Security analysis and fault detection against stealthy replay attacks

Amirreza Zaman a, Behrouz Safarinejadian b and Wolfgang Birk a

a Control Engineering Group, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden; b School of Electrical and Electronic Engineering, Shiraz University of Technology, Shiraz, Iran

ABSTRACT
This paper investigates the security issue of the data replay attacks on control systems with the LQG controller. The attacker tries to store measurements and replay them in further times. The main novelty in this paper is stated as proposing a different attack detection criterion under the existence of a packet-dropout feature in the network by using the Kullback-Leibler divergence method to cover more general problems and with higher-order dynamics. Formulations and numerical simulations prove the effectiveness of the newly proposed attack detection procedure. Unlike previous approaches that the trade-off between attack detection delay or LQG the performance was significant, in this approach it is proved that the difference in this trade-off is not considered in early moments when the attack happens since the attack detection rate is rapid and thus, the attacks can be stopped with defense strategies in the first moments with the proposed attack detection criterion.

1. Introduction
To totalise computations, control procedures, communication networks, and physical processes, cyber-physical systems (CPSs) are used as the next generation of engineered systems (Kim & Kumar, 2012). So, cyber-physical systems are essential nowadays since based on the data transfer procedure between different technologies and components and CPS can be threatened by different malicious attackers to change the components’ data or steal them which may lead to intense irrecoverable results on the global economy, social security or even human lives irreparable damages (Poovendran et al., 2012).

During the past decade, because of the rising usage of CPS, attack strategies and defense mechanism designings are increased significantly as well. Attackers in the system consideration can be determined as malicious agents in Wireless Sensor Networks. From the attacker’s side, the goal is to degrade the system performance considerably under a condition that attackers remain undetected from the system fault detector at each time step k (Teixeira et al., 2015). One type of attack is denial-of-service attacks. These kinds of attacks try to block the communication network to barricade the accurate access to the system components.

It should be noted that the jamming process needs a lot of transmission power in networks. Since the available energy for data transfer is limited, it can often be impossible to define and analyse such attacks. Besides, attack models based on jammer for attackers which considered to be resource-constrained were investigated in Gupta et al. (2010) and Zhang et al. (2015). Furthermore, some studies have been done about obtaining optimal data-forwarding programming against remote state estimation with game-theoretic formulation by Li et al. (2015) Li et al. (2017).

Another type of cyber attacks can be organised as deception attacks. In these types of attacks, the attacker’s goal is to threaten the authenticity of the sensors and actuators’ data by injecting false data among them. One control plan against vague deception attacks of nonlinear time-delay CPSs is studied in Yoo (2020), in which an adaptive, resilient, dynamic surface control using the neural-network scheme is formulated for these attacks on both sensor and actuator. The problem of designing a distributed filter for linear discrete-time networked control systems against deception attacks and bounded disturbances is investigated in Liu et al. (2020) using a Round-Robin-type protocol to monitor communication between filters because of the communication resource constraint. In Zhang (2014), an online attack strategy is designed and proved that the procedure can degrade the estimation quality by analysing the proposed cost deviation, which showed the difference between the estimation quality with and without the proposed attack strategy. Another recent work regarding deception attacks was proposed in Chabir et al. (2018) and Keller et al. (2016), in which authors proved that switching unknown input disturbances in stochastic discrete-time linear systems can affect the networked control systems significantly subject to deception attacks. Moreover, they proposed the unknown input Kalman filter to estimate unknown disturbances by concluding that the arrival binary sequence of data drops has a Bernoulli random procedure. The attack scheduling of deception attacks for discrete-time systems with attack detection is studied in Ding et al. (2016) particularly for a class of Kalman filters with χ² detectors by assuming different types of attack scenarios (i.e. consecutive deception attacks or randomly launched deception attacks).

Furthermore, in Yang et al. (2017), a distributed state estimator with an event-triggered scheme is formulated to defend
against false data injection attacks in Wireless Sensor Networks. An approach Kwon et al. (2013) has been made recently to investigate security problems against deception attacks. In this approach Kwon et al. (2013), instead of defining a unique cyber-attack model, authors focused on analysing the system’s response during false data injection attacks. Finally, they proposed the necessary and sufficient conditions under which the attacker could perform each kind of attack without being detected. Some other classes of attacks can be defined as replay attacks. According to its name, a replay attack aims to inject fake and unreal input control signals. Also, they attempt to replay the past sensory data to keep stealthiness altogether. Some studies have been done about obtaining suitable conditions and countermeasure of replay attacks by Mo and Sinopoli (2009) and Mo et al. (2014) for linear Gaussian systems. To analyse the interchange between control efficiency and system security, some studies were done under a random game frame (Miao et al., 2013). In the case of electric power grids, work was done to inject false data into the system versus state estimation at the remote estimation centre by Liu et al. (2009). Analysing malicious data injection attacks on remote estimation performance was investigated in Mo et al. (2010). Some remarkable works have been done about studying trade-off between attack sneakiness and system performance set back for control signal infusion attack for first-order systems under \( \epsilon \)-weakly marginal sneakiness measurement scale by Bai et al. (2015) and Bai et al. (2017), and for higher-order dynamic systems with linear attack strategies by Guo et al. (2018). In addition to that, developing integrity attacks and analysing results for secure state estimation was studied by Shi et al. (2016) and Shi et al. (2017).

It is worth noting that a worst-case attacker in control CPSs can be designed optimally, and therefore, it can degrade the control system’s performance disruptively. This matter has gained much attention to consider later, and a few approaches are devoting to this matter to struct effective defense strategies. So, obtaining useful intercepted-data detectors in the existence of smart attackers is still unverified.

