Game-Theoretical Strategies for Remote Sensors under Jamming Attack

Griffin Rule

EECE 580A

Abstract
This project uses game theoretical frameworks to analyze a cyber-physical system security game. Security in cyber-physical systems has become increasingly important as more sensor networks are connected through the internet. These systems are being used to control critical infrastructure such as the power grid, agriculture systems, and much more. This makes them large targets for terrorist and enemy nation states. These systems are extremely vulnerable to jamming attacks or Denial of Service attack (DoS) because of their connection to the internet. This can cause these systems to be controlled inefficiently or even cause catastrophic failure causing extreme harm to the people who rely on them. Using game theory the optimal strategies for the attacker and defender can be derived and the value of the game can be found. This has important implications for designing and implementing remote estimation systems.

Introduction
Cyber-Physical Systems are becoming a very important part of modern infrastructure. With wireless sensors becoming cheaper and including computational power they are added to systems to improve performance. Smart grids, smart transportation systems, and remote environmental sensing are just some of the application of remote state estimation. These smart sensors are connected to the internet which creates many security issues. A jamming attack or sometimes called a Denial of Service (DoS) attack prevents communication between the sensors and the estimator. The sensors are remote so the sensors and the system attacking are often power limited. This shapes the strategies of the attacker and the defender or estimator. Jamming attacks are relatively simple to implement and can cause serious damage. The blackout in Ukraine was a large scale attack on a power grid that had comprised of several different attacks including a DoS attack. Approximately 225,000 customers lost power for several hours, requiring the power company to manual operation. This is one example of how a DoS attack can be used to damage critical infrastructure. This incident also highlights the capabilities of attackers as it would have required large amounts of resources for the attacker. Analyzing this game of attacker and defender assists in the development of the systems by determining the outcome if the system were to come under attack. The optimal attacker and defender strategies have been analyzed for a single sensor when the attacker and defender have limited power. The attackers optimal strategy has be analyzed for a network of sensors that always transmit with a power limited attacker. Some assumptions were made about the situation in prior works about the system that simplify the equations but lead to suboptimal solutions. The joint attacker and defender strategies have yet to be analyzed for this problem setting. These strategies can be found by formulating a convex optimization problems. The attacker defender game is a zero sum game, meaning there is a saddle point equilibrium. By formulating a convex problem this equilibrium can be found using numerical software. The contributions of this project are the generation of payoff matrix for exact solutions, comparison and analysis of past works, and revisions to these convex optimization formulas.

Problem Definition

The system that will be studied is a single centralized estimator that can receive transmissions from multiple sensors and an attacker that can prevent the sensors transmission from making it to the estimator. There is a time horizon for this game T meaning the defender gets T opportunities to transmit a measurement. There are N sensors and attacker has a power budget M where $T \times N > M$. Only one sensor will be allowed to transmit at a time and the defender must come up with a communication schedule. The attacker may jam more than one sensor at any time instant and has its own attacking schedule. Jamming attacks have been studied for single sensors or just for the attacker but the complete game has not been analyzed for multiple sensors. The system is modeled as discrete linear time-invariant using a Kalman Filter. The Kalman Filtering equations are used to control the system and state how much error is in the system.

$$\hat{x}_{k|k-1} = A\hat{x}_{k-1}$$
$$P_0 = \Pi$$
$$P_{k|k-1} = AP_{k-1}A^T + Q$$
$$K_k = P_{k|k-1}C^T\left[CP_{k|k-1}C^T + R\right]^{-1}$$
$$P_k = P_{k|k-1} - K_k(CP_{k|k-1}C^T + R)K_k^T$$
$$\hat{x}_k = A\hat{x}_{k-1} + K_k(y_k - CA\hat{x}_{k-1})$$

Assumptions that may be made about the system include it be unstable, there is initial estimation error, and the sensors having a smaller error covariance than that of the process. The goal however should be a formulation that can solve for any situation. There are applications for stables systems and cases of extremely poor sensor measurements.

$$\det(A) > 1$$
$$Q > C^{-1}R(C^{-1})^T$$
$$\Pi > 0$$

If the transmission is blocked by the attacker the estimate is solely made based on the system dynamics and the previous state. P_k is the error covariance and defines how much error there is in the current estimate. The error covariance can be different from sensor to sensor resulting in different system error when used. The objective for both players the average covariance of the system. This quantity can be calculated without fully simulating the system.

$$J(\theta) = \frac{1}{T}\sum_{k=1}^{T} Tr(P_k)$$

With each sensor having different characteristics different sensors will be prioritized by the attacker and defender. From a game theory perspective the goal of the defender is to find the

strategy that minimizes the maximum of the objective function and the attacker wants to find the strategy that maximizes the minimum of the objective function. Will say the defender has action space θ_S and the attacker has action space θ_A then the optimization for the defender is to minimize with respect to θ_S the maximum error covariance with respect to θ_A. The attacker has the optimization the maximum with respect to θ_A the minimum error covariance with respect to θ_S.

