A Game-Theoretic Approach to Fake-Acknowledgment Attack on Cyber-Physical Systems

Yuzhe Li, Daniel E. Quevedo, Subhrakanti Dey, and Ling Shi

***Abstract*—A class of malicious attacks against remote state estimation in cyber-physical systems is considered. A sensor adopts an acknowledgement (ACK)-based online power schedule to improve the remote state estimation performance under limited resources. To launch malicious attacks, the attacker can modify the ACKs from the remote estimator and convey fake information to the sensor, thereby misleading the sensor with subsequent performance degradation. One feasible attack pattern is proposed and the corresponding effect on the estimation performance is derived analytically. Due to the ACKs being unreliable, the sensor needs to decide at each instant, whether to trust the ACK information or not and adapt the transmission schedule accordingly. In the meanwhile, there is also a tradeoff for the attacker between attacking and not attacking when the modification of ACKs is costly. To investigate the optimal strategies for both the sensor and the attacker, a game-theoretic framework is built and the equilibrium for both sides is studied.**

***Index Terms*—Cyber-physical systems, fake-ACK attack, game theory.**

I. Introduction

CYBER-PHYSICAL systems (CPS) have attracted much interest from both academic and industrial communities in the past few years. A wide spectrum of applications of CPS can be found in areas such as smart grid, intelligent transportation and environment monitoring [1] with the integration of sensing, control, communication and computation. In most CPS infrastructures, wireless sensors are key components with advantages such as low cost, easy installation, self-power [2], when compared with traditional wired sensors. Therefore, wireless sensors have been increasingly equipped in CPS to replace wired ones. New issues due to their special characteristics, however, arise naturally [3], [4].

The first issue is how to allocate the transmission energy of the sensors efficiently. Since most wireless sensors use on-board batteries which are difficult to replace, and these sensors are typically expected to work for several years without battery replacement, energy conservation is critical [5]–[7]. The work [8] designs multi-sensor scheduling and transmit power policies to adapt to the random wireless channel environment opportunistically. In [9], the authors consider the sensor scheduling problem of whether it should send its data to a remote estimator or not in the presence of communication energy constraints. The optimal offline sensor schedule is derived, where the term "offline" means that the sensor designs its strategy before the process starting, i.e., independent of the state of the process. In [10]–[12], the authors extend the result of [9] and propose a so-called "online" sensor power schedule by utilizing the real-time information of the process. One typical category of online information used here is the acknowledgement (ACK) packet from the remote estimator, indicating whether the data packet from the sensor arrives successfully or not. The ACK-based online power schedule gives rise to full-state information setups and only requires sending a 1-bit ACK packet. Not surprisingly, it improves the estimation performance significantly [11] compared with offline schedules.

Another issue when using wireless sensor modes is that, as the communication is through a wireless channel, these sensors are more vulnerable to cyber security threats, which leads to security and privacy concerns in CPS. In some safety-critical infrastructures, the wide use of CPS increases the risks and severities of such attacks. For example, as the largest and most complex CPS in the future, any severe attack on smart grids may have significant impacts on national economy and security or may even lead to loss of human life [13]. Therefore, the security issue is of fundamental importance to ensure the safe operation of CPS and are commonly investigated in the literature [14]–[17]. Cyber-Physical attacks can affect the integrity, availability and confidentiality in CPS [16]. Examples range from deception based attacks such as false-data-injection [18], sensor and actuator attacks, replay attacks [19], and also denial of service attacks [20]. Documented defence mechanisms can range from attack identification and detection, intrusion detection as well as physical watermarking of valid control signals [14].

Manuscript received July 6, 2015; revised February 22, 2016 and July 6, 2016; accepted September 4, 2016. Date of publication September 19, 2016; date of current version February 7, 2017. The work of L. Shi was supported by Hong Kong University of Science and Technology Caltech Partnership FP009. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Alejandro R. Ribeiro.

Y. Li is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada (e-mail: yuzhe2@ualberta.ca).

D. E. Quevedo is with the Department of Electrical Engineering, Paderborn University, Paderborn 33098, Germany (e-mail: dquevedo@ieee.org).

S. Dey is with the Department of Engineering Sciences, Uppsala University, Uppsala, Uppland SE 751 21, Sweden (e-mail: subhrakanti.dey@angstrom.uu.se).

L. Shi is with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (e-mail: eesling@ust.hk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSIPN.2016.2611446

In this context of CPS security, it should be noted that although the online power schedule proposed in [11] improves the estimation performance, the simple structure of the ACK packet employed therein makes it a more reachable (and likely) alternative for an adversary. By modifying the information on the arrivals of previous packets, the attacker may mislead the sensor and affect the estimation performance. Therefore, elucidating possible attack patterns and how they will affect the estimation performance are important to help us improve the design of CPS. This motivates us to investigate potential classes of malicious attacks against ACK-based remote state estimation based on the framework developed in [11]. In our previous work [21], a possible periodic attack pattern is proposed. The corresponding effect on the estimation performance under this attacking pattern is decided based on its capability to block ACKs. When the capability is quite limited, the attacker can block almost no ACKs and the online sensor schedule will operate normally. As a consequence, keeping the online schedule in such case will still guarantee a better performance than the offline schedule. On the other hand, when the attacker has sufficient capability and can block almost all the transmissions of the ACKs, it will make the estimation performance of the online sensor schedule under attack even worse than the offline schedule. In this case, the reasonable choice for the sensor is to adopt the offline schedule rather than keeping the online schedule. Since the proposed attack pattern in [21] will reduce the arrival rate of the ACKs significantly and the arrival rate of the ACKs without attacks is known [11], the sensor can distinguish whether the transmission of the ACKs are blocked by calculating the actual arrival rate and may choose to switch to offline schedule, hence it will no longer be affected by the attacker when the actual arrival rate is abnormal. In such cases where both the sensor and the attacker are more intelligent, it is worth investigating how the attacker can re-design their attacking pattern to avoid being detected. Similarly, when the sensor cannot detect the existence of the attacker any longer, it will need to decide whether or not to switch from online schedule to offline one without 100% confidence as in [21]. As a consequence, it is straightforward that, under certain conditions, the attacker may not launch the costly attacks since the sensor may adopt the offline schedule at the same time. The above line of thought motivates us to investigate the problem of the attack-switch game between the attacker and the sensor in a game-theoretic framework. The main contributions of the current work are summarized as follows:

1) We propose an analytical expression (Definition 4.1) to quantify feasible attacking patterns of the intelligent attacker without being detected by the sensor.
2) Instead of limiting the capability of the attacker described in [21], we extend the constraint model to assume that launching attacks are costly.
3) We build an attack-switch game between the attacker and the sensor in a game-theoretic framework when both sides involve and obtain the closed-form solution of the optimal actions for both sides in the state of Nash equilibrium.

The remainder of the work is organized as follows. Section II presents the system framework and states the main problem of interest. Section III provides some preliminaries about the optimal offline schedule and an online schedule. The analysis of our proposed feasible fake-ACK attack pattern is given in Section IV. The attack-switch game between the attacker and the sensor are investigated in Section V. Numerical examples and simulations are demonstrated in Section VI. Section VII provides some concluding remarks.

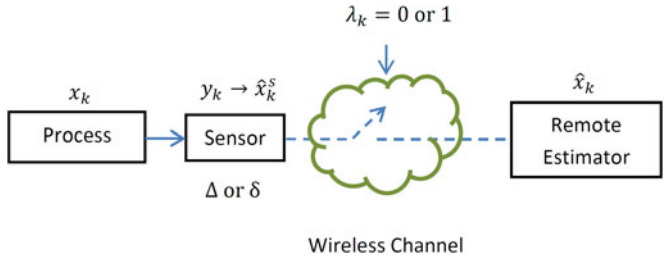


Fig. 1. System block diagram.

