

A State Estimation and Malicious Attack Game in Multi-Sensor Dynamic Systems

Jingyang Lu and Ruixin Niu

Department of Electrical and Computer Engineering
 Virginia Commonwealth University
 Richmond, VA 23284, U.S.A.
 {luj2, rniu}@vcu.edu

Abstract—In this paper, the problem of false information attack on and the Kalman filter’s defense of state estimation in dynamic multi-sensor systems is investigated from a game theoretic perspective. The relationship between the Kalman filter and the adversary can be regarded as a two-person zero-sum game. Under which condition both sides of the game will reach the Nash equilibrium is investigated in the paper. The multi-sensor Kalman filter system and the adversary are supposed to be rational players. The Kalman filter and the adversary have to choose their respective subsets of sensors to perform system state estimation and false information injection. It is shown how both sides pick their strategies in order to gain more and lose less. The optimal solutions are achieved by solving the minimax problem. Numerical results are also provided in order to illustrate the effectiveness of the derived optimal strategies.

I. INTRODUCTION

System state estimation in the presence of an adversary that injects false information into sensor readings is an important problem with wide application areas, such as target tracking with compromised sensors, secure monitoring of dynamic electric power systems, and radar tracking and detection in the presence of jammers. This topic has attracted considerable attention and interest recently [1], [2], [3], [4], [5], [6], [7]. In [1], the problem of how to take advantage of the power system configuration to introduce arbitrary bias to the system was investigated. In [2], the authors showed the impact of malicious attacks on real-time electricity market and how the attackers can make profit by manipulating certain values of the measurements. The relationship between the attackers and the control center was discussed in [3], where both the adversary’s attack strategies and the control center’s attack detection algorithms have been proposed. False data attacks on the electricity market have also been investigated in [4] and [5]. In [6], the data frame attack was formulated as a quadratically constrained quadratic program (QCQP). In [7], the relationship between a target and a MIMO radar was characterized as a two-person zero-sum game. However, in the aforementioned publications, only the problem of *static* system state estimation has been considered.

We are interested in *dynamic* system state estimation and in [8], we have studied the impact of the injected biases on a Kalman filter (KF)’s estimation performance, showing that if the false information is injected at a single time, its impact converges to zero as time goes on; if the false information

is injected into the system continuously, the estimation error tends to reach a steady state. In [9], we have found the best strategy for the adversary to attack the Kalman filter system from the perspective of the trace of the mean squared error (MSE) matrix, and obtained some close-form results. We have also studied how the attacker can maximize the determinant of the Kalman filter’s estimation MSE matrix in [10]. Based on our previous work, in this paper our goal is to use game theory to investigate the relationship between the Kalman filter and the attacker. The Kalman filter (the defender) and the attacker are supposed to be rational players. The trace of the state estimation MSE is used to construct the payoff matrix, and the problem can be characterized and solved as a minimax problem. Numerical results show the effectiveness of the optimal mixed defense strategy for the KF against the adversary’s attacks.

II. SYSTEM MODEL

The discrete-time linear dynamic system can be described as

$$\mathbf{x}_{k+1} = \mathbf{F}_k \mathbf{x}_k + \mathbf{G}_k \mathbf{u}_k + \mathbf{v}_k \quad (1)$$

where \mathbf{F}_k is the system state transition matrix, \mathbf{x}_k is the system state vector at time k , \mathbf{u}_k is a known input vector, \mathbf{G}_k is the input gain matrix, and \mathbf{v}_k is a zero-mean white Gaussian process noise with covariance matrix $E[\mathbf{v}_k \mathbf{v}_k^T] = \mathbf{Q}_k$. Let us assume that M sensors are used by the linear system. The measurement at time k collected by sensor i is

$$\mathbf{z}_{k,i} = \mathbf{H}_{k,i} \mathbf{x}_{k,i} + \mathbf{w}_{k,i} \quad (2)$$