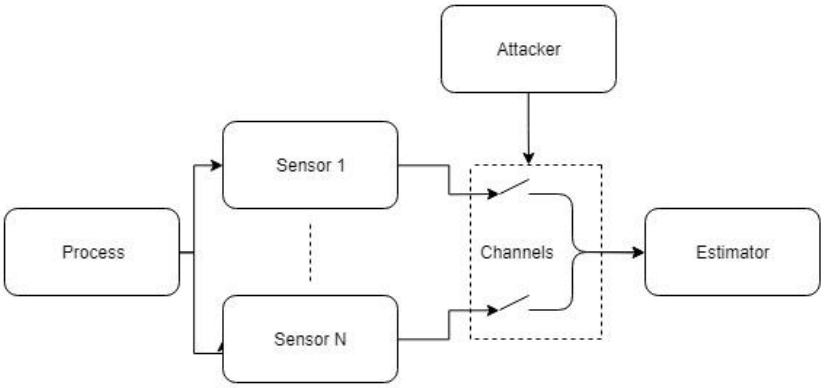

Figure 1: System Diagram

Formulation

There are N^T strategies for the defender and there are $T \times N$ choose M for the attacker. In order to generate the payoff matrix there must be an encoding system for the attacker and defender strategies. Each player must assign resources to the playing field, we can encode this by using the variables γ_k^i that represent whether a communication opportunity is used and η_k^i whether an attack opportunity is used at time k and on sensor i. We set them equal to one if the opportunity is used and zero otherwise. Once all $T \times N$ matrices have been generated the outcome of any two strategies can also be determined to find the outcome of these strategies.

$$\lambda_k^i = \gamma_k^i (1 - \eta_k^i)$$

Where λ_k^i represents if a transmission is received from sensor i at time k. From the result of the two strategies the error covariance can be easily calculated and put into the payoff matrix.

$$P_k = \left(P_{k|k-1}^{-1} + \sum_{i=1}^{N} \mathrm{C_i} R_i^{-1} {C_i}^T \lambda_k^i \right)^{-1}$$

This objective function is not convex. It is the composition of a convex function with a decreasing convex function.

Payoff Matrix

One strategy for solving the problem is to generate the outcome for all pure strategies. Using these a payoff matrix can be formed and a mixed strategy from the pure strategies can be found. This is the exact solution for the problem and easily solvable for small problems.

$$Minimize\ Max(A^T y)$$
$$Subject\ to$$
$$y \geq 0$$
$$y^T 1 = 1$$

$$Minimize\ \ Max(Az)$$
$$Subject\ to$$
$$z \geq 0$$
$$z^T 1 = 1$$

This can be converted to a linear programming problem so that it can be solved faster. Although generating the matrix is the most computationally difficult part of this solution. Ideas for reducing the time for generating them are discussed later.

$$Minimize\ \ t$$
$$Subject\ to$$

$$y \geq 0$$
$$y^T 1 = 1$$
$$A^T y \leq t$$

$$Minimize\ \ v$$
$$Subject\ to$$
$$z \geq 0$$
$$z^T 1 = 1$$
$$Az \leq v$$

Generating and solving for these matrices are extremely time consuming and may become infeasible as the time horizon and number of sensors increase. These solutions do offer insight into the problem. Looking at the structure of solutions may aid in solving for larger problems. It is beneficial to formulate a new convex problem though, so that the solution can be found for large problems. This requires some relaxation of constraints and approximation of the objective function. This means the solution found may not be optimal for the original problem but an approximate solution for large problems is still useful.

Past formulation

The results from Yang, Yang, and Shi. Their solution was for an attacker with a network of sensors that transmit at every time step. This provides a starting point and a comparison to the exact solution.

$$H_i = C_i^T \sqrt{R_i^{-1}}$$
$$H = (H_1^T, H_2^T, \dots, H_N^T)^T$$
$$\Gamma_k = diag((1-\lambda_k^1)I, (1-\lambda_k^2)I, \dots, (1-\lambda_k^N)I)$$
$$h(x) = AXA^T + Q$$
$$\tilde{\Gamma}_{\mathrm{k}}^{\mathrm{m}} = \gamma_k + \sigma_m^2(I - \Gamma_k)$$

$$Maximize \quad \frac{1}{T}\sum_{k=1}^{T} Tr(X_k)$$
$$Subject\ to$$
$$\begin{bmatrix} h(X_{k-1}) - X_k & h(X_{k-1})H^T \\ Hh(X_{k-1}) & Hh(X_{k-1})H^T + \tilde{\Gamma}_k^m \end{bmatrix} \geq 0$$
$$\sum_{k=1}^{T}\sum_{i=1}^{N} \lambda^i{}_k \leq M$$
$$0 \leq \lambda^i{}_k \leq 1$$