In this paper, the security issue of the data replay attack on control systems is investigated. The replay attacker is considered to interfere with the control system’s operation in a steady state. The attacker tries to read the sensors’ data and save their readings for a specific amount of time, and then, the attacker injects this stored data to the control system. Thus, the input data to the control system will not be the authentic real-time observed data, and the control system is not aware of this issue that can happen at any time. Therefore, by providing the wrong input control to the actuator based on the false data, the control system’s performance will be degraded quickly. This kind of attack is the most common attack occurring in the control systems. Also, the implementation of this attack is straightforward since the replay attacker just needs to be aware of the system’s steady-state behaviour and not the whole system’s dynamics. The control system in this approach is assumed to be a discrete-time linear time-invariant Gaussian control system using an infinite time horizon Linear Quadratic Gaussian (LQG) controller. As stated before, the outcomes on replay attacks’ detectability have not been defined in an integrated security scheme, and there represents not to settle a consent on the attack sneakiness’ measures. Previous work regarding detecting a replay attack (Mo & Sinopoli, 2009) applied a specific detection classic \( \chi^2 \) detector scheme as a detection criterion for a particular group of replay attacks. However, Mo and Sinopoli (2009) did not study the cases when attack policies are not rigorously stealthy to the attack’s detector. Different from the previous approach, in our work, the control system is equipped with the K-L divergence false-data detector as a measure of attack sneakiness.

Moreover, in this paper, the packet-dropout feature of the communication network is considered to derive formulas for more general cases as another case of novelty. Comparing to previous attack detection methods such as the Chi-Squared method (Mo & Sinopoli, 2009), we used Kullback-Leibler (K-L) divergence criterion to measure the replay attack’s stealthiness because based on the definition of the K-L divergence method, it is not required to define any detection windows like in Chi-Squared method. Moreover, the K-L divergence criterion can be applied to high-order nonlinear systems. Consequently, using the K-L divergence method would be independent of any specifically defined detection scheme. Therefore, our approach for replay attacks can be applied to systems with general dynamics and of higher-orders can be considered to provide security schemes. Furthermore, it is proved and illustrated that the detection response with the K-L divergence criterion and especially in this work to replay attacks, becomes so much faster than any other presented statistical detection methods.

The rest of this approach is organised as the following: In Section 2, the model of the control process is presented, and then, the state estimation procedure by considering the packet-dropout feature is analysed. Also, in Section 2, the problem is formulated by applying Kalman filter equations and optimal LQG controller with the K-L divergence fault detection criterion. In Section 3, the straightforward model of the malicious replay attack is investigated, and its influence on the control system is discussed. In Section 4, the fault detection scheduling scheme is presented in the existence of a replay attack, and its usefulness is demonstrated in Section 5. Eventually, in Section 6, the conclusion of this study is presented.

2. System architecture

In this section, the proposed problem is formulated by applying Kalman filter equations, the conventional LQG controller, and the K-L divergence fault detector for replay attacks.

Assume the general linear time-invariant (LTI) control system is described as follows:

\[
\begin{align*}
  x(k + 1) &= Ax(k) + Bu(k) + w(k) \quad (1) \\
  y(k) &= Cx(k) + v(k) \quad (2)
\end{align*}
\]

where \( x(k) \in \mathbb{R}^n \) is defined as the general vector of the state variables at each time step \( k \), \( w(k) \in \mathbb{R}^n \) is the noise of the process at time step \( k \). Also, \( y(k) \in \mathbb{R}^m \) is measurements’ vector with the measurement noise, which is defined as \( v(k) \) at time step \( k \). It is assumed that process and measurement noises are independent of each other and denoted with \( w(k) \sim N(0, W) \) and \( v(k) \sim N(0, V) \).
At every step $k$, the sensor transmits its measured data to a remote estimator. To estimate the system state in the remote estimator in a case that there is a packet dropout feature in the communication network (Shi et al., 2008), a Kalman filter is used to estimate the received data using the following equations:

$$\hat{x}(0) = \overline{x}(0), \quad P^-(0) = \Psi$$

$$\hat{x}^-(k) = A \hat{x}(k-1) + Bu(k)$$

$$P^+(k) = AP(k-1)A^T + W$$

$$K(k) = P^+(k)C^T(CP^+(k)C^T + V)^{-1}$$

$$\hat{x}(k) = \hat{x}^-(k) + \beta(k)K(k)(y(k) - C\hat{x}^-(k))$$

$$P(k) = P^-(k) - \beta(k)KK^T(k)CP^+(k)$$

It is considered that $\beta(k)$ which is the packet-dropout coefficient, is known to the attacker and the system at each time step $k$. In this approach, it is considered that $\beta(k)$ has a fixed value during the time. So, $P(k)$ and $K(k)$ will converge to steady-state values as follows:

$$P = \lim_{{k \to \infty}} P^-(k)$$

$$K = PC^T(CPC^T + V)^{-1}$$

Because of the assumption that any control systems run for a long time horizon in studies and by considering a fixed packet-dropout value, it is assumed that the control system in our approach can be run at a steady state from the starting point. In this case, the initial condition for the covariance matrix is assumed to be $\Psi = P$. With this assumption, the Kalman filter transforms to a fixed-value standard gain estimator, therefore:

$$\hat{x}^-(0) = \overline{x}(0)$$

$$\hat{x}^-(k) = A\hat{x}(k-1) + Bu(k)$$

$$\hat{x}(k) = \hat{x}^-(k) + \beta K(y(k) - C\hat{x}^-(k))$$

where $\beta$ is the fixed packet-dropout coefficient of the communication channel.

**Remark 2.1:** It is assumed that the transmitted data packets from the sensor to the estimator centre are available through a packet-dropping network. Thus, the parameter $\beta$ (packet-dropout coefficient) is an intrinsic feature of the communication network and it is assumed to be known to both system and the attacker. Additionally, the estimator will either get the perfect data packet or the data packet with some loss according to the packet-dropout coefficient value. Since it is assumed that the data packet is not completely dropped, the packet-dropout coefficient cannot be zero and the system will not be unstable because of the packet dropping. For different values of the packet-dropout coefficient, simulation results are brought to analyse the attack detection procedure.

