Cloud-Based Control Systems: Basics and Beyond

Magdi S. Mahmoud

Systems Engineering Department, King Fahd University of Petroleum and Minerals, P. O. 5067, Dhahran 31261, Saudi Arabia
E-mail: msmahmoud@kfupm.edu.sa

Abstract. Using advanced information technologies (IT) and Internet of things (IOT) methodologies, cloud-based control systems (CCS) emerge as natural paradigm of networked control systems (NCS) and it being under development by enforcing the concept of control as a service (CaaS). Day by day NCS methods strongly promoted for distributed closed-loop control and industrial automation systems and extremely developed to study the influence of bidirectional communication constraints. In this paper, we examine the basics of cloud-based control systems (CCS) where the controller methods and algorithms are remotely placed in cloud far from the physical system. This creates a two parts: cyber part and physical part. There are several issues arose including networking delays, data dropouts and vulnerability to attacks. Research activities into these and related directions are discussed.

Keywords: Cloud-based control, Networked control system, Non-cooperative game.

1. Introduction

Given the present information and communication technologies, networked control systems (NCS) arouse from the interconnection of distributed units of the control system via a suitable digital communication links. It turn out that transmission over NCS is confronted to communication limitations including variable/random time delay, data packets loss, quantization effects, and bandwidth constraints [1], [2]. Developments in control techniques are found in several practical applications including congestion control, transportation networks, smart grids. Recently, taking the merits of cloud computing technologies, NCS have been interestingly extended to cloud-based control systems (CCS) [3]. Several researchers pay special attention to internet of things (IOT) as well as distributed sensors networking. With in this frame, a huge information needs to transit through very large and complex systems.

The aim of this work is to build on [2], [3] and extend them further to address the secure control problem. The paper initially provides a review about the basics and features of CCS with focus on control and computing theories and technologies, see Fig. 1. Cloud-based control systems can be stated as following: it contains cyber physical system and then contains cyber physical control system. It is readily seen that CCC first contains the idea that ‘control as a service’ that is control algorithms can be scheduled as a kind of resources.

Looked at in this regard, the main features of cloud-based control systems with a significant computing potential have been investigated [4]. It is shown that subscribers of information technology (IT) computing environment have access cloud services using desktop-hosted web browsers as clients. Cloud computing can play an important function in enhancing the electric power scheduling namely
smart-grid in which it sustains the stability and reliability of the grid with reasonable price [5]. Moreover, cloud control infrastructure has a variety of advantages such as zero start-up cost, less effort and avoiding resource over/under provisioning [6].

![Cloud-based control system](image)

**Figure 1.** Cloud-based control system

2. Basics of Cloud-Based Control Systems

Cloud control systems (CCC) essentially contain cyber-physical system (CPS) and then contains cyber physical control system (CPCS). In this regard, CCC embraces the idea of 'control as a service', that is control algorithms can be scheduled as a kind of resources. In cloud control systems, there are three closed-loops:

1) the control loop
2) scheduling loop and
3) decision-making loop.

In a typical cloud control system, the focus is on managing the virtual control resources, especially control algorithm. Besides, a local control to satisfy a short time-delay tolerance system is necessary. A cloud control plus a local control scheme will achieve not only a powerful process of industrial automation but also an accurate and real-time control. The security on cloud control system includes the service secure, storage secure and also management secure besides network secure as in networked control systems (NCS).
3. Attack Detection

A secure CPS has a reliable attack detector at the core. In the literature, there are four major approaches for attack detection as listed in Fig. 2.

![Figure 2. Approaches of Detection](image)

On one hand in data fusion of sensor networks, Bayesian detection with binary hypothesis is the most effective approach, see [9], [7], [8]. On the other hand, stochastic estimation techniques are addressed in attack detection and require systems noises [10]. In this way, information about the mean and variance for alleviating the state distributions are propagated. It is crucial [10] to guarantee that the underlying state estimation method is faithful which is critical in engineering applications including guidance and navigation. It turns out that meaningful representation of the state distributions incorporating unknown-but-bounded (UBB) uncertainties is appealing. In this regard, based on addressing discrepancies between estimated and predicted behavior by a model, the $\chi^2$-detector is commonly utilized, where the estimated and predicted states constitute vectors in Kalman filtering setting. It is noted that the reliability of attack detection is decreased leading to sub-optimality of the resulting UBB noises.

4. Denial-of-Service Attack

Approaches of denial-of-service (DoS) attacks have the objective of incorporating the communication resources in order to block the transmission of measurement and/or control signals which might lead to excessive deterioration of the system performance.

It is recorded that the most dangerous type of DoS attacks is the distributed DoS (DDoS). Being a coordinated attack, a large number of compromised machines are used to achieve the DoS attack [11]. Due to the simplicity of generating it, low cost and its high impact on systems, It is frequently occurred and this might lead to the complete malfunction of corporations [12]–[13], causing instability of power grids [14] and/or producing long delay jitter on networked system packets [15].
5. Classification of radio frequency identification (RFID)

Based on several prime factors, the DoS attacks in radio frequency identification (RFID) system can be classified as follows [16]:

(i) Tag Data Modification: Changing the data to a random number which cannot be identified by the reader.