Notations: $\mathbb{Z}$ denotes the set of all integers and $\mathbb{N}$ the positive integers. $\mathbb{R}$ is the set of real numbers. $\mathbb{R}^n$ is the n-dimensional Euclidean space. $\mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$) is the set of n by n positive semi-definite matrices (and positive definite matrices). When $X \in \mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$), we write $X \geqslant 0$ (and $X > 0$) and $X \geqslant Y$ if $X - Y \in \mathbb{S}_+^n$. The curled inequality symbols $\succeq$ and $\preceq$ (and their strict forms $\succ$ and $\prec$) are used to denote generalized componentwise inequalities between vectors: for vectors $\mathbf{a} = [a_1, a_2, \ldots, a_n]', \mathbf{b} = [b_1, b_2, \ldots, b_n]'$, we write $\mathbf{a} \succeq \mathbf{b}$ if $a_i \geqslant b_i$, for $i = 1, 2, \ldots, n$. $\mathbf{1}$ denotes vector with all entries one. $\mathrm{Tr}(\cdot)$ is the trace of a matrix. The superscript $'$ stands for transposition. For functions g, h with appropriate domains, $g \circ h(x)$ stands for the function composition $g\big(h(x)\big)$, and $h^n(x) \triangleq h\big(h^{n-1}(x)\big)$, where $n \in \mathbb{N}$ and with $h^0(x) \triangleq x$. δ_{ij} is the Dirac delta function, i.e., δ_{ij} equals to 1 when $i = j$, and 0 otherwise. The notation $\mathbb{P}[\cdot]$ refers to probability and $\mathbb{E}[\cdot]$ to expectation. The subscript "k" is used as time index.

II. Problem Setup

A. System Model

Our interest lies in the security of a remote state estimation system as depicted in Fig. 1. Here we consider a general discrete-time linear time-invariant (LTI) process of the form:

$$x_{k+1} = Ax_k + w_k, \tag{1}$$

$$y_k^s = Cx_k + v_k, \tag{2}$$

where $k \in \mathbb{N}$, $x_k \in \mathbb{R}^{n_x}$ is the process state vector at time k, $y_k^s \in \mathbb{R}^{n_y}$ is the measurement taken by the sensor, $w_k \in \mathbb{R}^{n_x}$ and $v_k \in \mathbb{R}^{n_y}$ are zero-mean i.i.d. Gaussian noises with $\mathbb{E}[w_k w_j'] = \delta_{kj} Q$ $(Q \geqslant 0)$, $\mathbb{E}[v_k v_j{}'] = \delta_{kj} R$ $(R > 0)$, $\mathbb{E}[w_k v_j{}'] = 0\ \forall j, k \in \mathbb{N}$. The initial state x_0 is a zero-mean Gaussian random vector uncorrelated with w_k and v_k with covariance $\Pi_0 \geqslant 0$. The pair (A, C) is assumed to be detectable and $(A, Q^{1/2})$ is stabilizable.

We consider a so-called "smart sensor" as described in [22], which first locally estimates the state x_k based on all the measurements it has collected up to time k and then transmits its local estimate to the remote estimator.

Denote $\hat{x}_k^s$ and P_k^s as the sensor's local minimum mean-squared error (MMSE) estimate of the state x_k and the

corresponding error covariance:

$$\hat{x}_k^s = \mathbb{E}[x_k|y_1^s, y_2^s, \ldots, y_k^s], \tag{3}$$

$$\hat{P}_k^s = \mathbb{E}[(x_k - \hat{x}_k^s)(x_k - \hat{x}_k^s)'|y_1^s, y_2^s, \ldots, y_k^s], \tag{4}$$

which can be calculated by a standard Kalman filter.

As the estimation error covariance of the Kalman filter converges to a unique value from any initial condition ([23]), without loss of generality, we assume that the Kalman filter at the sensor side has entered the steady state and simplify our subsequent discussion by setting:

$$P_k^s = \overline{P},\ k \geqslant 1, \tag{5}$$

where $\overline{P}$ is the steady-state error covariance. For notational ease, we define the Lyapunov and Riccati operators $h, \tilde{g} : \mathbb{S}_+^n \to \mathbb{S}_+^n$ as:

$$h(X) \triangleq AXA' + Q,$$
$$\tilde{g}(X) \triangleq X - XC'[CXC' + R]^{-1}CX.$$

Then $\overline{P}$ is given by the unique positive semi-definite solution of $\tilde{g} \circ h(X) = X$ (see [23]).

B. Remote State Estimation

After obtaining $\hat{x}_k^s$, the sensor will transmit this vector as a data packet to the remote estimator. Due to fading and interference, random data drops will occur. As modelled in [9], [11], we assume that the sensor has two transmission power levels to choose from: when using a higher energy Δ, the packet will always arrive to the remote estimator; when using a lower energy δ, packets are dropped at the rate $1 - \lambda$, with $\lambda \in (0, 1)$. Note that we can also extend the result to multiple power levels or even continuous power levels in the future work. In the current work, we will start from the two-level model and aim to obtain some inspiring results. To simplify the following discussion, we denote the sensor power schedule as:

$$\theta = \{\gamma_1, \gamma_2, \ldots, \gamma_k, \ldots\}, \tag{6}$$

where $\gamma_k = 1$ or 0 represents that the sensor chooses energy Δ or δ, respectively, at time step k.

As a consequence, the transmission of $\hat{x}_k^s$ between the sensor and the remote estimator can be characterized by a binary random process $\{\lambda_k\}, k \in \mathbb{N}$:

$$\lambda_k = \begin{cases} 1, & \text{if } \hat{x}_k^s \text{ arrives at time } k, \\ 0, & \text{otherwise (regarded as dropout).} \end{cases}$$

Therefore, we have:

$$\mathbb{P}[\lambda_k = 1] = \begin{cases} 1, & \text{if } \gamma_k = 1, \\ \lambda, & \text{if } \gamma_k = 0, \end{cases} \tag{7}$$

and

$$\mathbb{P}[\lambda_k = 0] = 1 - \mathbb{P}[\lambda_k = 1]. \tag{8}$$

Denote $\hat{x}_k$ and P_k as the remote estimator's own MMSE state estimate and the corresponding error covariance based on all the sensor data packets received up to time step k. The remote state estimate $\hat{x}_k$ obeys the recursion:

$$\hat{x}_k = \begin{cases} \hat{x}_k^s, & \text{if } \lambda_k = 1, \\ A\hat{x}_{k-1}, & \text{if } \lambda_k = 0. \end{cases} \tag{9}$$

The corresponding state estimation error covariance P_k satisfies:

$$P_k = \begin{cases} \overline{P}, & \text{if } \lambda_k = 1, \\ h(P_{k-1}), & \text{if } \lambda_k = 0. \end{cases} \tag{10}$$

Intuitively, higher transmission power leads to better estimation performance. However, in practice, the sensor has a limited energy budget, which motivates us to consider the following optimization problem for the sensor:

Problem 2.1:

$$\min_{\theta}\ J(\theta) \triangleq \limsup_{T\to\infty} \frac{1}{T} \sum_{k=1}^{T} \mathrm{Tr}\left(\mathbb{E}[P_k]\right),$$

$$\text{s.t. } \Phi(\theta) \triangleq \limsup_{T\to\infty} \frac{1}{T} \sum_{k=1}^{T} \mathbb{E}\left[\gamma_k\Delta + (1-\gamma_k)\delta\right] \leqslant \Psi,$$

where Ψ is the average energy constraint for the sensor.

Remark 2.2: We assume that Δ, δ, and Ψ are all positive rational numbers satisfying $\delta < \Psi < \Delta$. Note that by setting $\lambda = 0$, the two-level power model can be regarded as a generalization of the sensor scheduling problem of sending the data packet or not.

The above problem was already considered in [21]. If a malicious attacker exists, however, the situation will become more involved, motivating our current work. For the attacker, the aim is to deteriorate the estimation quality, i.e., maximize the cost function $J(\theta)$ by choosing an appropriate attack strategy. We will describe the revised objective and the constraint model with more details in Sections IV and V.

III. Power Schedules Without Attacks

In this section, we will revisit some existing results about optimal offline schedules and an ACK-based online power schedule when there is no attacker.