### 2.2 Optimal control formulation using Linear Quadratic Gaussian (LQG) controller

Based on the obtained state estimation $\hat{x}(k)$ an objective function can be defined. Then, the goal of the LQG controller is to minimise the defined objective function as follows.

$$\lambda = \min_{u} \lim_{{t \to \infty}} \frac{1}{t} \left[ \sum_{{k=0}}^{t-1} (\hat{x}^T(k)F\hat{x}(k) + u^T(k)Gu(k)) \right]$$

where $F$ and $G$ are defined as positive semi-definite matrices and $u(k)$ is assumed to be measurable regards to $y(0), \ldots, y(k)$. So, $u(k)$ can be obtained as a function of the above measurements. The answer to the defined minimisation problem can be derived as a steady-gain controller like the following formulation:

$$u(k) = u^{opt}(k) = -(B^T RB + G)^{-1}B^T RA\hat{x}(k)$$

where $u^{opt}(k)$ is the obtained optimal control input and $R$ can be attained using the following Riccati equation:

$$R = A^T RA + F - A^T RB(B^T RB + G)^{-1}B^T RA$$

Let define $M = -(B^T RB + G)^{-1}B^T RA$, then $u^{opt}(k) = M\hat{x}(k)$.

Now, the determined objective function by considering optimal estimator and the LQG controller in this approach would be rewritten as:

$$\lambda = \text{Trace}(RW) + \text{Trace}\left[ \left( A^T RA + F - R \right) (P - B\beta C) \right]$$

### 2.3 Intercepted-data detector

To monitor and control the system behaviour at the remote estimator, we need to implement an intercepted-data detector to find out whether there are cyber-attacks or not. There are some ways to detect attacks in a cyber-physical system, such as $\chi^2$ detector or $K-L$ divergence between two probability distributions or game-theoric methods (Guo et al., 2018; Li et al., 2017, 2015; Liu et al., 2009). In this paper, we are going to use $K-L$ divergence method (Bai et al., 2015) to detect attacks in the system. The Kullback–Leibler divergence (K-L divergence) is a non-negative distance measurement criterion between two probability distributions, which is practical to use in cyber-attacks’ tracing theories (Bai & Gupta, 2014; Bai et al., 2015).

**Definition 2.1 (Kullback–Leibler Divergence):** This criterion expresses that if there are two stochastic sequences $x(k)$ and $y(k)$ with corresponding joint probability density functions $f_{x(k)}$ and $f_{y(k)}$, respectively, then, the Kullback–Leibler divergence between $x(k)$ and $y(k)$ will be defined as given below:

$$D(x(k) \parallel y(k)) = \int_{\{\mu(k)|f_{x(k)}(\mu(k)) > 0\}} \log \frac{f_{x(k)}(\mu(k))}{f_{y(k)}(\mu(k))} f_{x(k)}(\mu(k)) d\mu(k)$$

(18)
according to the above K-L divergence equation, if \( f_x(k) = f_y(k) \) then \( (x(k) \parallel y(k)) = 0 \). It is proved that K-L divergence criterion is not symmetric in general, thus \( (x(k) \parallel y(k)) \neq D(y(k) \parallel x(k)) \).

### 3. Linear replay attack strategy derivation against operating control system

In this section, to derive formulations, it is considered that an adverse third party tries to intrude on the presented control system. The replay attack model in this approach is defined as computer security problems. Also, the feasibility of these kinds of attacks on the control system is investigated. It is proved that the analysis of this work can be generalised to other types of control systems with higher orders. The attacker can inject the control input \( u_a(k) \) at any time. It is worth noticing that the identification process of the underlying dynamic model of the control system for attackers can be hard in general, and not all the attackers are such powerful to detect systems’ models. Therefore, this paper focuses on a straightforward attack strategy, which is much easier to implement. Besides, since the energy-consuming limitation exists in reality for both system and attacker, the goal of designing attack or defense strategies in CPSs is to develop with the lowest level of energy consumption for both parties.

In the existence of attack in control systems, to implement any counter-attack strategies, at first, the attacker should be detected as fast as it can. Thus, in the attack stage, the intercepted-data detector should work correctly. As mentioned, the attacker aims to inject fake stored measurements from any specific time step \( k \) to the control system. To have an integrated framework for analysing these kinds of attacks, the stored measures by the attacker can be considered as the output of a virtual network as given in the following:

\[
\begin{align*}
\dot{x}(k + 1) &= A\dot{x}(k) + Bu(k) \\
\dot{y}(k) &= C\dot{x}(k) + v(k)
\end{align*}
\]

(19)

(20)

It is assumed that \( w(k) \) and \( v(k) \) are independent of the attack. Therefore, they are the same as the ones described for the real system.

Also, the virtual system can be introduced as follows.

\[
\begin{align*}
\dot{\tilde{x}}^-(k) &= A\dot{\tilde{x}}^-(k - 1) + B\tilde{u}(k) \\
\dot{\tilde{x}}(k) &= \dot{\tilde{x}}^-(k) + \beta K\left(\tilde{y}(k) - C\tilde{x}^-(k)\right)
\end{align*}
\]

(21)

(22)

and

\[
\tilde{u}(k) = M\tilde{x}^-(k)
\]

(23)

with the specified initial conditions \( \tilde{x}(0) \) and \( \tilde{x}^-(0) \). If it is considered that the attacker can learn the system’s behaviour at each time step \( k \), then it is evident that the attacker would run the virtual network to maximise the attack’s influence on the system’s performance. To investigate a replay attack, consider that the attacker can store the previous system’s measurements. So, the mentioned virtual system would be just the time-shifted edition of the actual order. Let define \( T \) as the time shift. Then, it is easy to conclude that \( \dot{x}(k) = x(T + k) \) and \( \dot{x}^-(k) = x^-(T + k) \).

