Deception Attack Detection using Reduced Watermarking

Arunava Naha\(^1\), André Teixeira\(^1\), Anders Ahlén\(^1\) and Subhrakanti Dey\(^2\)

Abstract—The addition of physical watermarking to the control input is a well-adopted technique to detect the data deception attacks on the cyber-physical systems. However, the addition of the watermarking increases the control cost. On the other hand, the attack might be a rare event. In this paper, we propose to reduce the control cost when the system is not under attack by adding the watermarking as and when needed depending on a posterior probability of attack. We first formulate a stochastic optimal control problem, and then solve it using dynamic programming by keeping a balance between the detection delay, false alarm rate (FAR), and the reduction in control cost. We numerically find two thresholds from the value iterations, \(T_h\) and \(T_{h,u}\). \(T_h\) is greater than \(T_{h,u}\), for the posterior probability of attack \(P_u\). If \(P_u\) is greater than or equal to \(T_h\), then the watermarking signal is added for the \((k+1)\)-th instant of time. On the other hand, if \(P_u\) greater than or equal to \(T_{h,u}\), then we declare that the system is under attack. We have provided simulation results to illustrate our approach. For the example system model considered in this paper, we have achieved a considerable reduction in the control cost during the normal operation compared to the case where watermarking is always present without sacrificing much in the detection delay.

I. INTRODUCTION

Large cyber-physical systems (CPS) employing networked controls are getting deployed for various safety-critical applications, such as intelligent transportation, smart grids, manufacturing industries, etc. [1]. However, the use of commodity software and off-the-shelf components for networking and computation make the CPS vulnerable to the attacks [2]. Before we go for large scale implementations of the CPS for various safety-critical applications, such vulnerabilities must be addressed. Several effective protection schemes, such as cryptography, firewall, digital watermarking, etc. are in place to protect the cyber layer of the CPS. However, such protection schemes may not be adequate to protect the physical layer of the CPS against the data deception attacks and denial of service (DoS) attacks. There are multiple incidents in the past where the attacker successfully caused damage to the CPS despite the presence of various protection schemes for the cyber layer [2]. Stuxnet attack is probably the most famous one [3]. In the data deception attack, the attacker replaces the true observations and/or the actual control inputs with fake data and/or harmful exogenous inputs. In one form of data deception attacks, the attacker records the true observations and replays it back at some later point in time. Such attacks are called replay attacks, and the Stuxnet attack was an incident of a replay attack. In the DoS, the attacker overpowers the wireless communication channel so that the required information could not be transmitted. Attacks on the physical layer can cause monetary loss as well as it can pose serious threats to human safety. Therefore, it is of immense importance to detect the attack on the CPS as soon as possible to reduce the amount of damage.

In this paper, we have studied the problem of data deception attacks where the attacker replaces the true observations either with the fake data generated from a separate stochastic process or with the previous recordings of the true observations. A well-adopted technique to detect such data deception attacks on the networked control systems (NCS) is to add the watermarking signals to the control inputs. The watermarking signals may be generated randomly from some Gaussian distributions [4] or hidden Markov models (HMM) [2]. Attacks are generally detected by different statistical tests on the innovation signal [2] or the observations [5]. Such methods are studied intensively in the literature [2], [5]. However, the addition of the watermarking increases control cost. In [2], the authors provide an analytical expression for the increase in the linear quadratic Gaussian (LQG) control cost if the watermarking is added to the control inputs for every time instants during the normal operation of the system.

Since the attack on the system can be considered to be a rare event, the addition of the watermarking to the system operating under the normal conditions for a long time will increase the total control cost significantly. There are few approaches found in the literature that address the problem of increased control cost due to the added watermarking. In one approach, the authors add periodic watermarking to reduce the control cost and keep a balance between the improvement in terms of the control cost and the increase in the detection delay [6]. In another approach, the researchers add or multiply the watermarking signals to the observations before the transmission. At the receiver end, the watermarking signals are filtered out before feeding the observations to the controller. Therefore, the control cost does not increase. In [7], each output is modulated by a watermarking signal before the transmission. In [8], authors use pairs of filters to add and remove sinusoidal watermarking signals, whereas, in [9], random noise watermarking signals are used. However, if the attacker can hijack the sensor node and replaces the true observations before the addition of the watermarking, then such methods may not be able to detect the attacks.