Where σ_m is sufficiently large so that the results are accurate. The derivation of this can be found in their paper. Using this algorithm much larger games can be solved for but it only represents the strategy for attacking. An optimal strategy in this form should be a pure strategy as there are no options for the defender. That is not the result of this algorithm and the authors note this should be taken as setting the M largest values to one and the rest to zero. These results however still do not agree.

Results

When using the first strategy of generating the payoff matrix you can then find the probability of choosing an individual sensor at a specific time. These results have a clear structure. The results from the second method differ from those of the first. The structure is also different from that of the first method. We will first analyze when $T = 3, N = 2, M = 4$.

$$\text{Attacker} \begin{bmatrix} 0.4650 & 0.5350 \\ 1 & 1 \\ 0.4947 & 0.5053 \end{bmatrix} \quad \text{Defender} \begin{bmatrix} 0.5350 & 0.4650 \\ 0.5098 & 0.4924 \\ 0.5053 & 0.4947 \end{bmatrix}$$

Now looking at the results of Yang, Yang, and Shi with $T = 3, N = 2\ M = 4$. In this case however the defender is always transmitting. The solution as descripted by the authors does not agree with the brute force solution. The formulation is inaccurate due to the relation of λ and

how the objective is formulated. Due to the recursive payoff function and the formulation $\sum_{i=1}^{N} \mathrm{C_i} R_i^{-1} C_i^{T} \lambda_k^i$ which only holds for pure strategies or when λ is one or zero.

Attacker matrix solution- $\begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}$ Attacker semidefinite solution- $\begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$

Finally the setting where each individual sensor has limited energy was analyzed. The results show similar structure to the other formulations. The results for this section are for $T = 3, N = 2, M = 4$ defender having a power constrain $P = 2$ for each sensor with the same system dynamics.

Attacker - $\begin{bmatrix} 0.9831 & 0.9760 \\ 0.9858 & 0.9776 \\ 0.0311 & 0.0464 \end{bmatrix}$ Defender - $\begin{bmatrix} 0.6806 & 0.5348 \\ 0.6085 & 0.5026 \\ 0.7109 & 0.9627 \end{bmatrix}$

Attacker - $\begin{bmatrix} 0.9957 & 0.9956 \\ 0.9969 & 0.9948 \\ 0.9970 & 0.9950 \\ 0.0094 & 0.0126 \\ 0.0013 & 0.0038 \end{bmatrix}$ Defender - $\begin{bmatrix} 0.6101 & 0.4927 \\ 0.5694 & 0.4409 \\ 0.5525 & 0.4609 \\ 0.7318 & 0.9843 \\ 0.5361 & 0.6211 \end{bmatrix}$

Conclusions

We can analyze the results and draw conclusions about the structure of results. This may aid in developing algorithms that can solve for much larger more complex games. The first solution can be improved upon as there are ways of reducing the size of the matrix. In general around half of the pure strategies are dominate strategies. That is half of the pure strategies have a probability zero or near zero. By finding the dominate strategies and eliminating the others the problem can be solved much faster and for larger games. This is just the beginning of this work as there is still no full solution to the problem that can be done in real time. There is also mathematical analysis needed to confirm intuitions about results. The results do however illustrate the connection between attacker and defender strategies. Important analysis that could also be done using these algorithms is using them to design sensor networks or determining the minimum characteristics of the sensors such as energy, and error covariance. Significant improvements could also be made to the semidefinite programming solution so that results are more accurate. With an improved formulation large scale problems may become solvable in real time.

Acknowledgements
I would also like to thank Professor Wu for her input on the problem and for knowledge on convex optimization. I would like to thank Professor Akyol for his assistance and expertise in game theory and cyber-physical system security.

References
"Analysis of the cyber attack on the Ukrainian power grid: Defense use case", [online] Available: https://ics.sans.org/duc5.

G. Liang, S. Weller, J. Zhao, F. Luo, Z. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks", *IEEE Trans. Power Syst., vol. 32, no. 4, pp. 3317-3318, 2017.*

Y. Li, L. Shi, P. Cheng et al., "Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach", *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831-2836, 2015.

Chao Yang, Wen Yang, Hongbo Shi, "DoS attack in centralised sensor network against state estimation", *IET Control Theory & Applications*, 2018.