Assume that the system is under a replay attack and the system’s defender is applying the K-L divergence criteria between the actual system’s innovation sequence \( z(k) = y(k) - C\tilde{x}(k) \) and the input innovation sequence \( \tilde{z}(k) = \tilde{y}(k) - C\tilde{x}^-(k) \) which is sent via the virtual system to detect attack interference in the system. With this consideration, the Kalman filter equations can be rewritten as given below in a recursive way:

\[
\begin{align*}
\dot{\hat{x}}(k) &= A\hat{x}(k - 1) + Bu(k) \\
&= (A + BM)\hat{x}(k - 1) \\
&= (A + BM)\left[\tilde{x}^-(k) + \beta K\left(\tilde{y}(k) - C\tilde{x}^-(k)\right)\right] \\
&= (A + BM)\left(I - \beta KC\right)\tilde{x}^-(k) + (A + BM)\beta KY(k)
\end{align*}
\]

(24)

furthermore, for the virtual system, a similar equation for \( \tilde{x}^-(k) \) can be derived as follows:

\[
\begin{align*}
\dot{\tilde{x}}(k) &= (A + BM)\left(I - \beta KC\right)\tilde{x}^-(k) + (A + BM)\beta KY(k)
\end{align*}
\]

(25)

for simplicity, it is assumed that the time of the attack starts as \( t = 0 \). Define \( \Lambda \) as \( \Lambda = (A + BM)(I - \beta KC) \), then

\[
\begin{align*}
\tilde{x}^-(k) - \tilde{x}^-(0) &= \Lambda^k \left(\tilde{x}^-(0) - \tilde{x}^-(0)\right)
\end{align*}
\]

(26)

let define \( \tilde{x}^-(0) - \tilde{x}^-(0) \equiv \eta \), now the residue from the previous equations can be rewritten as follows.

\[
\tilde{y}(k) - C\tilde{x}^-(k) = \left(\tilde{y}(k) - C\tilde{x}^-(k)\right) - CA^k \eta
\]

(27)

according to the virtual system’s explanation, it can be inferred that the residue \( \tilde{y}(k) - C\tilde{x}^-(k) \) has a similar distribution to the residue \( y(k) - C\tilde{x}^-(k) \). Hereupon, if \( \Lambda \) is considered to be stable during the time horizon, the second term of the (27) will converge to zero. Therefore, the residue \( \tilde{y}(k) - C\tilde{x}^-(k) \) has the same distribution as \( z(k) = y(k) - C\tilde{x}^-(k) \). So, the attack innovation sequence \( \tilde{z}(k) = \tilde{y}(k) - C\tilde{x}^-(k) \) can be rewritten as \( \tilde{z}(k) = \tilde{y}(k) - C\tilde{x}^-(k) \). Moreover, because of the distribution similarity between innovation sequences \( z(k) \) and \( \tilde{z}(k) \), the calculated detection rate given by the K-L divergence intercepted-data detector will consist of the same false alarm detection rate as before. So, the proposed intercepted-data detector is ineffectual.

Now, the second case of \( \Lambda \) is investigated. If \( \Lambda \) is assumed to be unstable, the attacker is not able to carry on re-profiling the measurement \( \tilde{y}(k) \) over the time horizon of which the intercepted-data detection criteria will transform into an unbounded rule quickly. In this case, it can be concluded that the system is resilient to this kind of attack, as the defined intruder detection method can detect the attack’s existence. Besides, with derived formulas and calculations, it is proved that the obtained outcomes from the implementation on a specific group of the estimator, controller, and intercepted-data detector for our approach can be generalised to any virtual systems. Moreover, the outcomes from the studied K-L divergence intrusion detection method in this paper can be applied to any non-linear systems and higher-order systems since other detection methods like \( \chi^2 \) detector can only be used for first-order and linear systems, but with using the K-L divergence method, this issue can be solved.
Theorem 3.1: The K-L divergence criterion between two innovation sequences z(k) and \( \tilde{z}(k) \) can be obtained as follows:

\[
\tilde{y}(k) - C\hat{x}(k) = (\hat{y}(k) - C\hat{x}(k)) - CA^k\eta
\]  

(28)

where \( m \) is the dimension of \( z(k) \) as general.

Proof: The proof of this Theorem is stated in Guo et al. (2018).

4. Fault detection scheduling of deception replay attack

As mentioned in previous sections, it is necessary to consider designing detection and defense strategies against cyberattacks in vulnerable control systems, especially replay attacks.

To derive the attack detection strategy, it is assumed that \( \Delta \) is stable. According to the control systems with the LQG controller, the weak point of the LQG controller and Kalman filter is that they operate based on a fixed control gain, or a control gain that converges soon. Thus, we can conclude that the control approach, in this case, would be static from some viewpoints. As previous methods regarding the detection of replay attacks, the controller is assumed to be as the following form:

\[
u(k) = u^{opt}(k) + \Delta u(k)
\]

(29)

where \( u^{opt}(k) \) is the output of the LQG controller, and \( \Delta u(k) \)'s are collected from i.i.d Gaussian distribution with zero mean and covariance value of \( \tau \). It should be noticed that selected \( \Delta u(k) \)'s are independent of the optimal control input \( u^{opt}(k) \). The whole system's diagram can be presented in Figure 1.

The purpose of adding the signal \( \Delta u(k) \) is to verify the correct performance of the system. As mentioned before, \( \Delta u(k) \) at each time step \( k \) should be a zero-mean signal to prevent any bias to \( x(k) \). It can be inferred that without any attacks, the LQG controller will not be optimal anymore. So, to detect any attacks, the controller’s performance should be optimised, too. In the given Theorem (Mo & Sinopoli, 2009), the loss of the used LQG controller is distinguished when the signal \( \Delta u(k) \) exists.