In this paper, we have devised an adaptive technique for

---

\(^{1}\)Arunava Naha, André Teixeira, and Anders Ahlén are with the Department of Electrical Engineering, Uppsala University, 751 03 Uppsala, Sweden arunava.naha@angstrom.uu.se, andre.teixeira@angstrom.uu.se, and anders.ahlen@angstrom.uu.se

\(^{2}\)Subhrakanti Dey is with the Department of Electronic Engineering, Hamilton Institute, National University of Ireland, Maynooth, Ireland. He is also with the Department of Electrical Engineering, Uppsala University, 751 03 Uppsala, Sweden Subhra.Dey@signal.uu.se

---

\(^{*}\)This work is supported by The Swedish Research Council (VR) under grants 2017-04053 and 2018-04396, and by the Swedish Foundation for Strategic Research.
adding watermarking to reduce the control cost during the normal operation of the system. The proposed watermarking scheme is formulated as an optimal stochastic control problem inspired by the method of reducing the sampled data required to detect a change in a process [10]. In [10], a Bayesian sequential detection technique is applied, which is asymptotically optimal under certain conditions [11]. One of the conditions is that the prior distribution of the change point should obey either of the following two conditions, see (1) and (2). In our study, we assume the attack start point $\Gamma$ to be a random variable (RV) having a geometric distribution with parameter $\rho$, which is similar to several other literature [10], [12]. A geometric prior distribution of the attack start point meets the condition given in (1).

\[
\lim_{k \to \infty} \frac{\log P \{ \Gamma \geq k + 1 \}}{k} = -c, \quad c > 0,
\]

\[
\lim_{k \to \infty} \frac{\log P \{ \Gamma \geq k + 1 \}}{k} = 0, \quad k \in \mathbb{N}.
\]

At every time step $k$, we need to make two decisions, 1) whether to add the watermarking for the $k+1$-th time instant, 2) whether to accept that the attack is present in the system. We have used dynamic programming to find the optimal policy that will minimize the average detection delay (ADD) subject to some constraints on the false alarm rate (FAR) and the average number of times the watermarking (ANW) is added. By solving the optimization problem using dynamic programming, we find two thresholds $Th_c$ and $Th_a$ for the posterior probability of attack $p_k$. If for the $k$-th instant, the posterior probability $p_k \geq Th_a$, then the watermarking signal is added to the $k+1$-th instant control input $u_{k+1}$. On the other hand, if $p_k \geq Th_d$, then it is decided that the attack is present in the system, i.e., $k \geq \Gamma$. We have illustrated the proposed technique by numerical results from the simulation of a single-input-single-output (SISO) system under attack and no-attack conditions.

This paper is organized as follows. Section II provides the system model under normal and attack conditions. Section III explains the problem formulation and the proposed solution in detail. Section IV discusses the numerical results, and Section V concludes the paper.

II. SYSTEM MODEL

The system model during normal operations and the model with the data deception attack are discussed in this section.

A. System model during normal operation

A schematic diagram of the NCS, considered in this paper, during the normal operation is shown in Fig. 1. The state update and the measurement equations of the linear and time-invariant SISO system are given as

\[
x_k = Ax_{k-1} + Bu_{k-1} + w_{k-1}, \quad k \in \mathbb{N},
\]

\[
y_k = Cx_k + v_k,
\]

where $x_k$ and $u_k$ are the state and input variables at the $k$-th instant. $y_k$ is the observation at the $k$-th instant. The process noise $w_k$ and the observation noise $v_k$ are assumed to be independent and identically distributed (iid) zero-mean Gaussian processes with variances $Q$ and $R$ respectively. $w_k$ and $v_k$ are uncorrelated with each other, and both are uncorrelated to the initial state $x_0$. All the quantities in (3) and (4) are real and scalar. We also assume that the system was started a long time ago and currently is at a steady-state. The Kalman filter is used to estimate the state as follows,

\[
\dot{x}_{k|k} = A\dot{x}_{k-1|k-1} + Bu_{k-1}, \quad k \in \mathbb{N},
\]

\[
\dot{x}_{k|k} = \dot{x}_{k|k-1} + K\gamma_k,
\]

\[
\gamma_k = y_k - C\dot{x}_{k|k-1}.
\]

