23rd International Symposium on Mathematical Theory of Networks and Systems
Hong Kong University of Science and Technology, Hong Kong, July 16-20, 2018

Optimal Denial-of-Service Attack Sequence with Energy Constraint Over Lossy Networks

Menglin Li[1] and Jiahu Qin[1]

***Abstract*— A novel method is proposed for solving the optimal Denial-of-Service (DoS) attack scheduling problem against remote state estimation with energy constraint over the lossy network. The optimal attack scheduling squence that maximizes the average expected estimation error over lossy networks is derived. Details of the technique are outlined.**

I. INTRODUCTION

Cyber-Physical Systems (CPS) usually comprise components that can implement sensing, control, communication, and computation. The recent years have seen a surge of security issues of CPS. CPS are vulnerable to DoS attacks which may prevent he exchange of useful information among system components [2]. An attacker that does not have abundant power supply cannot jam the communication channel all the time [3], [4], [5]. And in wireless networks, it is inevitable for the data packet to randomly drop. However, in [3], [4], [5], packet dropouts as the key issue in wireless communication are neglected. To capture packet dropouts in wireless links, we consider the lossy network in which the packet may drop even if the channel is not attacked. Due to the introduction of the lossy network, it is hard to deal with the corresponding scenario. In the current work, a novel approach is proposed to derive the optimal DoS attack schedule which maximizes the trace of average expected estimation error covariance over the lossy network.

II. METHODS

Consider a general discrete linear time-invariant (LTI) process of

$$x_{k+1} = Ax_k + w_k,$$
$$y_k = Cx_k + v_k.$$

where $k \in \mathbb{Z}^+$, $x_k, w_k \in \mathbb{R}^n$ and $y_k, v_k \in \mathbb{R}^m$ are the process state vector, the process noise, the measurement vector, and the measurement noise, respectively, at time k, and w_k and v_k are zero-mean i.i.d. Gaussian noises with covariances $Q \geqslant 0$ and $R > 0$, respectively. Assuming the pair (A, C) is observable and $(A, \sqrt{Q})$ is controllable.

Sensors are assumed to be capable of storing data and performing computations. For time step k, obtaining the raw data y_k, the sensor runs a Kalman filter to obtain the minimum mean squared error (MMSE) estimate $\hat{x}_k^s = \mathbb{E}[x_k | y_1, \ldots, y_k]$, with the corresponding error covariance $P_k^s = \mathbb{E}[(x_k - \hat{x}_k^s)(x_k - \hat{x}_k^s)' | y_1, \ldots, y_k]$. Then the data packet that contains the information of $\hat{x}_k^s$ is sent from the sensor to a remote estimator over a lossy network. Consider the state estimation at the remote estimator side within a finite time horizon T, with data packets in transit under DoS attacks $\lambda \triangleq \{\lambda_1, \lambda_2, \ldots, \lambda_T\}$.

According to [4] there holds, for the state estimate $\hat{x}_k$ at the remote estimator side,

$$\hat{x}_k = \theta_k(\lambda)\hat{x}_k^s + (1 - \theta_k(\lambda))A\hat{x}_{k-1},\ k = 1, 2, \ldots, T,$$

where $\theta_k = 1$ stands for the arrival of data packets and $\theta_k = 0$ for the opposite, $\lambda_k = 1$ means the attacker imposes the DoS attack at time k, otherwise $\lambda_k = 0$. The DoS attacker is assumed to have a limited power supply. Energy limitation is formulated as $\sum_{k=1}^{T} \lambda_k = M$, where $M < T$. When the schedule λ is given, θ_k's are assumed to be i.i.d. Bernoulli random variables with probability distribution

$$\tilde{p}_k(\lambda) = Pr(\theta_k = 1) = (1 - \lambda_k)(1 - \alpha) + \lambda_k(1 - \beta),$$

where β and α are the packet dropout probabilities under the DoS attack and in the absence of attack, respectively ($\beta > \alpha$).

As k grows, P_k^s exponentially converges to $\overline{P}$, and the Kalman filter is in steady-state. Similar to [4], assume $P_k^s = \overline{P}, k \geq 0$. Define $h : \mathbb{S}_+^n \to \mathbb{S}_+^n$ as $h(X) \triangleq AXA' + Q$. Then the error covariance P_k [4] corresponding to $\hat{x}_k$ follows

$$P_k = \theta_k \overline{P} + (1 - \theta_k)h(P_{k-1}),\ k = 1, 2, \ldots, T \qquad (1)$$

We write $P_k(\lambda)$ as P_k, etc., when λ is given. For a given λ, the system metric is the average expected estimation error called *Average Error* [4], $J_A(\lambda) = \frac{1}{T}\sum_{k=1}^{T} \mathbb{E}[P_k(\lambda)]$.