Theorem 4.1 (Mo & Sinopoli, 2009): By considering the existence of the signal \( \Delta u(k) \) in the system, the LQG controller’s performance can be stated as follows.

\[
\tilde{\lambda} = \lambda + \text{Trace} \left[ (G + B^TB) \tau \right]
\]

(30)

Proof: The proof of this Theorem is given in Mo and Sinopoli (2009).

Now, different from the previous work, we consider the K-L divergence intercepted-data detector to consist of systems with more general features and higher-order dynamics after augmenting the accidental control signal. The following stated Theorem proves the usefulness of the K-L divergence intercepted-data detector under the altered control design.

Theorem 4.2: In the absence of any replay attacks or the case of occurring replay attacks without any new augmented detection strategies,

\[
D(\tilde{z}(k) \mid z(k)) = 0.
\]

(31)

and under a replay attack,

\[
D(\tilde{z}(k) \mid z(k)) \geq 2-m + \text{Trace} \left( \Sigma^{-1}2\Omega C^T \right) + \log |\Sigma| - \log \left| \Sigma + 2\Omega C^T \right|
\]

(32)

where \( m \) is the dimension of \( z(k) \) as general, and \( \Omega \) can be obtained by solving the given Lyapunov equation

\[
\Omega - BrB^T = \Lambda\Omega\Lambda^T
\]

(33)

and \( \Sigma \) is the covariance of the innovation sequence of the real system and equals to \( \Sigma = CPC^T + V \).

Proof: For the first equation, based on the fact that when there is no replay attack in the system or the case that there is a replay attack without any new augmented detection strategies, \( \tilde{z}(k) = z(T + k) \), then \( \text{cov}(\tilde{z}(k)) = \text{cov}(z(k)) \). So, it can be inferred that:

\[
D(\tilde{z}(k) \mid z(k)) = 0.
\]

This conclusion is an evident fact as a result of Gibb’s inequality for the K-L divergence criterion.

For proving the second part of the Theorem 4.2, rewrite \( \hat{\chi}(k) \) based on the augmented control input \( \Delta u(k) \), as presented as a detection strategy as follows.

\[
\hat{\chi}(k) = \Lambda\hat{\chi} - (A + BM)\beta K\tilde{y}(k) + B\Delta u(k)
\]

(34)

therefore,

\[
(\hat{\chi})^-(k) - \hat{\chi}^- - (k) = \Lambda^k\eta + \sum_{j=0}^{k-1} \Lambda^{k-j-1}B(\Delta u(j) - \Delta \hat{u}(j))
\]

(35)

where \( \eta = \hat{\chi}^-(0) - \hat{\chi}^- - (0) \).

Now, \( \tilde{y}(k) - C\hat{x}^- - (k) \) can be rewritten as:

\[
\tilde{y}(k) - C\hat{x}^- - (k) = \tilde{y}(k) - C\hat{x}^- - (k) - CA^k\eta
\]

\[
- C \sum_{j=0}^{k-1} \Lambda^{k-j-1}B(\Delta u(j) - \Delta \hat{u}(j))
\]

(36)
The first term of the above equation has just the same distribution as $y(k) - C\hat{x}^-(k)$. Also, by considering the stability of $\Lambda$, $\Lambda\Delta u(j)$ will be stable and converges to zero. Moreover, it is assumed that $\Delta u(j)$ is independent of the virtual system’s dynamic and for the mentioned virtual system, $\hat{y}(k) - C\hat{x}^-(k)$ will be independent of $\Delta u(j)$. Thus, the steady-state value of the virtual system’s innovation sequence’s covariance can be obtained as given in the following:

$$
\varphi = \lim_{k \to \infty} \text{cov} \left( \hat{y}(k) - C\hat{x}^-(k) \right)
= \lim_{k \to \infty} \text{cov} \left( \hat{y}(k) - C\hat{x}^-(k) \right) + \sum_{j=0}^{\infty} \text{cov} \left( C\Lambda^TB\Delta u(j) \right)
+ \sum_{j=0}^{\infty} \text{cov} \left( C\Lambda^TB\Delta \hat{u}(j) \right) = \Sigma + 2\sum_{j=0}^{\infty} C\Lambda^TB\text{Tr}(\Lambda^T)CT
$$

(37)

where $\Sigma = CPC^T + V$. Let define $\Omega$ as follows.

$$
\Omega = \sum_{j=0}^{\infty} \Lambda^TB\text{Tr}(\Lambda^T). \quad \text{By this definition, } \varphi \text{ is obtained as follows.}
$$

$$
\varphi = \lim_{k \to \infty} \text{cov} \left( \hat{y}(k) - C\hat{x}^-(k) \right) = \Sigma + 2\Omega C^T. \quad (38)
$$

Now, based on Theorem 3.1, the K-L divergence criterion between innovation sequences $\tilde{z}(k)$ and $z(k)$ can be obtained as follows.

$$
D \left( \tilde{z}(k) \parallel z(k) \right)
\approx \frac{1}{2} \text{Trace} \left( \Sigma^{-1} \varphi \right) - \frac{m}{2} + \frac{1}{2} \log \left| \Sigma \right|
= \frac{1}{2} \text{Trace} \left( \Sigma^{-1} \left[ \Sigma + 2\Omega C^T \right] \right) - \frac{m}{2} + \frac{1}{2} \log \left| \Sigma + 2\Omega C^T \right|
= \text{Trace} \left( \Sigma^{-1} \Sigma + \Sigma^{-1} 2\Omega C^T \right) - m
+ \log |\Sigma| - \log |\Sigma + 2\Omega C^T|
\approx 2 - m + \text{Trace} \left( \Sigma^{-1} 2\Omega C^T \right)
+ \log |\Sigma| - \log |\Sigma + 2\Omega C^T|
$$

where $m$ is the dimension of $z(k)$ as general and $\Omega = \sum_{j=0}^{\infty} \Lambda^TB\text{Tr}(\Lambda^T)\text{Tr}(\Lambda^T)$ and

$$
\Sigma = CPC^T + V,
$$

which finishes the proof.