A. Optimal Offline Schedule

When the sensor designs its power schedule without utilizing any online information, the optimal solution to the problem stated in Section II is provided by the following result:

Theorem 3.1 (Optimal Offline Schedule [9]): Suppose that p and q are two co-prime integers satisfying $\frac{p}{q} = \frac{\Psi-\delta}{\Delta-\delta}$. Then the optimal offline power schedule $\theta_{\text{off}}^{\star}$ to Problem 2.1 over a period q can be constructed in the following form:

$$\underbrace{(1\ \underbrace{0\cdots0}_{s_0+1\text{times}})\cdots(1\ \underbrace{0\cdots0}_{s_0+1\text{times}})}_{n\text{times}}\underbrace{(1\underbrace{0\cdots0}_{s_0\text{times}})\cdots(1\underbrace{0\cdots0}_{s_0\text{times}})}_{m\text{times}}$$

where 1 and 0 denote the designed value for γ_k in (6), $m = q - p(s_0+1)$, $n = p(s_0+2) - q$, and s_0 is the largest integer such that $s_0 \leqslant \frac{q}{p} - 1$.

Under the above optimal offline schedule $\theta^{\star}_{\text{off}}$, we have the following closed-form results about the corresponding energy consumption and estimation performance.

Proposition 3.2 ([9]): When $\theta^{\star}_{\text{off}}$ is used, the average energy cost is given by

$$\Phi(\theta^{\star}_{\text{off}}) = \frac{(m+n)\Delta + (ms_0 + ns_0 + m)\delta}{ms_0 + ns_0 + 2m + n} = \Psi,$$

and

$$\begin{aligned} J(\theta^{\star}_{\text{off}}) = & \frac{1}{m(s_0+2) + n(s_0+1)} \\ & \cdot \operatorname{Tr}\Big\{ m\big[1 + \lambda(s_0+1)\big]\overline{P} + n\big[1 + \lambda s_0)\big]\overline{P} \\ & + m \sum_{i=1}^{s_0+1} \big[1 + \lambda(s_0 + 1 - i)\big](1-\lambda)^i h^i(\overline{P}) \\ & + n \sum_{i=1}^{s_0} \big[1 + \lambda(s_0 - i)\big](1-\lambda)^i h^i(\overline{P}) \Big\}. \end{aligned} \quad (11)$$

B. Online Power Schedule

The offline power schedules given above are designed before the system is running without using the realtime measurement or state information. In [12], the authors showed that the utilization of online information can improve the estimation performance while requiring less energy consumption. To further improve the estimation performance, an online power schedule θ_{on} based on the ACKs from the remote estimator was recently proposed in [11] as follows: the remote estimator generates 1-bit ACKs ($= \lambda_k$) to indicate whether the data packet arrived successfully or not. An event-detector at the remote estimator's side then collects and stores the ACKs in its memory. Without loss of generality, assume the sensor uses Δ at the first time step. The memory is set to $11, \ldots, 11$ initially and the detector randomly chooses to activate z_0-bit memory with a given probability μ, or (z_0+1)-bit memory with probability $\eta = 1 - \mu$. At every time step, the memory shifts all bits one bit to the Most Significant Bit (MSB) direction with the existing MSB being deleted and the incoming ACK stored in the Least Significant Bit (LSB). When the memory becomes $00, \ldots, 00$, the detector sends an aggregated-ACK to inform the sensor to use high power in the following time step. In the meanwhile, the memory is set to $11, \ldots, 11$ again (see Fig. 2).

Remark 3.3: Note that the design of the parameter μ in the online sensor schedule θ_{on} is to tune the activated memory length between z_0 and $z_0 + 1$ in the event-detector to satisfy the energy constraint. When the energy constraint is in simple fraction form, e.g., $\frac{1}{2}$ or $\frac{1}{3}$, a fixed length activated memory with z_0 is sufficient. Without loss of generality, we shall assume that the event-detector adopts a fixed activated memory with length z_0 to facilitate the discussion and simplify the notation below.

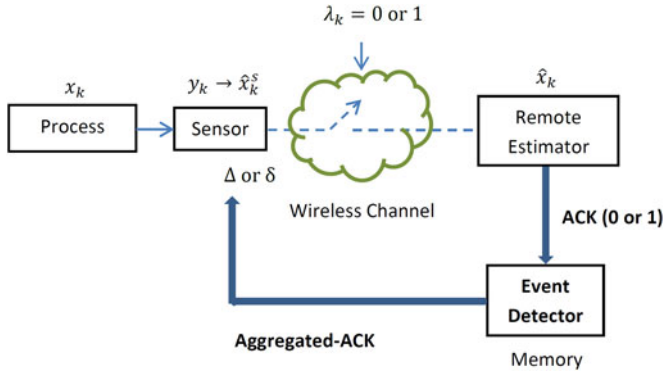


Fig. 2. System architecture under online sensor schedule.

Under the online schedule θ_{on} described above, the corresponding estimation performance is characterised by the following theorem:

Theorem 3.4 (Theorem 4.5 in [11]): When using the online power schedule θ_{on},

$$J(\theta_{\text{on}}) = \frac{\lambda}{1 - (1-\lambda)^{z_0+1}} \cdot \operatorname{Tr}\left[\sum_{i=0}^{z_0} (1-\lambda)^i h^i(\overline{P}) \right]. \quad (12)$$

Compared with the optimal offline schedule in Section III-A and under a given energy constraint , the online schedule θ_{on} gives a better estimation performance (see Theorem 5.3 of [11]): $J(\theta_{\text{on}}) < J(\theta^{\star}_{\text{off}})$.

IV. Feasible Fake-Acknowledgement Attack

As stated before, the ACK-based online power schedule can improve the estimation performance compared with the offline schedule. However, the simple structure of the 1-bit aggregated-ACK packet makes it a more reachable (and likely) alternative for an adversary, under both integrity attacks and DoS attacks. In this section, we propose a possible attack pattern for the attacker and investigate the corresponding effect on the estimation performance analytically.

A. Feasible Attacks

In our previous work [21], a periodic attack pattern is investigated. The attack pattern in [21], denoted as ω_c, requires an extra counter to keep track of the accumulated number of attacks. Interestingly, as the arrival rate of the aggregated-ACKs without attacks is known in [11], the sensor may check the actual arrival rate of the aggregated-ACKs to ensure the normal operation of the system. As a result, the sensor may aim to switch to an offline schedule and no longer be affected by the attacker when the actual arrival rate is abnormal.

The above discussion motivates the attacker to design its attacking pattern to maintain the original arrival rate. We assume that the verification conducted by the sensor is only to check the average arrival rate of the aggregated-ACKs. As a consequence, the attacker will adopt the following so-called "feasible" attack pattern which keeps the average arrival rate of the aggregated-ACKs.

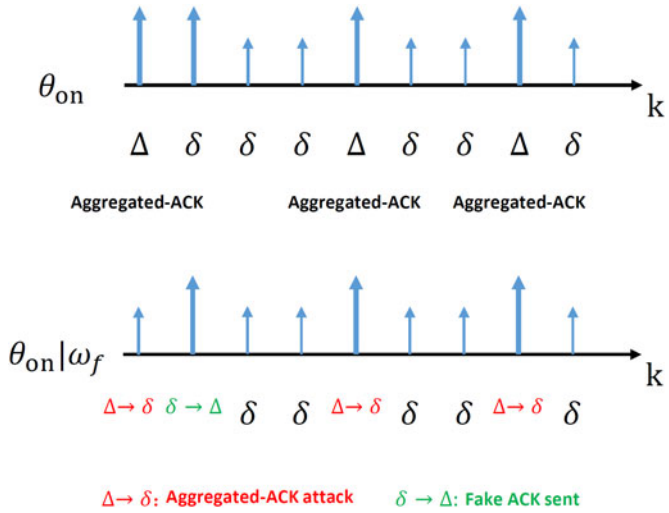


Fig. 3. Comparison between θ_{on} and $\theta_{\text{on}}|\omega_f$.

Definition 4.1: Define the average arrival rate of the aggregated-ACKs as $\Gamma \triangleq \lim_{T\to+\infty} \frac{t_0}{T}$, where t_0 is the number of occurrences that the sensor receives aggregated-ACKs from time step 1 to T.