The steady-state Kalman gain $K$ is as follows,

\[
K = CP(C^2P + R)^{-1}.
\]

Here, $P = E\left\{ (x_k - \dot{x}_{k|k-1})^2 \right\}$, which can be obtained from the solution to the following algebraic Riccati equation,

\[
P = A^2P + Q - A^2C^2P^2(C^2P + R)^{-1}.
\]

The optimal control signal $u^*_k$ is derived by minimizing the following infinite horizon LQG cost,

\[
J_{lqg} = \lim_{T \to \infty} E \left[ \frac{1}{2T+1} \sum_{k=-T}^{T} \left( Wx_k^2 + Uu_k^2 \right) \right],
\]

where $W$ and $U$ are the two positive weights. The LQG control policy gives a fixed-gain linear control signal as

\[
u_k^* = L\dot{x}_{k|k},
\]

and $L = -ABS(B^2S + U)$.

Here, $S$ is the solution to the following algebraic Riccati equation,

\[
S = A^2S + W - A^2B^2S^2(B^2S + U)^{-1}.
\]

B. Attack Model

We assume that the attacker has access to the sensor nodes and can replace the true observations with fake data. We also assume that the attacker has complete knowledge about the system parameters, i.e., $A$, $B$, $C$, $Q$, and $R$, and the control policy, i.e., $L$. However, the attacker can not alter the control signal. The attacker replaces the true observations $y_k$ by the fake data $z_k$ from $k \geq \Gamma$. The fake observation data $z_k$ is
assumed to be generated from a general stationary stochastic process as
\[ z_k = \alpha z_{k-1} + w_{a,k-1}, \]  
(14)
where \( \alpha \) is the attacker’s system parameter and \( w_{a,k} \) is the iid noise. \( w_{a,k} \sim \mathcal{N}(0, Q_a) \). Such an attack model can also be used for sequential replay attack detections after a few modifications as studied in [13]. The following statistics can be derived from (14).

\[
E[z_k^2] = \sigma_z^2 = \frac{Q_a}{1 - \alpha}, \quad \text{and} \quad E[z_k z_{k-k_0}] = \alpha^{k_0} \sigma_z^2, \quad [\alpha < 1].
\]

(15)
(16)

The attacker’s system parameters \( \sigma_z^2 \) and \( \alpha \) can be estimated online from the received observations, which will operate in parallel with the attack detection algorithm. During the attack, the Kalman predicted and filtered states are denoted as \( \hat{x}^F_{k|k-1} \) and \( \hat{x}^F_{k|k} \), respectively, which are derived from (5) and (6), but the innovation signal \( \gamma_k \) during the attack takes the following form,

\[ \gamma_k = z_k - C \hat{x}^F_{k|k-1}. \]

(17)
We assume that the defender will know the estimated values of \( \sigma_z^2 \) and \( \alpha \).

A schematic diagram of the system under the data deception attack is shown in Fig. 2.

![Schematic diagram of the system under attack](image)

**Fig. 2:** Schematic diagram of the system under attack.

The attack start point \( k = \Gamma \) is assumed to be a RV with a geometric distribution of parameter \( \rho \), where \( 0 < \rho < 1 \). Therefore, the probability \( \Pi_k = \mathbb{P}\{\Gamma = k\} \) will be [10]

\[
\Pi_k = \mathbb{P}\{\Gamma = k\} = \Pi_0 \mathbb{I}_{\{k=0\}} + (1 - \Pi_0) \rho (1 - \rho)^{k-1} \mathbb{I}_{\{k\geq 1\}}.
\]

(18)

Here, \( \Pi_0 = \mathbb{P}\{\Gamma \leq 0\}, i.e., \Pi_0 \) is the probability of the attack happening before the start of the observation time \( k = 0 \). \( \mathbb{I}_{\{condition\}} \) is the indicator function, \( \mathbb{I}_{\{condition\}} = 1 \) if the condition is satisfied, otherwise, \( \mathbb{I}_{\{condition\}} = 0 \). In general, \( 0 \leq \Pi_0 < 1 \). However, for our problem formulation we have taken \( \Pi_0 = 0 \). The defender does not know the exact value of the attack start point \( \Gamma \), but he knows about the prior distribution of \( \Gamma \) and the geometric distribution parameter \( \rho \).