**Remark 4.1:** One feasible way to design $\tau$ appropriately for simulating the results is to minimise equation $\hat{\lambda} - \lambda = \text{Trace}[(G + B^TRB)\tau]$, while trying to maximise the value of $D(\tilde{z}(k) \parallel z(k))$, which means maximising the term Trace($\Sigma^{-1} 2\Omega C^T$). Values of other necessary variables are addressed in the next section.

---

### 5. Numerical results

In this section, numerical simulations are provided to illustrate the analytical outcomes of this approach. Consider a comprehensive control system with two states described in section 2 with the following information:

$$
A = \begin{bmatrix}
0.7 & 0.2 \\
0.05 & 0.64
\end{bmatrix}, \quad C = \begin{bmatrix}
0.5 & -0.8 \\
0 & 0.7
\end{bmatrix},
$$

$$
W = \begin{bmatrix}
0.5 & 0 \\
0 & 0.7
\end{bmatrix}, \quad V = \begin{bmatrix}
1 & 0 \\
0 & 0.8
\end{bmatrix},
$$

$M$ is chosen as $M = -0.6180$.

One candidate for selecting $\tau$ can be the steady-state covariance value of the system’s state estimation without any attacks so that it can be chosen as $\tau = \begin{bmatrix} 1.1721 & 0.3146 \\ 0.3146 & 1.0229 \end{bmatrix}$. Also, it is considered that $F = G = I$.

In the present article, the theoretical outcomes are simulated for several iterations to monitor the system’s behaviour with or without the existence of the replay attack accurately. Without any control precautions against replay attacks, the system is defenseless to these attacks at first. It is also assumed that the attacker tries to begin replaying to the first ten state estimations at the filter’s 10th iteration and keeps on attacking.

From the mentioned Theorems, the K-L divergence criterion between innovation sequences $\tilde{z}(k)$ and $z(k)$ can be obtained as follows.

$$
D \left( \tilde{z}(k) \parallel z(k) \right)
\approx \frac{1}{2} \text{Trace} \left( \Sigma^{-1} \varphi \right) - \frac{m}{2} + \frac{1}{2} \log \left| \Sigma \right|
= \frac{1}{2} \text{Trace} \left( \Sigma^{-1} \left[ \Sigma + 2\Omega C^T \right] \right) - \frac{m}{2} + \frac{1}{2} \log \left| \Sigma + 2\Omega C^T \right|
= \text{Trace} \left( \Sigma^{-1} \Sigma + \Sigma^{-1} 2\Omega C^T \right) - m
+ \log |\Sigma| - \log |\Sigma + 2\Omega C^T|
\approx 2 - m + \text{Trace} \left( \Sigma^{-1} 2\Omega C^T \right)
+ \log |\Sigma| - \log |\Sigma + 2\Omega C^T|
$$

where $m$ is the dimension of $z(k)$ as general and $\Omega = \sum_{j=0}^{\infty} \Lambda^TB\text{Tr}(\Lambda^T)\text{Tr}(\Lambda^T)$ and

$$
\Sigma = CPC^T + V,
$$

which finishes the proof.

---

**Remark 4.1:** One feasible way to design $\tau$ appropriately for simulating the results is to minimise equation $\hat{\lambda} - \lambda = \text{Trace}[(G + B^TRB)\tau]$, while trying to maximise the value of $D(\tilde{z}(k) \parallel z(k))$, which means maximising the term Trace($\Sigma^{-1} 2\Omega C^T$). Values of other necessary variables are addressed in the next section.
coefficient $\beta$ equals 1 and the data packet from the sensor is completely transferred to the estimation centre without any data loss. By considering the existence of a replay attack, in this case, Figures 3–6 are presented. To compensate for the replay attack’s influence on the system’s performance, the newly presented fault detection strategy is implemented, and the original value of the K-L divergence intercepted-data detector is calculated again based on the Theorem 4.2. Figure 3 illustrates the computed value of the attack detection method based on the proposed fault detection strategy. As it is shown in Figure 3, the K-L divergence criterion detects the replay attack accurately and it has a specific extremum value in steady-state, which in this case, is 2. Thus, by considering a new control strategy, the system’s estimation performance can be controlled, and also the replay attack can be detected very quickly.

Besides, the loss of the LQG performance before and after injecting the signal $\Delta u(k)$ and its corresponding error is illustrated in Figures 4, 5. We can also conclude from the Figures 4, 5 that the control performance of the real system should be changed in a steady-state, and then it will not be optimal as
Figure 4. Output calculated value of the LQG performance before and after injecting $\Delta u(k)$ with $\beta = 1$.

Figure 5. Calculated error value of the LQG performance before and after injecting $\Delta u(k)$ with $\beta = 1$.

the no-attack case. Also, since the attack happens in 10th iteration, the signal $\Delta u(k)$ is injected from this iteration to detect an attack, and this matter can be observed in Figure 5 which causes an error in the signal $\Delta u(k)$ from this iteration. In Figure 6, the remote state estimation error covariance is illustrated with or without a replay attack with the assumption of $\beta = 1$. As it is illustrated in Figure 6, the trace value of the state estimation error covariance under no-attack condition converges to the cost of 2.195 while when a replay attack occurs, the state estimation procedure is affected by the attacker and the trace value of the state estimation error covariance is not going to converge during the time horizon. Consequently, without providing a new fault detection strategy to detect the replay attack to stop the system immediately, the attacker can degrade the control system’s performance as well as being stealthy in the system.