with $\mathbf{H}_{k,i}$ being the measurement matrix, and $\mathbf{w}_{k,i}$ a zero-mean white Gaussian measurement noise with covariance matrix $E[\mathbf{w}_{k,i} \mathbf{w}_{k,i}^T] = \mathbf{R}_{k,i}$, for $i = 1, \dots, M$. We further assume that the measurement noises are independent across sensors. The matrices \mathbf{F}_k , \mathbf{G}_k , $\mathbf{H}_{k,i}$, \mathbf{Q}_k , and $\mathbf{R}_{k,i}$ are assumed to be known with proper dimensions. For such a linear and Gaussian dynamic system, the Kalman filter is the optimal state estimator. In this paper, we assume that a bias $\mathbf{b}_{k,i}$ is injected by the adversary into the measurement of the i th sensor at time k intentionally. Therefore, the measurement equation becomes

$$\mathbf{z}'_{k,i} = \mathbf{H}_{k,i} \mathbf{x}_k + \mathbf{w}_{k,i} + \mathbf{b}_{k,i} = \mathbf{z}_{k,i} + \mathbf{b}_{k,i} \quad (3)$$

where $\mathbf{z}'_{k,i}$ is the corrupted measurement, $\mathbf{b}_{k,i}$ is false information injected into the i th sensor at time k , it is either an unknown constant or a random variable independent of $\{\mathbf{v}_{k,i}\}$ and $\{\mathbf{w}_{k,i}\}$. Let us define $\mathbf{b}_k = [\mathbf{b}_{k,1}, \dots, \mathbf{b}_{k,M}]^T$ as the bias vector containing false information at all the sensors.

III. IMPACT OF FALSE INFORMATION INJECTION

Let us first assume that the adversary attacks the system by injecting false information into the sensors while the Kalman filter is unaware of such attacks. We start with the case where biases (\mathbf{b}_k) are continuously injected into the system starting from a certain time K . Note that single injection is just a special case of continuous injection when \mathbf{b}_k are set to be nonzero at time K and zero otherwise.

In the continuous injection case, the Kalman filter's extra mean square error (EMSE), which is caused by the continuous bias injection alone, is derived in [11] and provided as follows.

Proposition 1. *When the bias sequence $\{\mathbf{b}_k\}$ is zero mean, random, and independent over time, the EMSE at time $K + N$ due to the biases injected at and after time K , denoted as \mathbf{A}_{K+N} , is*

$$\mathbf{A}_{K+N} = \sum_{m=0}^N \mathbf{D}_m \boldsymbol{\Sigma}_{K+N-m} \mathbf{D}_m^T \quad (4)$$

where $\mathbf{D}_m = \left(\prod_{i=0}^{m-1} \mathbf{B}_{K+N-i} \right) \mathbf{W}_{K+N-m}$, and $\mathbf{B}_K = (\mathbf{I} - \mathbf{W}_K \mathbf{H}_K) \mathbf{F}_{K-1}$. $\prod_{i=0}^{-1} \mathbf{B}_{K+N-i} = \mathbf{I}$ is an identity matrix, \mathbf{W}_K is the Kalman filter gain [12], and $\boldsymbol{\Sigma}_{K+N-m}$ is the covariance matrix of \mathbf{b}_{K+N-m} .

In [9], we investigated the optimal attack strategy that an adversary can adopt to maximize the system estimator's estimation error. The problem can be formulated as a constrained optimization problem. Without loss of generality, let us assume that the attacker is interested in maximizing the system state estimation error at time K right after a single false bias is injected at time K . In this case, we are interested in designing the injected random bias' covariance matrix such that

$$\begin{aligned} \max_{\boldsymbol{\Sigma}_K} & \text{Tr} [\mathbf{P}_{K|K} + \mathbf{A}_K(\boldsymbol{\Sigma}_K)] \\ \text{s.t.} & \text{Tr}(\boldsymbol{\Sigma}_K) = a^2 \end{aligned} \quad (5)$$

where a^2 is a constraint on the power of the injected noise, $\text{Tr}(\cdot)$ is the matrix trace operator, and $\mathbf{P}_{K|K}$ is the Kalman filter's state covariance matrix at time K in the absence of any false information. For both the cases where the attacker injects independent noises and dependent noises to position-only sensors in an object tracking system, we have derived the optimal strategies to maximize the trace of the state estimation MSE matrix as provided in the following two propositions [9].