A fake-ACK attack pattern for the attacker ω is "feasible" if the average arrival rate of the aggregated-ACKs under ω remains unchanged from the one without attacks, i.e.,

$$\Gamma(\theta_{\text{on}}|\omega) = \Gamma(\theta_{\text{on}}|\text{no attack}). \tag{13}$$

Remark 4.2: In the context of a two-player static game, it is reasonable that the sensor will decide its transmission scheme before the process begin and may not verify the data or only conduct simple detection procedures for the received aggregated-ACKs. In a practical setup, the sensor may only examine the arrival rate of aggregated-ACKs by choosing a window size T sufficiently enough to approximate the exact value of Γ and compare it with the theoretic value. We assume that other statistics of the arrival sequence of aggregated-ACKs will not be checked due to energy saving concerns.

Based on Definition 4.1, we propose the following attack pattern ω_f: when the aggregated-ACK is sent as the event happens, the attacker simply adopts an DoS attack to prevent the transmission of the packet. In order to maintain constant arrival rate of aggregated-ACKs, the attacker will send fake aggregated-ACKs to the sensor with the same probability p_0 at every time step when there is no aggregated-ACK from the event detector. The value of p_0 is chosen to meet (13), which will be discussed later in Proposition 4.4.

Example 4.3: A simple example is provided to illustrate how this attack pattern works. Assume that $z_0 = 2$. One possible realization and comparison between the online schedule θ_{on} without attack and the one under attack $\theta_{\text{on}}|\omega_f$ is shown in Fig. 3 (The long arrows represent the arrival packets while the short ones are for the dropped packets.). In the realization of θ_{on} without attack, the second and the third aggregated-ACK are sent due to two ($z_0 = 2$) consecutive packet losses. When there is an attacker following the attack pattern ω_f, it will attack all the original aggregated-ACKs, and randomly send fake ACKs with probability p_0 at instants when there is no aggregated-ACK from the event detector (e.g., at the second time step in $\theta_{\text{on}}|\omega_f$).

B. Performance Analysis

Denote the estimation performance of θ_{on} under the proposed attack pattern as $J(\theta_{\text{on}}|\omega_f)$. We will investigate the analytical form of $J(\theta_{\text{on}}|\omega_f)$ in the sequel.

Note that due to the recursion (10), the covariance P_k takes values in the infinitely countable set $\{\overline{P}, h(\overline{P}), h^2(\overline{P}), \ldots\}$ and only depends on the state of previous time step, i.e., P_{k-1}. Therefore, we have a simple expression for P_k as:

$$P_k = h^{\tau_k}(\overline{P}),$$

where $\tau_k \in \mathbb{N}$ is denoted as the holding time since the most recent time when the remote estimator successfully received the data from the sensor:

$$\tau_k \triangleq k - \max_{1\leqslant t\leqslant k}\{t : \lambda_t = 1\}. \tag{14}$$

Define $\mathcal{S}_k \triangleq \tau_k + 1$ as the state of the estimation process at time step k. It is easy to verify that τ_k satisfies the following Markovian recursion:

$$\tau_k = \begin{cases} 0, & \text{if } \lambda_k = 1, \\ \tau_{k-1} + 1, & \text{if } \lambda_k = 0, \end{cases} \tag{15}$$

and the process $\{\mathcal{S}_k\}$ constitutes a countably infinite stationary Markov chain. Define the corresponding state transition probability matrix with countably infinite dimensions as:

$$\mathcal{T}_s \triangleq \{T_{\text{ij}}\}, T_{\text{ij}} = \mathbb{P}[S_{k+1} = j | S_k = i].$$

Based on the mechanism of the online sensor schedule θ_{on} and the attack pattern ω_f, we can derive an expression for T_{ij} as follows:

1) At time step $k+1$, when the memory satisfies the triggering condition, i.e., $\tau_k \mod z_0 = 0$ ($i - 1 \mod z_0 = 0$) and $\tau_k \neq 0$, the aggregated-ACK will be sent and the attack will be launched to block the transmission. Then the sensor will use lower power δ (i.e., $\gamma_{k+1} = 0$). From (7) and (8), we have

$$T_{\text{ij}} = \begin{cases} \lambda, & \text{if } j = 1, \\ 1-\lambda, & \text{if } j = i+1, \\ 0, & \text{otherwise;} \end{cases}$$

2) At time step $k+1$, when $\tau_k \mod z_0 \neq 0$ ($i - 1 \mod z_0 \neq 0$) or $\tau_k = 0$, the aggregated-ACK will not be sent and the fake ACK will be sent with probability p_0. Then the sensor will use higher power Δ (i.e., $\gamma_{k+1} = 1$) with probability p_0 and lower power δ (i.e., $\gamma_{k+1} = 0$) with prababilty $1 - p_0$. Similarly, we have

$$T_{\text{ij}} = \begin{cases} p_0 + \lambda(1-p_0), & \text{if } j = 1, \\ (1-\lambda)(1-p_0), & \text{if } j = i+1, \\ 0, & \text{otherwise.} \end{cases}$$

From the above discussion, we can obtain the expression of the transition matrix $\mathcal{T}_s$, which will be in a periodic pattern. An illustrative example of $\mathcal{T}_s$ when $z_0 = 2$ is provided in equation (16) are shown at the bottom of this page.

Based on well-established ergodic Markov chain theory [24], $\{S_k\}$ has a stationary probability distribution, which is denoted as:

$$\Pi = [\pi_0, \pi_1, \pi_2, \ldots]', \pi_i \triangleq \mathbb{P}[\tau_k = i].$$

To calculate the stationary probability distribution, we need to solve the following equations:

$$\begin{cases} \mathcal{T}_s \Pi = \Pi, \\ \sum_{i=0}^{+\infty} \pi_i = 1. \end{cases} \tag{17}$$

Though the dimensions of Π and $\mathcal{T}_s$ are infinite, due to the periodic property of $\mathcal{T}_s$, we can solve (17) as follows.

Based on the expression of T_{ij} and the illustration in (16), there are only two non-zero elements in each column of $\mathcal{T}_s$: the first one is in the first row of each column and the second one is in the $(i+1)$-th row for the i-th column. Therefore, the first equation in (17) gives the recursive relations for $i > 0$:

$$\pi_{i+1} = \begin{cases} (1-\lambda)(1-p_0)\pi_i, & \text{if } i \mod z_0 \neq 0, \\ (1-\lambda)\pi_i, & \text{if } i \mod z_0 = 0. \end{cases}$$

Then it is easy to derive the general form of π_i for $i > 0$ as:

$$\pi_i = (1-\lambda)^i (1-p_0)^{i-j} \pi_0, \tag{18}$$

where $j = \lfloor \frac{i-1}{z_0} \rfloor$.

Thus replacing (18) into the second equation of (17) gives:

$$\pi_0 + \sum_{i=0}^{+\infty} \left[(1-\lambda)^{z_0}(1-p_0)^{z_0-1}\right]^i \left(\sum_{j=1}^{z_0} (1-\lambda)^j (1-p_0)^j\right) \pi_0 = 1,$$

and we can obtain:

$$\pi_0 = \frac{[1-(1-\lambda)(1-p_0)]\left[1-(1-\lambda)^{z_0}(1-p_0)^{z_0-1}\right]}{1-(1-\lambda)^{z_0}(1-p_0)^{z_0-1} + p_0(1-\lambda)^{z_0+1}(1-p_0)^{z_0}}. \tag{19}$$

On the other hand, when ω_f is feasible, i.e.,

$$\Gamma(\theta_{\text{on}}|\omega_f) = \Gamma(\theta_{\text{on}}|\text{no attack}),$$

the probability π_0 can be calculated in an alternative way as:

$$\begin{aligned} \pi_0 &= \mathbb{P}[\Delta|\omega_f] + \lambda \mathbb{P}[\delta|\omega_f] \\ &= \Gamma(\theta_{\text{on}}|\omega_f) + \lambda\big(1 - \Gamma(\theta_{\text{on}}|\omega_f)\big) \\ &= \Gamma(\theta_{\text{on}}|\text{no attack}) + \lambda\big(1 - \Gamma(\theta_{\text{on}}|\text{no attack})\big). \end{aligned}$$

Since $\Gamma(\theta_{\text{on}}|\text{no attack})$ is given as (see [11]):

$$\Gamma(\theta_{\text{on}}|\text{no attack}) = \frac{\lambda(1-\lambda)^{z_0}}{1-(1-\lambda)^{z_0+1}},$$

we have

$$\pi_0 = \frac{\lambda}{1-(1-\lambda)^{z_0+1}}. \tag{20}$$

The closed-form expressions for the stationary distribution of the state are given by (20) and (18). The estimation performance of θ_{on} under the proposed fake-ACK attack ω_f is thus given by[1]:

$$\begin{aligned} J(\theta_{\text{on}}|\omega_f) &= \limsup_{T\to\infty} \frac{1}{T} \sum_{k=1}^{T} \text{Tr}\left(\mathbb{E}[P_k]\right) \\ &= \limsup_{k\to\infty} \text{Tr}\left(\mathbb{E}[P_k]\right) = \sum_{i=0}^{+\infty} \pi_i \text{Tr}\Big(h^i(\overline{P})\Big). \end{aligned} \tag{21}$$

In order to choose the value of p_0 to meet the feasible attack pattern condition (13), we have the following result.