Case 2. In this case, the packet-dropout coefficient $\beta$ is reduced to $\beta = 0.5$. Therefore, in this case, half of the data packet is considered to be lost in a communication network. By assuming the existence of the replay attacker, Figures 7–10 are obtained.
As the previous case ($\beta = 1$), Figure 7 depicts the calculated value of the K-L divergence fault detection criterion based on the newly proposed attack detection strategy, which has the same value as in Case 1 because changes in packet-dropout coefficient $\beta$ has the least influence altering the output calculated value of the K-L divergence fault detection criterion.

In Figures 8, 9, the loss of the LQG performance before and after injecting the signal $\Delta u(k)$ and their corresponding error are depicted by assuming $\beta = 0.5$, which more loss in the LQG performance can be observed. Additionally, in Figure 10, the evolutions of the system’s estimation error covariance with and without replay attacks with $\beta = 0.5$ are illustrated.

Case 3. In this case, the communication network is assumed to be very defective and most of the data packet drops among the communication network. For this reason, to analyse this case, the packet-dropout coefficient can be selected as $\beta = 0.2$, which denotes that 80% of the data packet drops and only 20% of the data packet arrives at the estimation centre successfully under the replay attacker. Figures 11–14 are shown for Case 3. The calculated value of the K-L divergence fault detection method
according to the presented augmented attack detection method is shown in Figure 11. In Figures 12, 13, the loss of the LQG performance before and after injecting the signal $Δu(k)$ and their corresponding error are shown by assuming $β = 0.2$, which more loss in the LQG performance can be observed comparing to cases 1 and 2. Furthermore, in Figure 14, the evolutions of the system’s estimation error covariance with and without replay attacks with $β = 0.2$ are demonstrated.

Some observations can be achieved based on the above simulation results. Firstly, according to Figures 3, 7, 11, it is obvious to verify that the packet-dropout coefficient $β$ has no effects on calculating the proposed K-L divergence fault detection criterion, which shows that the presented fault detection method can detect replay attacks quickly and it is absolutely independent of the communication network’s quality. Secondly, based on Figures 4, 5, 8, 9, 12, 13, it is easy to conclude that less efficient communication network leads to be in danger of more cyberattacks, especially replay attacks. Finally, Figures 6, 10, 14 denote the increasing effect of the replay attack on the system’s state estimation evolution process by decreasing the quality of the communication network. Observed from figures, we can conclude that the difference in the mentioned trade-off is not considered when replay attack happens since the attack detection rate is rapid in first moments with the K-L divergence method rather than using $χ^2$ detector (Mo & Sinopoli, 2009),
Remark 5.1: Since the replay attacker attempts to replay and inject the system’s previous states, and because of the consideration of this paper that the attack starts at early iteration (10th iteration), the replay attacker tries to inject the transient states to the system and prevents the system to converge quickly, which can be defined as the worst-case of a replay attack that occurs at early stages of the system’s performance and consequently, the replay attacker is working in an optimal condition that degrades the system’s state estimation performance at the highest level by replaying transient states to the system. It is obvious that replaying and injecting the steady-state data to the system cannot make a big destructive difference in the state estimation procedure.

6. Conclusion
In the present article, we presented a replay attack scenario on cyber-physical systems and developed the security issue of the control systems under this type of attack. Additionally, we proposed a K-L divergence intercepted-data detector to find
the replay attack’s existence as quickly as possible. Besides, we proved that for some control systems, the previously developed conventional estimation, control, and fault detection strategy cannot be resilient to the replay attacks. Then, for such mentioned systems, we presented a novel fault detection technique that enhances the control system’s fault detection ability against replay attacks. Consequently, under replay attacks, the control system can be stopped with any defense strategies in the early stages of happening the replay attack. Since the proposed fault detection criterion is based on the K-L divergence method, more general control systems with even higher-order dynamics can be considered to operate with this article’s proposed fault detection method against replay attacks which are very common cyberattacks to industrial control systems these days. Numerical results and comparisons were developed to illustrate and verify the analytical results. Observed from numerical simulations, the efficacy of the proposed K-L divergence false-data detection framework was concluded for various types of communication networks, from the ideal communication network to the most vulnerable communication network. The worst-case analysis of various cyber-physical systems under injection replay attack combined with other types of attacks and the design of associated false-data detection and protection classical and game-theoretical strategies allocate directions for future work.
Disclosure statement
No potential conflict of interest was reported by the author(s).

ORCID
Amirreza Zaman http://orcid.org/0000-0001-6289-5450
Behrouz Safarinejadian http://orcid.org/0000-0001-5442-5600
Wolfgang Birk http://orcid.org/0000-0002-5888-8626