An attacker aims to maximize the trace of the average error, which leads to the following problem:

Problem 1:

$$\max_{\lambda \in \Lambda} \quad Tr[J_A(\lambda)]$$
$$s.t. \quad \sum_{k=1}^{T} \lambda_k = M,$$

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

A squence in which M attacks are launched over the time horizon T can be denoted by $(\gamma^d, \lambda^{k_1}, \gamma^{d_1}, \lambda^{k_2}, \ldots, \lambda^{k_s}, \gamma^{d_s})$, which is corresponding to

$$(\underbrace{0, \ldots, 0}_{d \text{ times}}, \underbrace{1, \ldots, 1}_{k_1 \text{ times}}, 0, \ldots, 0, \underbrace{1, \ldots, 1}_{k_s \text{ times}}, \underbrace{0, \ldots, 0}_{d_s \text{ times}}),$$

where $\sum_{i=1}^{s} k_i = M$, and $d + \sum_{j=1}^{s} d_j = T - M$. Assume that the data packet which contains the information of $\hat{x}_0^s$ successfully arrives at the remote estimator at time $k = 0$, i.e., $P_0 = \overline{P}$.

[1]Menglin Li and Jiahu Qin are with the Department of Automation, University of Science and Technology of China, Hefei 230027, China lml95@mail.ustc.edu.cn; jhqin@ustc.edu.cn

Denote by $p_{i,k}$ the probability that $P_k = h^i(\overline{P})$, $i = 0,1,\ldots,T$. We have, from (1),

$$J_A(\lambda) = \frac{1}{T}\sum_{k=1}^{T}\sum_{i=0}^{T} p_{i,k} h^i(\overline{P}). \tag{2}$$

Problem 1 is a combinational optimization problem which, to the best of our knowledge, no unified methods or algorithms can be employed to deal with. Here we exploit the special structure of the proposed problem to solve it. From (2), the expression of the average error is rather complicated. However, the difference between the average errors under two similar attack squences may be more tractable. Motivated by this, first we focus on the following three types of attack schedules over the time horizon T. We can see that these three types of attack squences have similar structures.

$$\begin{cases} \phi = (\gamma^d, \lambda^{k_1}, \gamma^{d_1}, \lambda^{k_2}, \ldots, \lambda^{k_s}, \gamma^{d_s}). \\ \phi^0 = (\gamma^{d_s}, \lambda^{k_s}, \ldots, \lambda^{k_2}, \gamma^{d_1}, \lambda^{k_1}, \gamma^{d}). \\ \phi^1 = (\gamma^{d+1}, \lambda^{k_1}, \gamma^{d_1-1}, \lambda^{k_2}, \ldots, \lambda^{k_s}, \gamma^{d_s}). \end{cases} \tag{3}$$

To compare the effects under ϕ, ϕ^0 and ϕ^1 on $Tr[J_A]$, we focus on the differences, i.e., $J_A(\phi) - J_A(\phi^0)$ and $J_A(\phi) - J_A(\phi^1)$. More specifically, according to (2), we have $J_A(\phi) - J_A(\phi^1) = \frac{1}{T}\sum_{i=0}^{T} h^i(\overline{P}) F_i$, where $F_i = \sum_{k=1}^{T}(p_{i,k}(\phi) - p_{i,k}(\phi^1))$. Then we can respectively calculate F_i for $t = 0,\ldots,T$ and obtain the following proposition.

Proposition 1 ([1]) : Let $H_t = \sum_{i=0}^{t} F_i$, for $t = 0,\ldots,T$, where $F_i = \sum_{k=1}^{T}(p_{i,k}(\phi) - p_{i,k}(\phi^1))$. Then we have the following three statements.

(1) $H_T = 0$.

(2) $H_t \geq 0$, for $t = 0,\ldots,T-1$, when $d < d_s$ and $s = 1$.

(3) $H_t \geq 0$, for $t = 0,\ldots,T-1$, when $d \leq d_s + 1$ and $s \geq 2$.

Now we can state the main results in the next section.

III. RESULTS

The following theorem is stated to present the results of comparison among ϕ, ϕ^0 and ϕ^1 in (3).

Theorem 1 ([1]) : For J_A in (2), and ϕ, ϕ^0, ϕ^1 in (3), the following three statements hold.

(a) $J_A(\phi) = J_A(\phi^0)$.

(b) $J_A(\phi) \leq J_A(\phi^1)$ when $d < d_s$ and $s = 1$.

(c) $J_A(\phi) \leq J_A(\phi^1)$ when $d \leq d_s + 1$ and $s \geq 2$.