Proposition 4.4: The proposed attack pattern ω_f is feasible, i.e., $\Gamma(\theta_{\text{on}}|\omega_f) = \Gamma(\theta_{\text{on}}|\text{no attack})$, when p_0 satisfies the following condition:

$$p_0\left[1 - \frac{(1-\lambda)^{z_0}(1-p_0)^{z_0-2}}{1-(1-\lambda)^{z_0}(1-p_0)^{z_0-1}}\pi_0\right] = \frac{\lambda(1-\lambda)^{z_0}}{1-(1-\lambda)^{z_0+1}}. \tag{22}$$

Proof: As the fake-ACK is sent with probability p_0 only when no aggregated-ACK is sent from the event detector,

[1]Note that a necessary and sufficient condition for boundedness of $J(\theta_{\text{on}}|\omega_f)$ is given by $\rho(A)(1-\lambda)(1-p_0) < 1$, where $\rho(A)$ is the spectral radius of A.

$$\mathcal{T}_s = \begin{bmatrix} p_0+\lambda(1-p_0) & p_0+\lambda(1-p_0) & \lambda & p_0+\lambda(1-p_0) & \lambda & p_0+\lambda(1-p_0) & \lambda & \cdots \\ (1-\lambda)(1-p_0) & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & (1-\lambda)(1-p_0) & 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1-\lambda & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & (1-\lambda)(1-p_0) & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & 1-\lambda & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & 0 & (1-\lambda)(1-p_0) & 0 & \cdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 1-\lambda & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix} \tag{16}$$

we have

$$\Gamma(\theta_{\text{on}}|\omega_f) = p_0\left(1-\sum_i^{+\infty}\pi_{iz_0}\right) = p_0\left(1-\sum_i^{+\infty}\pi_{iz_0}\right)$$
$$= p_0\left[1-\frac{(1-\lambda)^{z_0}(1-p_0)^{z_0-2}}{1-(1-\lambda)^{z_0}(1-p_0)^{z_0-1}}\pi_0\right].$$

Since $\Gamma(\theta_{\text{on}}|\text{no attack}) = \frac{\lambda(1-\lambda)^{z_0}}{1-(1-\lambda)^{z_0+1}}$, the value of p_0 to meet the feasible attack pattern condition is obvious given by solving (22).

V. Attack-Switch Game Between the Attacker and the Sensor

In this section, we formulate an attack-switch game between the attacker and the sensor and investigate the optimal responses for both sides when they involve in this game-theoretic framework. We will show that the equilibrium of the sensor-attacker game will have different forms based on the capability of the attacker.

A. Game-Theoretic Framework

As stated in [21], the proportion of aggregated-ACKs that can be attacked under the attacking pattern ω_c will determine the effect on the estimation performance. When the capability is quite limited, the attacker can block almost no aggregated-ACK and the online sensor schedule will operate normally. As a consequence, keeping the online schedule in such case will still guarantee a better performance than the offline schedule $\theta^\star_{\text{off}}$. On the other hand, when the attacker has sufficient capability and can block almost all the transmissions of the aggregated-ACKs, it will result in the sensor using the low power δ within the entire time-horizon and the estimation performance of the online sensor schedule under attack ω_c is proved to be even worse than the offline schedule ([21]). In such cases, a reasonable choice for the sensor is to adopt the offline schedule rather than keeping the online schedule.

We assume that to detect the existence of the attacker, the sensor compares the arrival rate of aggregated-ACKs with the theoretical arrival rate. The would enable the sensor to estimate the capability of the attacker and decide whether to switch from the online schedule to the offline schedule.

However, when the attack pattern proposed in our current work, ω_f, is adopted, as the feasible pattern has $\Gamma(\theta_{\text{on}}|\omega) = \Gamma(\theta_{\text{on}}|\text{no attack})$, the sensor cannot detect the existence of the attacker any longer. Now the sensor will need to decide whether or not to switch from online schedule to offline one without 100% confidence as in [21]. On the other hand, instead of limiting the capability of the attacker, we extend the constraint model to assume that launching attacks are costly (the original capability model in [21] can be regarded as a special case of our present formulation with infinite cost on extra attacks). In such a situation, it is straightforward that, under certain conditions, the attacker may not launch the (costly) attacks since the sensor may adopt the offline schedule at the same time. In the following part, we aim to investigate the optimal strategies for both the sensor and the attacker simultaneously in such a situation. To be more precise, we next summarize the elements of such two-player game as follows:

1) *Player*: The sensor and the attacker;
2) *Action*: As discussed before, the sensor needs to decide whether it adopts the online schedule θ_{on} (denoted as action $\sigma(1)$) or switches to the offline schedule $\theta^\star_{\text{off}}$ (denoted as action $\sigma(2)$). Similarly, the attacker needs to choose the attack pattern ω_f (denoted as action $\epsilon(1)$) or not to attack (denoted as action $\epsilon(2)$);
3) *Payoff*: The objective of the sensor is to minimize the trace of the expected average state estimation error covariance. Define the payoff for the sensor as:

$$V_S(\sigma,\epsilon) \triangleq -\limsup_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}\text{Tr}\left(\mathbb{E}[P_k]\right),$$

hence the sensor seeks to maximize the payoff $V_S(\sigma,\epsilon)$. Based on the discussion before, we have:

$$\begin{cases} V_S\big(\sigma(1),\epsilon(1)\big) = -J(\theta_{\text{on}}|\omega_f), \\ V_S\big(\sigma(1),\epsilon(2)\big) = -J(\theta_{\text{on}}), \\ V_S\big(\sigma(2),\epsilon(1)\big) = -J(\theta^\star_{\text{off}}), \\ V_S\big(\sigma(2),\epsilon(2)\big) = -J(\theta^\star_{\text{off}}), \end{cases} \tag{23}$$

where $J(\theta_{\text{on}}|\omega_f)$, $J(\theta_{\text{on}})$ and $J(\theta^\star_{\text{off}})$ are given in (21), (12) and (11), respectively. As for the attacker, its objective is essentially the opposite except for taking the attacking cost into account. Accordingly, define the payoff for the attacker as:

$$V_A(\sigma,\epsilon) \triangleq \limsup_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}\text{Tr}\left(\mathbb{E}[P_k]\right) - \Gamma(\theta_{\text{on}}|\omega_f)\Omega,$$

where Ω represents the cost of launching one attack in ω_f. Similarly, we have

$$\begin{cases} V_A\big(\sigma(1),\epsilon(1)\big) = J(\theta_{\text{on}}|\omega_f) - \Gamma(\theta_{\text{on}}|\omega_f)\Omega, \\ V_A\big(\sigma(1),\epsilon(2)\big) = J(\theta_{\text{on}}), \\ V_A\big(\sigma(2),\epsilon(1)\big) = J(\theta^\star_{\text{off}}) - \Gamma(\theta_{\text{on}}|\omega_f)\Omega, \\ V_A\big(\sigma(2),\epsilon(2)\big) = J(\theta^\star_{\text{off}}). \end{cases} \tag{24}$$

B. Nash Equilibrium

To analyze the optimal actions for both sides in the state of equilibrium, we first recall the following concepts on Nash Equilibrium [25], [26].