### III. Defence Mechanism

In this section, we discuss the proposed defence mechanism against the data deception attack by adaptively adding watermarking to the control input.

#### A. Watermarking the Inputs

For attack detection, we perform hypothesis testing to decide from the following two hypotheses.

\( H_0 \): No attack present.

\( H_1 \): Attack present in the system.

We add iid zero-mean Gaussian noise watermarking signal \( e_k \) with variance \( \sigma_e^2 \) to the optimal LQG control input \( u_k^* \) to authenticate the observations. The addition of watermarking increases the attack detectability [2], at the same time, it also increases the control cost. If watermarking is added to the input signal for every \( k \)-th instant of time, then the increase in the LQG control cost, \( \Delta LQG \), during the normal system operation becomes [4]

\[
\Delta LQG = \left( U + B^2 (W + L^2 U) \left[ 1 - (A + BL)^2 \right]^{-1} \right) \sigma_e^2.
\]

(19)

\( \Delta LQG \) is the time average of the increase in the control cost. Since an attack is a rare event, the system is expected to run normally for a long time. Therefore, the increase in the total control cost becomes significant over time. Hence, we propose an adaptive technique for the addition of watermarking to reduce the average number of times we add the watermarking, i.e., ANW, to the control input. The reduction in the watermarking will reduce the control cost compared to the case where watermarking is present all the time. We decide to add the watermarking or to declare an attack is present in the system based on the posterior probability \( p_k \) defined as follows,

\[
p_k \triangleq \mathbb{P}\{\Gamma \leq k|\mathcal{I}_k\}.
\]

(20)
\( \mathcal{I}_k \) is the set of all available information up to the \( k \)-th instant of time. Therefore, we need two decision variables, \( s_k \) and \( d_k \) as follows,

\[
s_k = \begin{cases} 0, & \text{no watermarking for} \ (k+1)\text{-th time instant} \\ 1, & \text{add watermarking for} \ (k+1)\text{-th time instant}. \end{cases}
\]

(21)

\[
d_k = \begin{cases} 0, & \text{Hypothesis } H_0 \ \text{selected} \\ 1, & \text{Hypothesis } H_1 \ \text{selected}. \end{cases}
\]

(22)

A schematic diagram of the system with need-based watermarking is shown in Fig. 3. The input signal under the proposed defence mechanism takes the following form,

\[
u_k = u_k^* + s_k-1 e_k.
\]

(23)

Detection of attacks without the watermarking is a limiting case for the proposed scheme, where \( \sigma_e^2 = 0 \). However, such a choice will result in a large detection delay.

![Schematic diagram of the system with need-based watermarking](image)

**Fig. 3:** Schematic diagram of the system with need-based watermarking.
B. Selection of test data

The innovation signals before and after the attack, $\gamma_k$ and $\tilde{\gamma}_k$, for the watermarking input, take the following forms [4],

\[
\gamma_k = CA (x_{k-1} - \hat{x}_{k-1|k-1}) + CW_{k-1} + \nu_k, \quad (24)
\]

\[
\tilde{\gamma}_k = z_k - C (A + BL) \hat{x}_{k-1|k-1} - CBE_{k-1}. \quad (25)
\]

Therefore, the innovation signal $\gamma_k$ before the attack is uncorrelated to the watermarking signal $e_{k-1}$, and on the contrary, the innovation signal $\tilde{\gamma}_k$ after the attack is correlated with the watermarking signal $e_{k-1}$. Such property motivates the use of the innovation signal as the test data for attack detections. If the watermarking is added to the input, then we use the joint distributions of the innovation signal and the watermarking signal, because it increases the Kullback-Leibler divergence (KLD) between the two distributions

\[
KLD(\gamma_k, \tilde{\gamma}_k) = \int p(\gamma_k) \log \frac{p(\gamma_k)}{p(\tilde{\gamma}_k)} d\gamma_k \]

Now, the optimization problem can be formulated as

\[
\min_{u_d} ADD \quad \text{s.t.} \quad FAR \leq FAR_{th}, \quad (33)
\]

\[
ANW \leq ANW_{th},
\]

where $FAR_{th}$ and $ANW_{th}$ are the thresholds for $FAR$ and $ANW$ respectively. $u_d$ represents the policy for the decision variables $s_k$ and $d_k$. The control space of the stochastic optimization problem under study is finite, and we have discretized the state-space into a finite set. From the accessibility hypothesis as defined in [14], the constrained optimization problem of (33) can be converted into an unconstrained Lagrangian form as follows [10], [14],

\[
J^* = \min_{u_d} ADD + \lambda_f FAR + \lambda_e ANW, \quad (34)
\]

where $\lambda_f > 0$ and $\lambda_e > 0$ are the Lagrangian multipliers.