References
Bai, C., & Gupta, V. (2014). On kalman filtering in the presence of a compromised sensor: Fundamental performance bounds. In 2014 American Control Conference (pp. 3029–3034). https://doi.org/10.1109/ACC.2014.6859155
Bai, C.-Z., Pasqualetti, F., & Gupta, V. (2017). Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs. Automatica, 82, 251–260. https://doi.org/10.1016/j.automatica.2017.04.047
Bai, C., Pasqualetti, F., & Gupta, V. (2015). Security in stochastic control systems: Fundamental limitations and performance bounds. In 2015 American Control Conference (ACC) (pp. 195–200). https://doi.org/10.1109/ACC.2015.7170734
Chabir, K., Rhouma, T., Keller, J. Y., & Sauter, D. (2018). State filtering for networked control systems subject to switching disturbances. International Journal of Applied Mathematics and Computer Science, 28(3), 473–482. https://doi.org/10.2478/amcs-2018-0036
Ding, D., Wei, G., Zhang, S., Liu, Y., & Alsaaadi, F. (2016). On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors. Neurocomputing, 219, 99–106. https://doi.org/10.1016/j.neucom.2016.09.009
Guo, Z., Shi, D., Johansson, K., & Shi, L. (2018). Worst-case stealthy innovation-based linear attack on remote state estimation. Automatica, 89, 117–124. https://doi.org/10.1016/j.automatica.2017.11.018
Gupta, A., Langbort, C., & Başar, T. (2010). Optimal control in the presence of an intelligent jammer with limited actions. In 49th IEEE Conference on Decision and Control (CDC) (pp. 1096–1101). https://doi.org/10.1109/CDC.2010.5717544
Keller, J.-Y., Chabir, K., & Sauter, D. (2016). Input reconstruction for networked control systems subject to deception attacks and data losses on control signals. International Journal of Systems Science, 47(4), 814–820. https://doi.org/10.1080/00207721.2014.906683
Kim, K.-D., & Kumar, P. (2012). Cyber-physical systems: A perspective at the centennial. Proceedings of the IEEE, 100, 1287–1308. https://doi.org/10.1109/JPROC.2012.2189792
Kwon, C., Liu, W., & Hwang, I. (2013). Security analysis for cyber-physical systems against stealthy deception attacks. In 2013 American Control Conference (pp. 3344–3349). https://doi.org/10.1109/ACC.2013.6580348
Li, Y., Quevedo, D. E., Dey, S., & Shi, L. (2017). Sin-based dos attack on remote state estimation: A game-theoretic approach. IEEE Transactions on Control of Network Systems, 4(3), 632–642. https://doi.org/10.1109/TCNS.2016.2549640
Li, Y., Shi, L., Cheng, P., Chen, J., & Quevedo, D. E. (2015). Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. IEEE Transactions on Automatic Control, 60(10), 2831–2836. https://doi.org/10.1109/TAC.2015.2461851
Liu, K., Guo, H., Zhang, Q., & Xia, Y. (2020). Distributed secure filtering for discrete-time systems under round-robin protocol and deception attacks. IEEE Transactions on Cybernetics, 50(8), 3571–3580. https://doi.org/10.1109/TCYB.6221036
Liu, Y., Ning, P., & Reiter, M. K. (2009). False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th ACM Conference on Computer and Communications Security (pp. 21–32). Association for Computing Machinery.
Miao, F., Pajic, M., & Pappas, G. (2013). Stochastic game approach for replay attack detection. pp. 1854–1859. https://doi.org/10.1109/CDC.2013.6760152
Mo, Y., Chabukswar, R., & Sinopoli, B. (2014). Detecting integrity attacks on scada systems. IEEE Transactions on Control Systems Technology, 22(4), 1396–1407. https://doi.org/10.1109/TCST.2013.2280899
Mo, Y., Garone, E., Casavola, A., & Sinopoli, B. (2010). False data injection attacks against state estimation in wireless sensor networks. In 49th IEEE Conference on Decision and Control (CDC) (pp. 5967–5972). https://doi.org/10.1109/CDC.2010.5718158
Mo, Y., & Sinopoli, B. (2009). Secure control against replay attacks. In 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton) (pp. 911–918). https://doi.org/10.1109/ALLERTON.2009.5394956
Poovendran, R., Sampigethaya, K., Gupta, S. K. S., Lee, I., Prasad, K. V., Corman, D., & Paunicka, J. L. (2012). Special issue on cyber – physical systems: Fundamental tradeoffs and performance analysis. Journal of Systems and Control Engineering, 226(4), 425–443. https://doi.org/10.1080/09596518.2012.685484
systems [scanning the issue]. *Proceedings of the IEEE*, 100(1), 6–12. https://doi.org/10.1109/JPROC.2011.2167449

Shi, D., Chen, T., & Darouach, M. (2016). Event-based state estimation of linear dynamic systems with unknown exogenous inputs. *Automatica*, 69, 275–288. https://doi.org/10.1016/j.automatica.2016.02.031

Shi, D., Elliott, R. J., & Chen, T. (2017). On finite-state stochastic modeling and secure estimation of cyber-physical systems. *IEEE Transactions on Automatic Control*, 62(1), 65–80. https://doi.org/10.1109/TAC.2016.2541919

Shi, L., Epstein, M., & Murray, R. M. (2008). Kalman filtering over a packet dropping network: A probabilistic approach. In 2008 10th International Conference on Control, Automation, Robotics and Vision (pp. 41–46). https://doi.org/10.1109/ICARCV.2008.4795489

Teixeira, A., Sou, K. C., Sandberg, H., & Johansson, K. H. (2015). Secure control systems: A quantitative risk management approach. *IEEE Control Systems Magazine*, 35(1), 24–45. https://doi.org/10.1109/MCS.2014.2364709

Yang, W., Lei, L., & Yang, C. (2017). Event-based distributed state estimation under deception attack. *Neurocomputing*, 270, 145–151. https://doi.org/10.1016/j.neucom.2016.12.109

Yoo, S. J. (2020). Neural-network-based adaptive resilient dynamic surface control against unknown deception attacks of uncertain nonlinear time-delay cyberphysical systems. *IEEE Transactions on Neural Networks and Learning Systems*, 31(10), 4341–4353. https://doi.org/10.1109/TNNLS.5962385

Zhang, H. (2014). Online deception attack against remote state estimation. *IFAC Proceedings Volumes*, 47(3), 128–133. https://doi.org/10.3182/20140824-6-ZA-1003.02668

Zhang, H., Cheng, P., Shi, L., & Chen, J. (2015). Optimal denial-of-service attack scheduling with energy constraint. *IEEE Transactions on Automatic Control*, 60(11), 3023–3028. https://doi.org/10.1109/TAC.9