Proposition 2. *For a system with M sensors, if the adversary injects independent random noises, the best strategy is to allocate all the power to the sensor with the smallest measurement noise variance.*

Proposition 3. *For a system with M sensors, the optimal strategy for the adversary is to inject dependent random noises with a pairwise correlation coefficient of 1. The noise power is allocated such that $\sigma_{b_i} = \frac{c_i a}{\sqrt{\sum_{j=1}^M c_j^2}}$, $i \in \{1, \dots, M\}$, where σ_{b_i} is the standard deviation (s.d.) of the noise injected to the i th sensor, $c_i = \frac{1/\sigma_{w_i}^2}{\sum_{j=1}^M (1/\sigma_{w_j}^2)}$ and σ_{w_i} is the i th position-only sensor's measurement noise s.d.*

IV. A TARGET TRACKING EXAMPLE

In this paper, we give a concrete target tracking example, and assume that the target moves in a one-dimensional space according to a discrete white noise acceleration model [12], which can still be described by the plant and measurement equations provided in (1) and (2). In such a system, the state is defined as $\mathbf{x}_k = [\xi_k \ \dot{\xi}_k]^T$, where ξ_k and $\dot{\xi}_k$ denote the target's position and velocity at time k respectively. The input \mathbf{u}_k is a zero sequence. The state transition matrix is

$$\mathbf{F}_k = \begin{bmatrix} 1 & \Delta \\ 0 & 1 \end{bmatrix}, \quad \forall k \quad (6)$$

where Δ is the sensor sampling interval. The process noise is $\mathbf{v}_k = \Gamma v_k$, where v_k is a zero mean white acceleration noise, with variance σ_v^2 , and the vector gain multiplying the scalar process noise is given by $\Gamma = [\Delta^2/2 \ \Delta]^T$. The covariance matrix of the process noise is therefore $\mathbf{Q} = \sigma_v^2 \Gamma \Gamma^T$. The observation matrix in (2) is given as

$$\mathbf{H}_{k,i} = [1 \ 0], \quad \forall k, i \quad (7)$$

Once the system model is known, it is straightforward for both the Kalman filter and the adversary to calculate the Kalman filter's state covariance matrix $\mathbf{P}_{K|K}$ as in [12]. Using Proposition 1, we can obtain the trace of the total state estimation MSE matrix:

$$\text{Tr}(\text{MSE}) = \text{Tr}(\mathbf{P}_{K|K} + \mathbf{W}_K \boldsymbol{\Sigma}_K \mathbf{W}_K^T) \quad (8)$$

V. NONCOOPERATIVE TWO-PERSON ZERO-SUM GAME

In a noncooperative two-person zero-sum game [13], we assume that there are two players, referred to as Players 1 and 2, and an $m \times n$ payoff matrix $\mathbf{L} = \{l_{ij}\}$. Each entry of the matrix is an outcome of the game corresponding to a particular pair of decisions made by both players. Player 1 gets m rows of the matrix as his/her strategy set, while for Player 2, the strategy set is the corresponding n columns of the same matrix.

In our problem, suppose there are totally M sensors, the Kalman filter and the adversary can choose any non-empty subsets of sensors to perform state estimation and attack respectively, which means $m = n = 2^M - 1$. \mathbf{L} is a square matrix of the size $(2^M - 1) \times (2^M - 1)$. The payoff in the game between the Kalman filter system and the adversary will be the trace of the state estimation MSE matrix. For each set of sensors he/she chooses to attack, the adversary is under a total injected noise power constraint as specified in (5). The

Nash equilibrium between the Kalman filter and the adversary is achieved by solving the minimax optimization problem.