Definition 5.1: A player's *strategy* refers to the players's plan or policy that will determine all the actions to take during the game.

A *pure strategy* provides a complete definition of how a player will play a game.

A *mixed strategy* is an assignment of probability to each pure strategy in the strategy set, which allows the player to randomly select a pure strategy.

A *strategy profile* (strategy combination) is a set of strategies for each player which fully specifies all actions in a game.

Remark 5.2: We can regard the pure strategy as a degenerate case of the mixed strategy, where the particular pure strategy

is selected with probability 1 and every other strategy with probability 0.

Definition 5.3: If in a game, each player has chosen a strategy and no player can benefit by changing his own strategy while the other players keep theirs unchanged, then the current *strategy profile* constitutes a Nash equilibrium.

Define the best response for one player as the strategy which gives the most payoff, given other players' strategies. Then the Nash equilibrium is the point at which each player in a game has selected the best response (or one of the best responses) to the other players' strategies. To be more specific, a Nash equilibrium in this attack-switch game is a pair of strategies $(\sigma^\star, \epsilon^\star)$ such that:

$$V_S(\sigma^\star, \epsilon^\star) \geqslant V_S(\sigma, \epsilon^\star),\ \forall \sigma,\ V_A(\sigma^\star, \epsilon^\star) \geqslant V_A(\sigma^\star, \epsilon),\ \forall \epsilon.$$

In some cases, there may exist no Nash equilibrium in terms of purely using the available actions i.e., pure strategy Nash equilibrium. In [25], Nash defined the mixed strategy Nash equilibrium, which also include the pure strategy Nash equilibrium as a special case.

Theorem 5.4 ([25]): For any game with a finite set of actions, there exists at least one mixed strategy Nash equilibrium in the game.

From the Definition 5.3, to seek the maximization of their payoffs whilst being aware of the existence of their opponents, it is easy to conclude that the optimal responses for both the sensor and the attacker constitute a Nash equilibrium. Simple analysis (e.g., based on (24), when the sensor choose $\sigma(1)$, the attacker will choose $\epsilon(1)$ if Ω is small; when the sensor choose $\sigma(2)$, the attacker will choose $\epsilon(2)$) reveals that there may not always exist a pure strategy Nash equilibrium. However, due to the finite action sets for both sides, a mixed strategy Nash equilibrium exists. We have the following conclusion about the optimal responses for both sides.

Theorem 5.5: When the attacker adopts feasible an attacking pattern as defined in Definition 4.1, the optimal responses for the sensor and the attacker $(\sigma^\star, \epsilon^\star)$ exist in the form of a mixed strategy Nash equilibrium.

1) When $\Gamma(\theta_{\text{on}}|\omega_f)\Omega < J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})$, $(\sigma^\star, \epsilon^\star)$ is given by:

$$\sigma^\star = \begin{cases} \sigma(1),\ \text{with probability} \dfrac{\Gamma(\theta_{\text{on}}|\omega_f)\Omega}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \\ \sigma(2),\ \text{with probability} 1 - \dfrac{\Gamma(\theta_{\text{on}}|\omega_f)\Omega}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \end{cases}$$

and

$$\epsilon^\star = \begin{cases} \epsilon(1),\ \text{with probability} \dfrac{J(\theta^\star_{\text{off}}) - J(\theta_{\text{on}})}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \\ \epsilon(2),\ \text{with probability} 1 - \dfrac{J(\theta^\star_{\text{off}}) - J(\theta_{\text{on}})}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \end{cases}$$

with the payoff for both sides given by:

$$V_S(\sigma^\star, \epsilon^\star) = -J(\theta^\star_{\text{off}}),$$

and

$$V_A(\sigma^\star, \epsilon^\star) = J(\theta^\star_{\text{off}}) - \Gamma(\theta_{\text{on}}|\omega_f)\Omega \frac{J(\theta^\star_{\text{off}}) - J(\theta_{\text{on}})}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})};$$

2) When $\Gamma(\theta_{\text{on}}|\omega_f)\Omega \geqslant J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})$, one obtains the pure strategy $(\sigma^\star, \epsilon^\star) = \big(\sigma(1), \epsilon(2)\big)$, with the payoff for both sides given by:

$$V_S(\sigma^\star, \epsilon^\star) = -J(\theta_{\text{on}}),\ V_A(\sigma^\star, \epsilon^\star) = J(\theta_{\text{on}}).$$

Proof: To calculate the mixed strategy Nash equilibrium, suppose that the mixed strategy for the sensor is $\sigma_{\text{mix}} = \big(\mathbb{P}[\sigma(1)], \mathbb{P}[\sigma(2)]\big)$, i.e.,

$$\sigma_{\text{mix}} = \begin{cases} \sigma(1), & \text{with probability} \mathbb{P}[\sigma(1)], \\ \sigma(2), & \text{with probability} \mathbb{P}[\sigma(2)], \end{cases}$$

where $\mathbb{P}[\sigma(2)] = 1 - \mathbb{P}[\sigma(1)]$. Similarly, the mixed strategy for the attacker is assumed to be $\epsilon_{\text{mix}} = \big(\mathbb{P}[\epsilon(1)], \mathbb{P}[\epsilon(2)]\big)$. Given the attacker's strategy ϵ_{mix}, the expected payoff for the sensor under σ_{mix} is:

$$\begin{aligned} V_S(\sigma_{\text{mix}}, \epsilon_{\text{mix}}) = {} & \mathbb{P}[\sigma(1)](V_S(\sigma(1), \epsilon(1))\mathbb{P}[\epsilon(1)] \\ & + V_S\big(\sigma(1), \epsilon(2)\big)\mathbb{P}[\epsilon(2)]) \\ & + \mathbb{P}[\sigma(2)](V_S(\sigma(2), \epsilon(1))\mathbb{P}[\epsilon(1)] \\ & + V_S(\sigma(2), \epsilon(2))\mathbb{P}[\epsilon(2)]). \end{aligned}$$

According to (23), to maximize $V_S(\sigma_{\text{mix}}, \epsilon_{\text{mix}})$, the best response for the sensor can be calculated as:

$$\mathbb{P}^\star[\sigma(1)|\epsilon_{\text{mix}}] = \begin{cases} 1, & \text{if } \mathbb{P}[\epsilon(1)] < \dfrac{J(\theta^\star_{\text{off}}) - J(\theta_{\text{on}})}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \\ 0, & \text{if } \mathbb{P}[\epsilon(1)] > \dfrac{J(\theta^\star_{\text{off}}) - J(\theta_{\text{on}})}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \\ [0,1], & \text{if } \mathbb{P}[\epsilon(1)] = \dfrac{J(\theta^\star_{\text{off}}) - J(\theta_{\text{on}})}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \end{cases} \tag{25}$$

and

$$\mathbb{P}^\star[\sigma(2)|\epsilon_{\text{mix}}] = 1 - \mathbb{P}^\star[\sigma(1)|\epsilon_{\text{mix}}]. \tag{26}$$

Following the same procedure, we can calculate the best response for the attacker based on the value of $\Gamma(\theta_{\text{on}}|\omega_f)\Omega$.

1) When $\Gamma(\theta_{\text{on}}|\omega_f)\Omega < J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})$, i.e., the cost of launching attack is relatively small, we have:

$$\mathbb{P}^\star[\epsilon(1)|\sigma_{\text{mix}}] = \begin{cases} 1, & \text{if } \mathbb{P}[\sigma(1)] > \dfrac{\Gamma(\theta_{\text{on}}|\omega_f)\Omega}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \\ 0, & \text{if } \mathbb{P}[\sigma(1)] < \dfrac{\Gamma(\theta_{\text{on}}|\omega_f)\Omega}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \\ [0,1], & \text{if } \mathbb{P}[\sigma(1)] = \dfrac{\Gamma(\theta_{\text{on}}|\omega_f)\Omega}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \end{cases} \tag{27}$$

and

$$\mathbb{P}^\star[\epsilon(2)|\sigma_{\text{mix}}] = 1 - \mathbb{P}^\star[\epsilon(1)|\sigma_{\text{mix}}]. \tag{28}$$

Note that $\mathbb{P}^\star[\epsilon(1)|\sigma_{\text{mix}}] = [0,1]$ when

$$\mathbb{P}[\sigma(1)] = \frac{\Gamma(\theta_{\text{on}}|\omega_f)\Omega}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}$$

denotes that the sensor can choose its mixed strategy arbitrarily to obtain maximal payoffs in such a case.

