - d + 1, T - d + 2, \ldots, T \) is optimal. If the sensor also has energy constraint (10) with \( N > n \), we can prove that the optimal attack schedule is \( \gamma_{(k)} = 1, k = T - n + 1, T - n + 2, \ldots, T, \gamma_k = 0 \) otherwise.

**VI. EXAMPLES**

Consider system (1) with

\[
A = \begin{bmatrix} 1.2 & 0.1 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \Sigma_w = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \Sigma_v = 0.5C.
\]
The effects of different attack schedules are evaluated. In Fig. 3, where we examine the performance under different attack times from 1 to 10 with $T = 100$, $\alpha = 1$. It can be seen that the performance under the optimal attack schedules given by Theorem 3.1, i.e., $Tr(J_a)_{\text{max}}$, increases rapidly with the allowable attack times. $Tr(J_a)_{\text{min}}$, which is under the attack schedule obtained in Theorem 3.2, and $Tr(J_a)_{\text{P RR max}}$, which is under the attack schedule given in Theorem 4.1 with $PRR \leq \frac{3}{7}$, grow much slower than $Tr(J_a)_{\text{max}}$. It also can be found that $Tr(J_a)_{\text{max}}$ and $Tr(J_a)_{\text{P RR max}}$ are overlapping since they have the same optimal attack schedule set $\gamma^n$ when $n \leq 4$. But if $n > 4$, $Tr(J_a)_{\text{P RR max}}$ grows much slower than $Tr(J_a)_{\text{max}}$ as the attack schedules need to be re-designed under the given intrusion detection mechanism. It also can been seen that the attack effectiveness is significantly reduced by this detection constraint.

In Fig. 4, we examine the estimation quality with different successful attack probabilities. In this example, the adversary can attack 10 times in the time horizon $[1, 100]$. From Fig. 4, we can see that $Tr(J_a)_{\text{max}}$ increases rapidly when the success probability $\alpha$ increases. On the other hand, $Tr(J_a)_{\text{min}}$ grows much slower when $\alpha$ increases, which also demonstrates the attack effectiveness of our designed attack schedule. $Tr(J_a)_{\text{P RR max}}$ also grows slower due to the constraint of avoiding being detected.

**TABLE I**  
**ATTACK SCHEDULES**

<table>
<thead>
<tr>
<th>attack schedule</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$ with $\gamma_{t(i)} = 1$</td>
<td>1,2,3</td>
<td>2,3,4</td>
<td>3,4,5</td>
<td>1,2,4</td>
<td>1,2,5</td>
</tr>
<tr>
<td>attack schedule</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>$i$ with $\gamma_{t(i)} = 1$</td>
<td>1,3,4</td>
<td>1,3,5</td>
<td>2,3,5</td>
<td>2,4,5</td>
<td>1,4,5</td>
</tr>
</tbody>
</table>

In Fig. 5, we examine the estimation quality under different attack schedules when the sensor has energy constraint. Here $T = 14$, $N = 5$, $n = 3$. The sensor transmission schedule is chosen as $\vartheta^* = (100)(100)(10)(100)(100)$. There are 10 attack schedules which has been listed in TABLE I. We assume
\( \vartheta_{-1} = 1, \vartheta_0 = 0 \) for the time \( t = -1, 0 \), respectively. The effectiveness of the attack is studied with attack successful probability \( \alpha = 0.8 \) and \( \alpha = 0.1 \) in Fig. 5 (a) and (b), respectively. In Fig. 5 (a), it can be seen that attack schedule 2 (\( \gamma_{t(2)} = \gamma_{t(3)} = \gamma_{t(4)} = 1 \)) and attack schedule 3 (\( \gamma_{t(3)} = \gamma_{t(4)} = \gamma_{t(5)} = 1 \)) are optimal when the attack successful probability \( \alpha = 0.8 \). However, when \( \alpha = 0.1 \), from Fig. 5 (b) we can see that attack schedule 5 (\( \gamma_{t(1)} = \gamma_{t(2)} = \gamma_{t(5)} = 1 \)), attack schedule 8 (\( \gamma_{t(2)} = \gamma_{t(3)} = \gamma_{t(5)} = 1 \)), and attack schedule 9 (\( \gamma_{t(2)} = \gamma_{t(4)} = \gamma_{t(5)} = 1 \)) are optimal which is different from \( \alpha = 0.1 \). In general, it is difficult to find these optimal attack schedules explicitly. On the other hand, the suboptimal attack schedules 1, 2, 3 only depend on sensor transmission schedule \( \vartheta \), and can be easily obtained.