Let $\{\text{row } i, \text{column } j\}$ be a pair of strategies adopted by the players, and the corresponding outcome (payoff) be l_{ij} , which means that Player 1 should pay Player 2 the amount of l_{ij} . If $l_{i^*j} \leq l_{i^*j^*} \leq l_{ij^*}$, for all $i = 1, \dots, m$ and all $j = 1, \dots, n$, the pair $\{i^*, j^*\}$ is said to constitute a saddle-point equilibrium, and the game is said to have a saddle point in pure strategy. On the other hand, if the pair of inequalities does not exist, one can derive the mixed strategy to obtain the equilibrium. A mixed strategy is a probability distribution on the space of the player's pure strategies. A mixed strategy allows for a player to select a pure strategy randomly with a certain probability. In this case, the utility function u is defined as

$$u(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^m \sum_{j=1}^n x_i l_{ij} y_j = \mathbf{x}^T \mathbf{L} \mathbf{y} \quad (9)$$

where \mathbf{x} and \mathbf{y} are the probability distribution vectors for the mixed strategies. Also, $\mathbf{x} \in X$, $\mathbf{y} \in Y$, where the set $X = \{\mathbf{x} \in R^m : \mathbf{x} \geq \mathbf{0}, \sum_{i=1}^m x_i = 1\}$, and Y is defined in the same way. The Kalman filter playing as defender is trying to minimize the utility function $u(\mathbf{x}, \mathbf{y})$ by choosing the best defending strategy, while the attacker wants to maximize the utility function by choosing the best attack strategy. For the payoff matrix \mathbf{L} of size $m \times n$, a vector of \mathbf{x}^* is the best mixed strategy for the Kalman filter if

$$\bar{U}_m(\mathbf{L}) = \max_{\mathbf{y} \in Y} (\mathbf{x}^*)^T \mathbf{L} \mathbf{y} \leq \max_{\mathbf{y} \in Y} \mathbf{x}^T \mathbf{L} \mathbf{y}, \mathbf{x} \in X \quad (10)$$

The $\bar{U}_m(\mathbf{L})$ is known as the average security level (loss ceiling) of the defender, the average security level (gain-floor) of the attacker \underline{U}_m can also be defined as below,

$$\underline{U}_m(\mathbf{L}) = \min_{\mathbf{x} \in X} \mathbf{x}^T \mathbf{L} \mathbf{y}^* \geq \min_{\mathbf{x} \in X} \mathbf{x}^T \mathbf{L} \mathbf{y}, \mathbf{y} \in Y \quad (11)$$

It always holds that $\bar{U}_m(\mathbf{L}) = \underline{U}_m(\mathbf{L})$ for mixed strategies in noncooperative two-person zero-sum game. The saddle point in the mixed strategies is defined when the two bounds are equal to each other, which can be found by solving the following linear programming problem [13]:

$$\begin{aligned} \min_{\mathbf{x} \in X} \quad & b_u \\ \text{s.t.} \quad & \mathbf{L}^T \mathbf{x} \leq b_u \mathbf{1} \\ & \mathbf{x}^T \mathbf{1} = 1 \\ & \mathbf{x} \geq \mathbf{0} \end{aligned} \quad (12)$$

where b_u denotes a constant upper bound. For the attacker, the formula is the other way around,

$$\begin{aligned} \max_{\mathbf{y} \in Y} \quad & b_l \\ \text{s.t.} \quad & \mathbf{L} \mathbf{y} \geq b_l \mathbf{1} \\ & \mathbf{y}^T \mathbf{1} = 1 \\ & \mathbf{y} \geq \mathbf{0} \end{aligned} \quad (13)$$

where b_l denotes a constant lower bound. From the formulation above, it is easy to see that (13) is the dual form of the

optimization problem (12). The optimal function for the two problems are the same. Interested readers are referred to [13] for more details.

VI. GAME WITH INCOMPLETE INFORMATION

So far, it has been assumed that the defender has the knowledge on what type of false information has been injected by the adversary to the sensors. In practice, this knowledge may not be readily available to the defender. So let us suppose that the Kalman filter does not know the type of false information the adversary uses to attack the system. If the adversary has S types of false information like independent or dependent false information as discussed earlier in the paper, there should be S ($m \times n$) payoff matrices $\mathbf{L}_k = \{l_{kij}\}$, and $\sum_{k=1}^S p_k = 1$, $k \in S$. Based on p_k , the prior probability of the k th false information type, the Bayesian equilibrium can be achieved by solving the following linear optimization problem.

$$\begin{aligned} \min_{\mathbf{x} \in X} \quad & b_u \\ \text{s.t.} \quad & \sum_{k=1}^S p_k \mathbf{L}_k^T \mathbf{x} \leq b_u \mathbf{1} \\ & \mathbf{x}^T \mathbf{1} = 1 \\ & \mathbf{x} \geq \mathbf{0} \end{aligned} \quad (14)$$

where b_u denotes a constant upper bound.