Combing (25), (26), (27) and (28), we can solve the unique mixed strategy Nash equilibrium $(\sigma^\star_{\text{mix}}, \epsilon^\star_{\text{mix}})$ as:

$$\sigma^\star_{\text{mix}}: \begin{cases} \mathbb{P}^\star[\sigma(1)] = \dfrac{\Gamma(\theta_{\text{on}}|\omega_f)\Omega}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \\ \mathbb{P}^\star[\sigma(2)] = 1 - \dfrac{\Gamma(\theta_{\text{on}}|\omega_f)\Omega}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \end{cases}$$

and

$$\epsilon^\star_{\text{mix}}: \begin{cases} \mathbb{P}^\star[\epsilon(1)] = \dfrac{J(\theta^\star_{\text{off}}) - J(\theta_{\text{on}})}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}, \\ \mathbb{P}^\star[\epsilon(2)] = 1 - \dfrac{J(\theta^\star_{\text{off}}) - J(\theta_{\text{on}})}{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}. \end{cases}$$

Therefore, when $\Gamma(\theta_{\text{on}}|\omega_f)\Omega < J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})$, i.e., the cost of launching an attack is relatively small, the optimal responses for the sensor and the attacker $(\sigma^\star, \epsilon^\star)$ exist in the form of a mixed strategy Nash equilibrium: $(\sigma^\star, \epsilon^\star) = (\sigma^\star_{\text{mix}}, \epsilon^\star_{\text{mix}})$.

2) On the other hand, when $\Gamma(\theta_{\text{on}}|\omega_f)\Omega \geqslant J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})$, we have:

$$\begin{cases} \mathbb{P}^\star[\epsilon(1)|\sigma_{\text{mix}}] = 0, \\ \mathbb{P}^\star[\epsilon(2)|\sigma_{\text{mix}}] = 1, \end{cases} \tag{29}$$

i.e., the best response for the attacker is always $\epsilon(2)$, i.e., not attacking, no matter what the sensor's strategy is. In such case, based on (25), the best response for the sensor is $\sigma(1)$, i.e., to keep the online schedule θ_{on}.

Consequently, when $\Gamma(\theta_{\text{on}}|\omega_f)\Omega > J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})$, the optimal responses for the sensor and the attacker $(\sigma^\star, \epsilon^\star)$ exists in the form of pure strategy Nash equilibrium $(\sigma^\star, \epsilon^\star) = \big(\sigma(1), \epsilon(2)\big)$. The payoffs for both sides can be calculated accordingly. ■

Remark 5.6: The results in Theorem 5.5 can be interpreted as follows: as a result of the game, both sides will adopt a mixed strategy that randomly chooses actions to obtain better payoffs. When the cost of launching attacks is small, the attacker has more incentive to attack, while the sensor is more willing to adopt the offline schedule, which is intuitive. On the other hand, as the attacking cost becomes larger, the optimal strategy for the attacker is to reduce the probability of attacking, until a pure strategy is obtained. The sensor will draw a similar conclusion. Such conclusions may help the sensor to better understand the behaviors of the attacker and evaluate the corresponding effects on the estimation performance.

Remark 5.7: Note that the framework and results developed in this section only require the attacking pattern to be feasible, as defined in Definition 4.1. Therefore, they also apply to a more general set of attacking patterns, provided the feasibility condition in Definition 4.1 is satisfied.

VI. Simulation Study

In this section, we provide numerical examples to illustrate the main results.

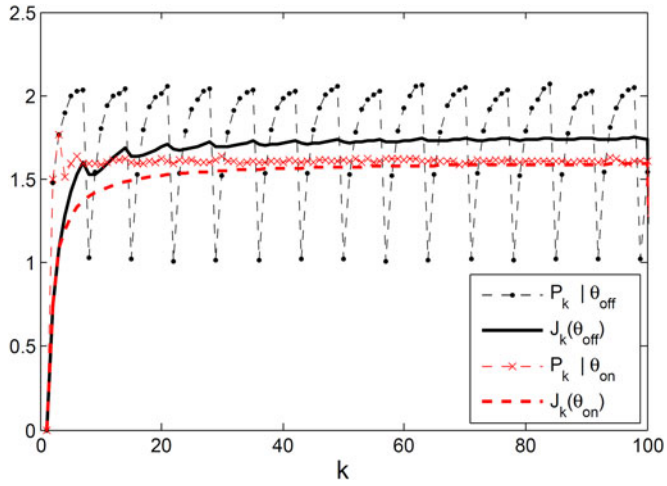


Fig. 4. Comparison between $\theta^\star_{\text{off}}$ and θ_{on}.

Consider a scalar system with parameters $A = 1.01, C = 0.7$, $R = Q = 1, \lambda = 0.5$. Suppose that the energy constraint for the sensor is given by $\Psi = \frac{1}{7}\Delta + \frac{6}{7}\delta$, i.e., the sensor can use the higher power Δ with a proportion of 1 out of every 7. Based on Theorem 3.1, it is easy to verify that the optimal offline schedule is given in a periodic form of $\{1000000, 1000000, \ldots\}$ with performance $J(\theta^\star_{\text{off}}) = 1.7609$. Given the energy constraint for the sensor, the parameter for the online schedule θ_{on} is $z_0 = 2$ with performance $J(\theta_{\text{on}}) = 1.5895$.

Define $J_k(\theta) = \frac{1}{k}\sum_{i=1}^{k}(\mathbb{E}[P_i])$ as the empirical approximation (via 100000 Monte Carlo simulations) of $J(\theta)$ at every time instant k. As shown in Fig. 4, when there is no attack, the estimation performance $J(\theta_{\text{on}})$ is better than the performance using the offline schedule $\theta^\star_{\text{off}}$. Note that P_k under $\theta^\star_{\text{off}}$ fluctuates periodically due to the special pattern of $\theta^\star_{\text{off}}$.

However, when there exists an attacker adopting the attacking pattern ω_f, the estimation performance of the online schedule θ_{on} under the attack, i.e., $J(\theta_{\text{on}}|\omega_f)$, is worse even than the optimal offline schedule $\theta^\star_{\text{off}}$. This may indeed motivate the sensor to switch from the online schedule to the offline one to obtain better estimation performance as considered in the present work. Given the parameters $\lambda = 0.5$ and $z_0 = 2$, from (22), we have $p_0 = 0.0716$. Fig. 5 shows the comparison of the estimation performance of $\theta^\star_{\text{off}}$, θ_{on}, and $\theta_{\text{on}}|\omega_f$ to support our results: since $J(\theta_{\text{on}}|\omega_f) > J(\theta^\star_{\text{off}})$, the sensor can obtain a better estimation performance by choosing $\theta^\star_{\text{off}}$ rather than θ_{on} under the attack.