![Fig. 5. Illustrating example on trace of average expected error covariance under different attack schedules when the sensor has energy constraint.](image)

**VII. Conclusion**

In this paper, we considered optimal attack scheduling against remote state estimation through a wireless channel. We proved that consecutive attacks maximize the expected average error covariance. We also showed that when the attacks are separated uniformly, the attack effect on the estimation quality is minimum. We further proposed the optimal attack schedules when a special intrusion detection mechanism in the estimator is available. We finally studied the optimal attack schedules when both the sensor and the attacker have energy constraints. It is interesting but challenging to find a closed-form solution for optimal attack scheduling over packet lossy network environment. This will be left as a future work. We will also formulate the infinite-horizon attack model and study the optimal attack schedule in the future. It is also interesting to consider optimal defensive strategies assuming that the sensor knows the existence of the attacker. We will further validate our results using some physical experiments, and consider optimal attack scheduling against feedback control and evaluating the corresponding effectiveness.
A. Proof of Property 3.1

Proof: Firstly, let us exploit mathematical induction method to prove 1) of Property 3.1. When $k = 1$, we have

$$Pr\{P_{s+k} = h^i(P)\} = \begin{cases} 1 - \alpha, & i = 0; \\ \alpha, & i = 1. \end{cases}$$

Assume 1) is true for $k = l$, i.e.,

$$Pr\{P_{s+l} = h^i(P)\} = \begin{cases} \alpha^i - \alpha^{i+1}, & i = 0, 1, \ldots, l-1; \\ \alpha^l, & i = l. \end{cases}$$

Then for $k = l+1$, we have

$$Pr\{P_{s+l+1} = h^i(P)\} = Pr\{P_{s+l+1} = h^i(P)\mid P_{s+l} = h^{i-1}(P)\}Pr\{P_{s+l} = h^{i-1}(P)\}$$

$$= \alpha Pr\{P_{s+l} = h^{i-1}(P)\}$$

$$= \begin{cases} \alpha^i - \alpha^{i+1}, & i = 1, 2, \ldots, l; \\ \alpha^{l+1}, & i = l+1. \end{cases}$$

And

$$Pr\{P_{s+l+1} = \overline{P}\} = 1 - \sum_{i=1}^{l+1} Pr\{P_{s+l+1} = h^i(P)\} = 1 - \alpha.$$

Thus 1) is true for $k = l+1$ and the proof of 1) completes.

Secondly, let us prove 2) of Property 3.1. When $k = 1$, we have

$$Pr\{P_{s+1} = h^j(P)\mid P_s = h^i(P)\} = \begin{cases} 1 - \alpha, & j = 0; \\ \alpha, & j = i + 1. \end{cases}$$

Assume 2) is true for $k = l$, i.e.,

$$Pr\{P_{s+l} = h^j(P)\mid P_s = h^i(P)\} = \begin{cases} \alpha^j - \alpha^{j+1}, & j = 0, \ldots, l-1; \\ \alpha^l, & j = i + l. \end{cases}$$