Now, the system can be in one of the following three stages at any $k$-th instant of time, see (35).

\[
\theta_k = \begin{cases} 
0 & \text{No attack,} \\
1 & \text{System under attack,} \\
T_e & \text{Termination stage, attack detected.}
\end{cases}
\]

C. Problem Formulation

Our objective is to find the optimal policy for the decision variables, $s_k$ and $d_k$, so that it minimizes the ADD for the fixed thresholds on FAR and ANW. We define ADD, FAR, and ANW as in [10],

\[
ADD = E_1[\tau - \Gamma | \tau \geq \Gamma], \quad (30)
\]

\[
FAR = P_0[\tau < \Gamma], \quad (31)
\]

\[
ANW = E_0[N_e]. \quad (32)
\]

Here, $E_0[\cdot]$ and $E_1[\cdot]$ represent the expectation with respect to the before and after attack distributions $P_0$ and $P_1$, respectively. $\tau$ is the time when the attack is detected by the algorithm. $N_e$ is the number of times the watermarking is added before the attack start point. After the attack start point, our primary objective is to detect the attack as soon as possible to reduce the amount of damage to the CPS, and we are not concerned about the increase in the control cost.
where $T_m = p_k + (1-p_k)\rho$. $L(\tilde{\gamma}_{k+1})$ and $L(\tilde{\gamma}_{k+1}, e_k)$ are the likelihood ratios as given below,

$$L(\tilde{\gamma}_{k+1}) = \frac{f(\tilde{\gamma}_{k+1})}{f(\tilde{\gamma}_{k+1})}$$ (44)

$$L(\tilde{\gamma}_{k+1}, e_k) = \frac{f(\tilde{\gamma}_{k+1}, e_k)}{f(\tilde{\gamma}_{k+1}, e_k)}$$ (45)

where $\tilde{\gamma}_k = \gamma_k$ if $k < \Gamma$, and $\tilde{\gamma}_k = \tilde{\gamma}_k$ if $k \geq \Gamma$. $f(\cdot)$ denote the likelihoods before and after the attack respectively.

**Proof 1:** Using the Baye’s rule the recursion of $p_k$ can be proved directly [10].

The value iteration in [16] is used to solve the optimization problem (39) in the following steps.

**Step-1:** Discretize $0 \leq p_k \leq 1$ into 50 discrete levels and denote them as $i$. Therefore, $i \in \{1, 2, \ldots, 50\}$.

**Step-2:** Simulate the system model as given in Section II with and without the watermarking for several test runs.

1) Attack start point $\Gamma$ selected from a geometric distribution with parameter $\rho$.

2) Likelihood ratios are evaluated using the distributions given in (26) to (29).

3) Evaluate and store $p_k$ for all $k$ using (43). We assume $p_0 = 0$.

4) Convert the real valued $p_k$ into the discrete level as defined in Step-1.

5) Two state transition matrices $P_{ne}$ and $P_e$ are estimated for the systems without and with the watermarking, respectively. The maximum likelihood estimation technique is used for the $50 \times 50$ state transition matrix evaluation.

**Step-3:** Run the following value iteration, see (46), several times till it converges for each grid point of the search space bounded by $0 \leq \lambda_f \leq 1000$ and $0 \leq \lambda_e \leq 1$.

$$T^{k+1}J = \min_{u_{d,k}} \left[ g(u_{d,k}) + P_{ne} [T^kJ]_{\{d_k=0\}} \chi_{\{s_k=0\}} + P_e [T^kJ]_{\{d_k=0\}} \chi_{\{s_k=1\}} \right]$$ (46)

Here, $T$ represents the transformation operator. $J$ and $g(u_{d,k})$ are given as

$$J = [J(1) \cdots J(50)]^T,$$ (47)

$$g(u_{d,k}) = [g_{E,k}(1, u_{d,k}) \cdots g_{E,k}(50, u_{d,k})]^T.$$ (48)

$J(i)$ represents the cost function value when the initial state is $i$. $g_{E,k}(i, u_{d,k})$ is derived from (42) by replacing the discrete state $i$ with a corresponding real value of $p_k$. The decision variable $u_{d,k}$ has three discrete level to choose from, as given in Table I.