When the communication channel is perfect, i.e., $\alpha = 0$, the optimal attack squence [4] is any schedule in the set $\lambda^{(M)} = \{(\gamma^d, \lambda^M, \gamma^{d_1}) : d = 0,1,\ldots,T-M\}$. All attack squences in the set $\lambda^{(M)}$ lead to the same average error. This is because the assumption in [4] that $\alpha = 0$, causes $P_k = \overline{P}$ when an attack is not launched at time k. In contrast, according to statement (b) in *Theorem 1*, under a lossy network, two different attack squences in the set $\lambda^{(M)}$ may lead to different effects on the system performance. Hence, the proposed optimal attack squence in [4] is not the solution to *Problem 1*. The following theorem is stated to present the optimal attack schedule in this paper.

Theorem 2 ([1]) : The optimal attack squence, i.e., the solution to *Problem 1*, is $\lambda_* = (\gamma^{D_1}, \lambda^M, \gamma^{D_2})$, where $D_1 + D_2 = T - M$, and $|D_1 - D_2| \leq 1$, i.e., $D_1 = D_2$ or $|D_1 - D_2| = 1$.

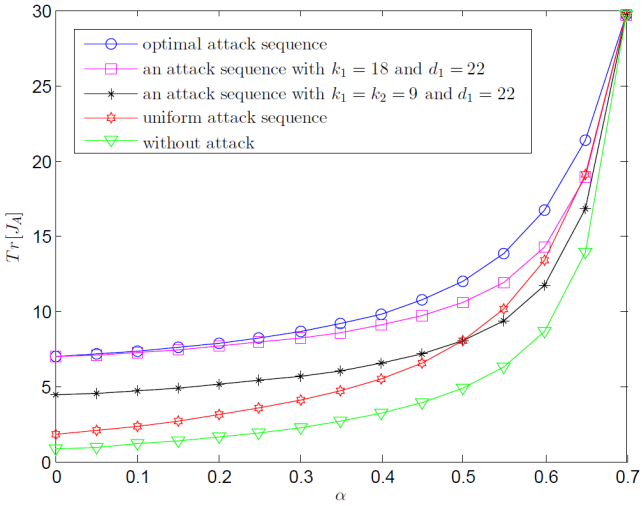

Fig. 1. $Tr[J_A]$ under different attack squences while the packet dropout probability in the absence of attack α is varying ($\beta = 0.7$).

From *Theorem 2*, we see that the attacker should group the attacks together and jam the channel in the middle of the considered time horizon T to maximize the trace of average expected estimation error at the remote estimator. Next we demonstrate the theoretical results by simulations.

We consider a system with parameters $A = \begin{bmatrix} 1.2 & 0.1 \\ 0 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $Q = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$, $R = 0.5C$. Let $T = 40$, $M = 18$ and $\beta = 0.7$. In Fig. 1, we examine the variation of $Tr[J_A]$ with different attack schedules under different packet dropout probabilities without attacks from $\alpha = 0$ to $\alpha = 0.7$. As shown in the figure, larger α leads to larger $Tr[J_A]$, which makes intuitive sense. In [4], the attack schedule with $k_1 = 18$ and $d_1 = 22$ is also optimal. But from statement (b) of *Theorem 1*, it is no longer optimal in the lossy scenario, which can be also seen from the figure. From [4], the uniform distribution of the attack times over the time horizon T leads to the minimum average error. This is incorrect in the lossy scenario. From Fig. 1, the common attack squence with $k_1 = k_2 = 9$ and $d_1 = 22$ leads to the smaller $Tr[J_A]$ than the uniform one when $\beta = 0.7$ and $0.55 \leq \alpha \leq \beta$. The issue of finding the worst attack squence which minimizes the average error will be studied in the future.

REFERENCES

[1] J. Qin, M. Li, L. Shi, and X. Yu, Optimal Denial-of-Service Attack Scheduling with Energy Constraint Over Packet-dropping Networks, IEEE Trans. Autom. Control, DOI: 10.1109/TAC.2017.2756259.

[2] A. Cárdenas, S. Amin, and S. Sastry, Research challenges for the security of control systems, in Proc. 3rd Conf. Hot Topics Security, 2008, pp. 1–6.

[3] H. Zhang, P. Cheng, L. Shi, and J. Chen, Optimal DoS attack scheduling in wireless networked control system, IEEE Trans. Control Syst. Technol., Vol. 24, No. 3, pp. 843–852, 2016.

[4] H. Zhang, P. Cheng, L. Shi, and J. Chen, Optimal denial-of-service attack scheduling with energy constraint, IEEE Trans. Autom. Control, Vol. 60, No. 11, pp. 3023–3028, 2015.

[5] H. S. Foroush and S. Martínez, On event-triggered control of linear systems under periodic denial of service attacks, in Proc. IEEE Conf. Decision Control, Maui, HI, USA, 2012, pp. 2551–2556.