VII. NUMERICAL RESULTS

In the example, for simplicity and ease of presentation, we assume that there are three sensors denoted as $\{z_1, z_2, z_3\}$ in the system having independent measurement noises with noise standard deviations $\sigma_{w_1} = 3$, $\sigma_{w_2} = 4$, $\sigma_{w_3} = 5$. The system process noise s.d. is $\sigma_v = 0.5$, sensors's sampling interval is $\Delta = 1s$, and the system initial state \mathbf{x}_0 is assumed to follow a $\mathcal{N}(\hat{\mathbf{x}}_{0|0}, \mathbf{P}_{0|0})$ distribution, where $\hat{\mathbf{x}}_{0|0} = [1 \ 1]^T$ and

$$\mathbf{P}_{0|0} = \begin{bmatrix} 0.25 & 0.25 \\ 0.25 & 0.5 \end{bmatrix}.$$

The adversary can choose any combination of sensors from the set $P_1 = \{z_1, z_2, z_3, z_1 z_2, z_1 z_3, z_2 z_3, z_1 z_2 z_3\}$ to attack with the power constraint of $\sum_{i=1}^3 \sigma_{b_i}^2 = 100$, where σ_{b_i} is the s.d. of the random noise injected to Sensor i . Likewise, the defender can choose any combination of sensors to perform state estimation, and its strategy set is the same: $P_2 = P_1$. The game is played as below: if the defender uses data from Sensors i and j for state estimation, while the adversary attacks Sensors i and k , then system state estimation is affected by the false information from the i th sensor only.

In this game, the trace of the state estimation MSE matrix is regarded as the payoff of the game. In the games of the independent and dependent attacks, the system is attacked according to the strategies provided in Propositions 2 and 3 respectively. Let us assume that the adversary attacks the sensors at time $k = 100$, and the payoff matrix is given

TABLE I
PAYOFF MATRIX (INDEPENDENT CASE)

KF/At	z_1	z_2	z_3	z_1z_2	z_1z_3	z_2z_3	$z_1z_2z_3$
z_1	25.4	4.7	4.7	25.4	25.4	4.7	25.4
z_2	7.2	23.5	7.2	7.2	7.2	23.5	7.2
z_3	10	10	23.6	10	10	10	10
z_1z_2	13.5	6.6	3.4	13.5	13.5	6.6	13.5
z_1z_3	16.4	3.8	5.4	16.4	16.4	3.8	16.4
z_2z_3	5.0	12.4	8.0	5.0	5.0	12.4	5.0
$z_1z_2z_3$	10.2	5.2	3.9	10.2	10.2	5.2	10.2

TABLE II
PAYOFF MATRIX (DEPENDENT CASE)

KF/At	z_1	z_2	z_3	z_1z_2	z_1z_3	z_2z_3	$z_1z_2z_3$
z_1	25.4	4.7	4.7	13.2	15.9	4.7	10.3
z_2	7.2	23.5	7.2	9.3	7.2	13.3	8.6
z_3	10	10	23.6	10	11.0	12.1	10.5
z_1z_2	13.5	6.6	3.4	16.7	12.4	5.6	15.6
z_1z_3	16.4	3.8	5.4	15.0	18.1	4.2	15.0
z_2z_3	5.0	12.4	8.0	6.8	5.3	15.5	8.2
$z_1z_2z_3$	10.2	5.2	3.9	12.5	11.1	6.2	13.4

in Tables I and II. From Tables I and II, we can see that there is no pure strategy Nash Equilibrium. Instead, we use mixed strategies to find the Nash Equilibrium. In order to obtain the optimal probability distribution vector, we solve the optimization problem formulated in (12). The solution to (12) is the optimal probability vector for the defender, and the dual solution is the optimal mixed strategy for the attacker. The optimal solutions for independent- and dependent-attack cases are shown in Tables III and IV respectively.