Under the game-theoretic framework, the results of Theorem 5.5 provide the optimal strategies for both the sensor and the attacker. Given the parameter in this simulation section, the threshold for Ω is given by $\frac{J(\theta_{\text{on}}|\omega_f) - J(\theta_{\text{on}})}{\Gamma(\theta_{\text{on}}|\omega_f)} = \frac{1.9295 - 1.5895}{0.1429} = 2.3793$. For example, when $\Omega = 3 > 2.3793$, we have $(\sigma^\star, \epsilon^\star) = \big(\sigma(1), \epsilon(2)\big)$. When $\Omega = 1 < 2.3793$, we have:

$$\sigma^\star_{\text{mix}}: \begin{cases} \mathbb{P}^\star[\sigma(1)] = 0.4203, \\ \mathbb{P}^\star[\sigma(2)] = 0.5797, \end{cases} \quad \epsilon^\star_{\text{mix}}: \begin{cases} \mathbb{P}^\star[\epsilon(1)] = 0.5041, \\ \mathbb{P}^\star[\epsilon(2)] = 0.4959. \end{cases}$$

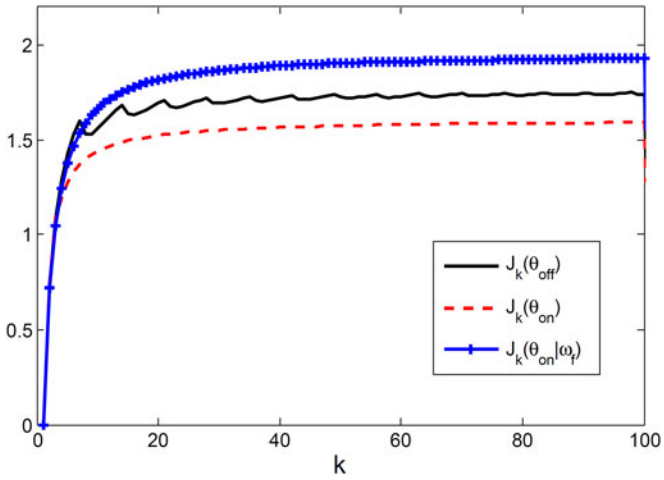


Fig. 5. Comparison of the estimation performance of $\theta^{\star}_{\text{off}}$, θ_{on}, and $\theta_{\text{on}}|\omega_f$.

VII. Conclusion

In this work, a potential class of malicious attacks on a remote state estimation setup was studied. We proposed an attack strategy which can modify aggregated-ACKs from the remote estimator and convey fake information to the sensor without being detected. The corresponding effect on the estimation performance was analyzed based on well-established Markov chain theory. To investigate the optimal strategies for both the sensor and the attacker in the attack-switch game, a game-theoretic framework was introduced and the equilibrium for both sides was analyzed. Future work includes investigating the security issues in a multi-sensor scenario and the case with the participation of the remote estimator.

References

[1] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[2] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[3] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, Jan. 2007.

[4] J. Baillieul and P. J. Antsaklis, "Control and communication challenges in networked real-time systems," *Proc. IEEE*, vol. 95, no. 1, pp. 9–28, Jan. 2007.

[5] K. Gatsis, A. Ribeiro, and G. J. Pappas, "Optimal power management in wireless control systems," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1495–1510, Jun. 2014.

[6] O. C. Imer and T. Başar, "Optimal estimation with limited measurements," in *Proc. IEEE Conf. Decis. Control Eur. Control Conf.*, 2005, pp. 1029–1034.

[7] D. E. Quevedo, A. Ahlén, and J. Østergaard, "Energy efficient state estimation with wireless sensors through the use of predictive power control and coding," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4811–4823, Sep. 2010.

[8] K. Gatsis, M. Pajic, A. Ribeiro, and G. J. Pappas, "Opportunistic sensor scheduling in wireless control systems," in *Proc. IEEE 53rd Annu. Conf. Decis. Control*, 2014, pp. 3777–3782.

[9] L. Shi, P. Cheng, and J. Chen, "Sensor data scheduling for optimal state estimation with communication energy constraint," *Automatica*, vol. 47, no. 8, pp. 1693–1698, 2011.

[10] Y. Li, D. E. Quevedo, V. Lau, and L. Shi, "Online sensor transmission power schedule for remote state estimation," in *Proc. IEEE 52nd Aunn. Conf. Decis. Control*, 2013, pp. 4000–4005.

[11] D. Han, P. Cheng, J. Chen, and L. Shi, "An online sensor power schedule for remote state estimation with communication energy constraint," *IEEE Trans. Autom. Control*, vol. 59, no. 7, pp. 1942–1947, Jul. 2014.

[12] J. Wu, K. Johansson, and L. Shi, "An improved hybrid sensor schedule for remote state estimation under limited communication resources," in *Proc. 51st IEEE Conf. Decis. Control*, 2012, pp. 3305–3310.

[13] Y. Mo *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[14] K.-D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, May 2012.

[15] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Syst.*, vol. 35, no. 1, pp. 110–127, Feb. 2015.

[16] A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, 2008, pp. 495–500.

[17] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in *Proc. 1st Int. Conf. High Confidence Netw. Syst.*, 2012, pp. 47–54.

[18] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 21–32, 2011.

[19] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. IEEE 47th Annu. Allerton Conf. Commun., Control, Comput.*, 2009, pp. 911–918.

[20] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[21] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "Fake-acknowledgment attack on ACK-based sensor power schedule for remote state estimation," in *Proc. IEEE 54th Annu. Conf. Decis. Control.*, 2015, pp. 5795–5800.

[22] P. Hovareshti, V. Gupta, and J. S. Baras, "Sensor scheduling using smart sensors," in *Proc. 46th IEEE Conf. Decis. Control*, 2007, pp. 494–499.

[23] B. D. O. Anderson and J. Moore, *Optimal Filtering*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1979.

[24] J. R. Norris, *Markov Chains*. Cambridge, U.K.: Cambridge Univ. Press, 1998, no. 2.

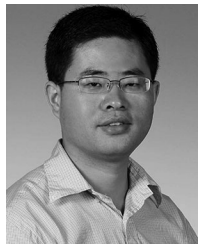
[25] J. Nash, "Non-cooperative games," *Annals Math.*, vol. 54, no. 2, pp. 286–295, 1951.

[26] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

Yuzhe Li received the B.S. degree in mechanics and B.A. degree in economics from Peking University, Beijing, China, in 2011 and the Ph.D. degree in electronic and computer engineering from the Hong Kong University of Science and Technology, Kowloon, Hong Kong, in 2015. Between June 2013 and August 2013, he was a Visiting Scholar in the University of Newcastle, Australia. He is currently working as a Postdoctoral Fellow in the Department of Electrical and Computer Engineering, University of Alberta, Alberta, Canada. His research interests include cyber-physical system security, sensor power control, and networked state estimation.

Daniel E. Quevedo received the Ing. Civ. Electrónico and M.Sc. degrees from the Universidad Técnica Federico Santa María, Chile, in 2000 and 2005, respectively and the Ph.D. degree from the University of Newcastle, Australia. He holds the Chair in Automatic Control at the Paderborn University, Germany. In 2009, he was awarded a five-year fellowship from the Australian Research Council. He is an Editor of the *International Journal of Robust and Nonlinear Control* and serves as the Chair of the IEEE CSS *Technical Committee on Networks & Communication Systems*. His research interests include networked estimation and control and on predictive control of power converters.

Subhrakanti Dey received the B.Tech. and M.Tech. degrees from the Indian Institute of Technology, Kharagpur, India, in 1991 and 1993, respectively, and the Ph.D. degree from the Australian National University, Canberra, Australia, in 1996. He is currently working as a Professor in the Department of Engineering Sciences, Uppsala University, Uppsala, Sweden. His research interests include networked control systems, wireless communications and networks, signal processing for sensor networks, and stochastic and adaptive signal processing and control. He currently serves in the Editorial Board of IEEE TRANSACTIONS ON SIGNAL PROCESSING and IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS. He was also an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING during 2007–2010 and the IEEE TRANSACTIONS ON AUTOMATIC CONTROL during 2004–2007, and an Associate Editor for Elsevier *Systems and Control Letters* during 2003–2013.



Ling Shi received the B.S. degree in electrical and electronic engineering from the Hong Kong University of Science and Technology, Kowloon, Hong Kong, in 2002 and the Ph.D. degree in control and dynamical systems from the California Institute of Technology, Pasadena, CA, USA, in 2008. He is currently working as an Associate Professor in the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Kowloon. His research interests include networked control systems, wireless sensor networks, event-based state estimation and sensor scheduling, and smart energy systems. Since 2015, he has been serving as a Subject Editor for *International Journal of Robust and Nonlinear Control*. He also served as an Associate Editor for a special issue on Secure Control of Cyber Physical Systems in the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS in 2015.