<table>
<thead>
<tr>
<th>$u_{d,k}$</th>
<th>$d_k$</th>
<th>$s_k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Remark 1:** Depending on the selected parameters, there could also be a three-threshold policy. Two thresholds, say $Th_e$ and $Th_{e2}$, and one threshold, $Th_d$, which makes the third threshold unnecessary.

**IV. NUMERICAL RESULTS**

We have considered a SISO system for the numerical simulations. The system is open-loop unstable. All the parameters needed for the simulation are as follows, $A = 1.1$, $B = C = R = Q = W = 1$, $U = 0.4$, $\sigma_i^2 = 5$, $\alpha = 0.5$, and $\rho = 0.01$.

Figure 4 shows the optimal decision variable $u_{d,k}^*$ with respect to different values of $p$ for three different values of $\lambda_f$, where $\lambda_e$ is kept fixed. We can observe two distinct thresholds, $Th_e$ and $Th_d$, which decide the addition of the watermarking and the presence of an attack, respectively. With the increase in $\lambda_e$, the threshold $Th_e$ also charges to a higher value. Higher $Th_e$ reduces the amount of the watermarking added, but at the same time, it increases the ADD as shown later.

**Figure 4:** Optimal policy for different $\lambda_e$ but fixed $\lambda_f$.

Figure 5 shows the optimal decision variable $u_{d,k}^*$ with respect to different values of $p$ for three different values of $\lambda_f$, while $\lambda_e$ is kept fixed. Comparing the plots, we can comment that $\lambda_f$ controls the threshold $Th_{d}$, which decides whether the attack is present in the system or not. Higher $\lambda_f$ increases $Th_{d}$, which in turn reduces the FAR, but increases ADD as shown later. It is also observed from Figure 4 and Figure 5 that $\lambda_e$ does not have effect on $Th_d$ and at the same
time $\lambda_f$ does not effect $Th_e$.

Figure 6 shows two trial runs for two different values of $\lambda_e$, while $\lambda_f$ is kept fixed. We have plotted $p_k, s_k, d_k$, and the actual attack point with respect to the time index $k$. Figure 7 shows the similar plots for two different values of $\lambda_f$, while $\lambda_e$ is kept fixed. We can observe that the number of times the watermarking has been added before the attack point reduces with the increase in $\lambda_e$ and $Th_e$.

Figure 8 plots ADD and FAR vs. $\sigma_e^2$ for the proposed method, and ADD and FAR vs. $\sigma_e^2$ when the watermarking is added all the time for two different values of $\lambda_e$, while $\lambda_f$ is kept fixed. We observe the increase in ADD for the proposed method for the same FAR, but the increase is not much. For the Fig. 8.a the increase is only 12.2% at $\sigma_e^2 = 0.99$. The increase in $\lambda_f$ and $Th_d$ reduces FAR but it also increases ADD, see Fig. 9.

Figure 10 plots $\Delta LQG$ vs. $\sigma_e^2$ for the proposed method and $\Delta LQG$ vs. $\sigma_e^2$ when the watermarking is added all the time for two different values of $\lambda_e$, while $\lambda_f$ is kept fixed. We can certainly observe that we achieve a huge benefit in
V. Conclusion

The proposed method reduces the $\Delta LQG$ to a significant amount at the expense of only a small increase in the ADD. We solve the optimization problem of minimizing the ADD for the fixed thresholds on the FAR and ANW using the value iteration. The dynamic programming solution of the optimization problem provides two thresholds on the posterior probability of attack. The numerical results from the simulation of a SISO system illustrate the proposed method in details. We also provide useful insights regarding the choice of the Lagrangian multiplier values. As the future scope, the proposed method can be extended for the more general case of multi-input-multi-output (MIMO) systems. Furthermore, the analytical expressions of the ADD, FAR, and $\Delta LQG$ for the two threshold policy can be derived.

REFERENCES