For the independent case, we can see from Table I that (6, 6) and (7, 7) elements of the payoff matrix (\mathbf{L}) are the smallest among the seven diagonal elements. This means that in the worst cases for the KF when its chosen sensor combination happens to be the same as that being attacked by the adversary, the strategies z_2z_3 and $z_1z_2z_3$ will lead to the smallest state estimation MSEs. In addition, for the KF, the values of last two rows are relatively small. As a result, for the KF, the probabilities of the last two strategies (z_2z_3 and $z_1z_2z_3$) are much larger than those of other strategies, which are shown in Table III.

In the dependent case, for the KF, the probabilities for the last two pure strategies (z_2z_3 and $z_1z_2z_3$) are relatively large as shown in Table IV. This can be explained similarly as in the independent case. In \mathbf{L} , the entries of the rows corresponding to z_3 , z_1z_2 , and z_1z_3 are relatively large, so the KF assigns nearly zero probabilities to these three strategies. In the first two rows of \mathbf{L} , even though the diagonal elements are large, the rest of the elements are relatively small, so strategies z_1 and z_2 are assigned significant probabilities for the KF as shown in Table IV.

When the information is incomplete, the defender is not sure whether independent or dependent false information will be injected by the adversary. Table V shows the Kalman filter's best defending strategy under the condition that the Kalman

TABLE III
OPTIMAL STRATEGY PROBABILITIES (INDEPENDENT CASE)

$Player$	z_1	z_2	z_3	z_1z_2	z_1z_3	z_2z_3	$z_1z_2z_3$
KF	0.00	0.00	0.00	0.00	0.00	0.40	0.60
Attacker	0.14	0.22	0.00	0.14	0.14	0.22	0.24

TABLE IV
OPTIMAL STRATEGY PROBABILITIES (DEPENDENT CASE)

$Player$	z_1	z_2	z_3	z_1z_2	z_1z_3	z_2z_3	$z_1z_2z_3$
KF	0.16	0.14	0.00	0.00	0.00	0.37	0.33
Attacker	0.14	0.02	0.00	0.00	0.00	0.34	0.50

filter can be attacked by the two types of false information equally probably. This result could be explained by the results for the case with complete information about the type of attacks. Clearly from Tables III and IV, the defender assigns significant probabilities to the last two strategies (z_2z_3 and $z_1z_2z_3$). As a result, the optimal strategy for the case with incomplete knowledge of the type of the false information also assigns most probabilities to the last two strategies.

We also provide a simulation result to demonstrate the optimality of the derived strategy for the independent case. In this example, four different scenarios are explored: 1) there is no attack and the KF uses all the sensors' data; 2) the KF uses the optimal mixed strategy; 3) the KF uses a mixed strategy to pick each pure strategy with an equal probability 1/7; 4) the KF always chooses the first sensor to do the system estimation. In Scenarios 2)-4), the attacker injects false information according to his/her optimal mixed strategy to the sensors at time $k = 100$. The resulting position estimation MSEs are plotted in Fig. 1. It is clear that the optimal mixed strategy provides the best defense against the attacker, with the minimum increase in the MSE after the attack. Fig. 2 shows the case when the defender's knowledge about the attacking false information is incomplete. Let us suppose that Kalman filter can be attacked by independent and dependent false information with equal probability. The results corresponding to three different defending strategies, the best defending strategy for independent attacks, the best defending strategy for dependent attacks, and the best defending strategy for incomplete information case, are shown in Fig. 2. It is clear that the optimal defending strategy derived from (14) leads to smaller MSE after the attack than the other two defending strategies corresponding to the independent and dependent attacks respectively.