Then for $k = l+1$, we can obtain

$$Pr\{P_{s+l+1} = h^j(P)\mid P_s = h^i(P)\}$$

$$= Pr\{P_{s+l+1} = h^j(P)\mid P_{s+l} = h^{j-1}(P)\}Pr\{P_{s+l} = h^{j-1}(P)\mid P_s = h^i(P)\}$$

$$= \alpha Pr\{P_{s+l} = h^{j-1}(P)\mid P_s = h^i(P)\}$$

$$= \begin{cases} \alpha^j - \alpha^{j+1}, & j = 1, \ldots, l; \\ \alpha^{l+1}, & j = i + l + 1. \end{cases}$$

And

$$Pr\{P_{s+l+1} = \overline{P}\mid P_s = h^i(P)\} = 1 - \sum_{i=1}^{l+1} Pr\{P_{s+l+1} = h^i(P)\mid P_s = h^i(P)\} = 1 - \alpha.$$

Thus 2) is true for $k = l+1$ and the proof of 2) completes.
B. Proof of Property 3.3

Proof: 1) We have $J_a^{(m_2)} - J_a^{(m_1)} = \frac{1}{T} \sum_{k=m_1+1}^{m_2} \mathbb{E}[P_k] \geq 0$.

2) The system performance function $J$ with consecutive $n$ times attack can be written as

$$J_a^{(n)} = \frac{1}{T} \left\{ \sum_{k=1}^{n_1} \sum_{i=0}^{k-1} [(\alpha^i - \alpha^{i+1})h^i(\mathcal{F}) + \alpha^k h^k(\mathcal{F})] + (T - n)\mathcal{F} \right. \\
+ \left. \sum_{k=n_1+1}^{n} \sum_{i=0}^{n_1} \mathbb{E}[P_k | P_{n_1} = h^i(\mathcal{F})] Pr\{P_{n_1} = h^i(\mathcal{F})\} \right\},$$

and the function $J_a$ with attack schedule $\gamma^{n_1 \oplus n_2}$ is

$$J_a^{(n_1 \oplus n_2)} = \frac{1}{T} \left\{ \sum_{k=1}^{n_1} \sum_{i=0}^{k-1} [(\alpha^i - \alpha^{i+1})h^i(\mathcal{F}) + \alpha^k h^k(\mathcal{F})] + (T - n)\mathcal{F} \right. \\
+ \left. \sum_{k=n_1+1}^{n} \sum_{i=0}^{n_1} \mathbb{E}[P_k | P_{n_1} = \mathcal{F}] Pr\{P_{n_1} = \mathcal{F}\} \right\}.$$

By applying the statement 1) from Property 3.2, we have

$$\sum_{k=n_1+1}^{n} \sum_{i=0}^{n_1} \mathbb{E}[P_k | P_{n_1} = \mathcal{F}] Pr\{P_{n_1} = \mathcal{F}\} \geq \sum_{k=n_1+1}^{n} \sum_{i=0}^{n_1} \mathbb{E}[P_k | P_{n_1} = \mathcal{F}] Pr\{P_{n_1} = \mathcal{F}\} = \sum_{k=n_1+1}^{n} \mathbb{E}[P_k | P_{n_1} = \mathcal{F}],$$

Thus one has $J_a^{(n_1 \oplus n_2)} \leq J_a^{(n)}$.

3) The system performance function $J$ with consecutive $n$ times attack can be written as

$$J_a^{(n)} = \frac{1}{T} \left\{ \sum_{k=1}^{n_1} \sum_{i=0}^{k-1} [(\alpha^i - \alpha^{i+1})h^i(\mathcal{F}) + \alpha^k h^k(\mathcal{F})] + (T - n)\mathcal{F} \right. \\
+ \left. \sum_{j=1}^{s-1} \sum_{k=n_1+n_j+1}^{n_1+n_j+n_{j+1}} \sum_{i=0}^{n_1+n_j} \mathbb{E}[P_k | P_{n_1+\ldots+n_{j+1}} = h^i(\mathcal{F})] Pr\{P_{n_1+\ldots+n_{j+1}} = h^i(\mathcal{F})\} \right\},$$

and the function $J_a$ with attack schedule $\gamma^{n_1 \oplus n_2 \oplus \ldots \oplus n_s}$ is

$$J_a^{(n_1 \oplus n_2 \oplus \ldots \oplus n_s)} = \frac{1}{T} \left\{ \sum_{k=1}^{n_1} \sum_{i=0}^{k-1} [(\alpha^i - \alpha^{i+1})h^i(\mathcal{F}) + \alpha^k h^k(\mathcal{F})] + (T - n)\mathcal{F} \right. \\
+ \left. \sum_{j=1}^{s-1} \sum_{k=n_1+n_j+1}^{n_1+n_j+n_{j+1}} \sum_{i=0}^{n_1+n_j} \mathbb{E}[P_k | P_{n_1+\ldots+n_{j+1}} = \mathcal{F}] Pr\{P_{n_1+\ldots+n_{j+1}} = \mathcal{F}\} \right\}.$$

From statement 1) of Property 3.2, we can see that

$$\sum_{j=1}^{s-1} \sum_{k=n_1+n_j+1}^{n_1+n_j+n_{j+1}} \sum_{i=0}^{n_1+n_j} \mathbb{E}[P_k | P_{n_1+\ldots+n_{j+1}} = \mathcal{F}] Pr\{P_{n_1+\ldots+n_{j+1}} = \mathcal{F}\} \geq \sum_{j=1}^{s-1} \sum_{k=n_1+n_j+1}^{n_1+n_j+n_{j+1}} \sum_{i=0}^{n_1+n_j} \mathbb{E}[P_k | P_{n_1+\ldots+n_{j+1}} = \mathcal{F}] Pr\{P_{n_1+\ldots+n_{j+1}} = \mathcal{F}\} = \sum_{j=1}^{s-1} \sum_{k=n_1+n_j+1}^{n_1+n_j+n_{j+1}} \mathbb{E}[P_k | P_{n_1+\ldots+n_{j+1}} = \mathcal{F}].$$
Thus one has $J_a^{(m_1\oplus m_2\oplus\cdots\oplus m_k)} \leq J_a^{(n)}$.

4) It suffices to prove $J_a^{(m_1\oplus m_2)} \leq J_a^{((m_1+1)\oplus (m_2-1))}$, with $m_1 \geq m_2$. In fact,

$$J_a^{((m_1+1)\oplus (m_2-1))} - J_a^{(m_1\oplus m_2)} = \frac{1}{T}\{\mathbb{E}[P_{s+m_1+1}] - \mathbb{E}[P_{s+m_2}]\} \geq 0.$$

The last inequality is from statement 2) in Property 3.2.

C. Proof of Property 4.1

Proof: Alarm triggering condition $PRR \leq PRR_0$ is equivalent to $\sigma \leq \sigma_0$. Thus it is also equivalent to that the packets drop number $d_{\text{num}}$ in any time window is larger than $d = \tau - \tau_0$, i.e., $d_{\text{num}} > d$. In order to obtain the result, we prove by contradiction, i.e., $d_{\text{num}} \leq d$ is equivalent to $P_k \leq h^d(\overline{P})$, $k = 1, 2, \ldots, T$, which clearly holds.

D. Proof of Theorem 4.1

Proof: Firstly, if $d \geq n$, any $n$ times consecutive attack schedules satisfy the conditions $P_k \leq h^d(\overline{P})$, $k = 1, 2, \ldots, T$. Thus these schedules are optimal for Problem 4.1 when $d \geq n$.

Secondly, if $d < n$, from Property 4.1 and statements 1) and 3) of Property 3.3, one can see that the attacker can attack $d$ times consecutively at most. Then one has the following statements:

1) The total attack times $n$ should be divided into $m$ groups with $d$ times consecutive attack for each group and 1 group with $r$ times consecutive attack, where $n = d \cdot m + r$, $0 \leq r < d$.

2) Before and after $d$ times consecutive attack, the attacker has to stop $\sigma_0$ times at least.

Thus, we can construct the general structure of an optimal attack schedule as (8).

REFERENCES