TABLE V
OPTIMAL STRATEGY PROBABILITIES (INCOMPLETE INFORMATION CASE)

$Player$	z_1	z_2	z_3	z_1z_2	z_1z_3	z_2z_3	$z_1z_2z_3$
KF	0.00	0.00	0.00	0.00	0.00	0.45	0.55

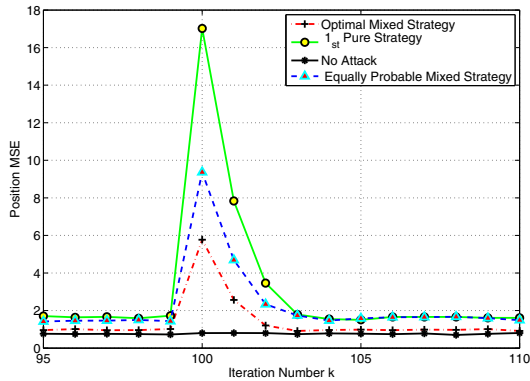


Fig. 1. Optimal Mixed Strategy vs. Other Options

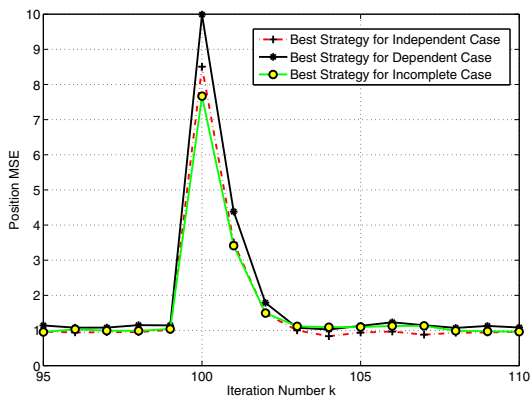


Fig. 2. Optimal Mixed Strategy vs. Other Options with Incomplete Information about Attacks

VIII. CONCLUSION

In this paper, we investigated the relationship between the Kalman filter and the adversary in a two-person zero-sum game. The Kalman filter (defender) tries to achieve more accurate system state estimation and avoid being attacked by the adversary. The adversary tries to mislead the Kalman filter as much as possible. Both sides of the game will reach a Nash Equilibrium through the mixed strategies. Using minimax techniques, we found the mixed strategy saddle point in the game. In the future, we will put more practical constraints in our problem by letting both players in the game have more limited information about the other player and introduce the detection mechanism to the Kalman filter system.

REFERENCES

[1] Y. Liu, M.K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. the 16th ACM Conference on Computer and Communications Security*, Chicago, IL, November 2009.

[2] L. Jia, R.J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *Proc. International Conference on Acoustics, Speech, and Signal Processing*, Prague, Czech Republic, May 2011, pp. 5952–5955.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attack on Smart Grid State Estimation: Attack Strategies and Countermeasures," in *Proc. First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, Oct. 2010, pp. 220–225.

[4] L. Jia, R. J. Thomas, and L. Tong, "On the nonlinearity effects on malicious data attack on power system," in *Power and Energy Society General Meeting*, San Diego, CA, July 2012, pp. 1–8.

[5] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. Global Communications Conference*, San Diego, CA, Dec. 2012, pp. 3153–3158.

[6] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1460–1470, July 2014.

[7] X. Song, P. Willett, S. Zhou, and P. B. Luh, "The mimo radar and jammer games," *IEEE Trans. on Signal Processing*, vol. 60, no. 2, pp. 687–699, February 2012.

[8] R. Niu and L. Huie, "System State Estimation in the Presence of False Information Injection," in *Statistical Signal Processing Workshop (SSP)*, Ann Arbor, MI, Aug. 2012, pp. 385–388.

[9] J. Lu and R. Niu, "False Information Injection Attack on Dynamic State Estimation in Multi-Sensor Systems," in *Proc. of the 17th International Conference on Information Fusion*, Salamanca, Spain, July 2014.

[10] J. Lu and R. Niu, "Malicious Attacks on State Estimation in Multi-Sensor Dynamic Systems," in *Proc. of the 2nd IEEE Global Conference on Signal and Information Processing*, Atlanta, GA, December 2014.

[11] R. Niu, "Dynamic System State Estimation in the Presence of Continuous False Information Injection," Tech. Rep., Extension Grant from Visiting Faculty Research Program, Air Force Research Laboratory Information Directorate, March 2012.

[12] Y. Bar-Shalom, X.R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*, Wiley, New York, 2001.

[13] T. Basar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, Society for Industrial and Applied Mathematics, Philadelphia, PA, 1999.