(ii) Random DoS Attack: Which is affecting the system by injecting short periods of noise signals.

(iii) Kill Command Attack: The attacker send a kill command with the hacked password causing a permanent disabling of the tag.

(iv) System Jamming: Electromagnetic jamming is done in this type to prohibit tags from communicating with readers.

(v) Desynchronization Attack: It is destroying synchronization between the tag and the RFID reader causing a permanent disabling of the authentication capability of an RFID tag.

6. Secure Control Problem

Several approaches were applied in the literature for controlling CPS subject to DoS attacks. Following are discussion on the main approaches which are summarized in Fig. 3.

**Figure 3. Secure control approaches**

There are two fundamental models of DoS attacks in CPS: Queueing model and Stochastic model.

6.1. Queueing model

Networking devices including firewalls, end computers, and routers, become ill-behaved under DoS attacks while dealing with high packet rate due to the constraints on memory resources, central processing units, interrupt processing, and input/output (I/O) processing. This in turn may affect
performance of the control system such as: rise and settling time, mean-squared error, and percentage overshoot.

The packet transmission of NCS under DoS attacks is approximated by applying two simple models based on a multiple-input queue [25]:

- **Type I:** The attackers launch DoS attacks to an endpoint from computers in the local area close to the endpoint. This causes a lost in a large number of packets.
- **Type II:** The attackers launch DoS attacks remotely to service-provider-edge routers leading to slow down the network links between a remote plant and a controller.

![Figure 4. Block diagram of the closed-loop system](image)

As demonstrated earlier, the DoS phenomenon that may prohibit the control signal from being processed at the desired time [26]. This implies that measurement and control channels can be affected independently. One basic idea is to assume that during DoS attack, data can be neither sent nor received. Let \( \{h_n\}_{n \in \mathbb{N}_0} \), where \( h_0 \geq 0 \), be the sequence of DoS off/on transitions, meaning that the time instants at which DoS change a transition from zero to one:

\[
H_n := \{h_n\} \cup [h_n, h_n + \tau_n]
\]

where \( H_n \) is the time-interval of \( n \)th DoS attack, and its length is \( \tau_n \in \mathbb{R}_\geq 0 \), during that time the communication is not available. If \( \tau_n = 0 \), the \( n \)th DoS attack is represented as a single pulse at time \( h_n \).

The actuator generates an input based on the most recent data received from the controller during the DoS attack. Given \( \tau, t \in \mathbb{R}_\geq 0 \) with \( t \geq \tau \), consider that

\[
\Xi(\tau, t) := \bigcup_{n \in \mathbb{N}_0} H_n \cap [\tau, t]
\]

\[
\Theta(\tau, t) := [\tau, t] \setminus \Xi(\tau, t).
\]

That means, for each interval \( [\tau, t] \), \( \Xi(\tau, t) \) and \( \Theta(\tau, t) \) are referring to the sets of time instants where communication is prohibited and allowed, respectively. The control signal applied to the system at each \( t \in \mathbb{R}_\geq 0 \) can be represented as:

\[
u(t) = Kx(t_{k(t)})\]
where

\[ k(t) := \begin{cases} -1, & \text{if } \Theta(0,t) = \emptyset \\ \sup \{ k \in \mathbb{N}_0 \mid t_k \in \Theta(0,t) \}, & \text{otherwise} \end{cases} \]  

(5)

That means, for each \( t \in \mathbb{R}_0^+ \), \( k(t) \) represents the most recent successful control update.

A similar model for DoS was presented in [27]–[28].

**Remark 1** One drawback of this approach is the start and end of the attack is not determined, so it is more applicable to post records.

### 6.2. Stochastic model

Stochastic model could be either Bernoulli model [29]–[30] or Markov model [31]. The Bernoulli model could be seen from the following LTI system:

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

(6)

where \( w(k) \) and \( v(k) \) are the process and measurement noises, respectively, and normally considered as independent and identically distributed (i.i.d.) Gaussian random vectors with mean 0 and covariance \( Q \), and \( \alpha(k) \) and \( \beta(k) \) are i.i.d. Bernoulli related to occurrences of the DoS attack on the process and measurement noises, respectively [30].

For the Markov model, consider the following system:

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

(7)

where \( \alpha(\xi(k+1)) \in \{0,1\} \) is the Markov modulated DoS attack sequence that prevents transmitting the control signal packets to the actuator where \( \xi(k) \) is related to the internal state of the attacker [31].

### 6.3. Secure control methods

Discussion on the main methods of controlling CPS subject to DoS attacks are portrayed in Fig. 3. Following a stochastic time delay system approach, the DoS is modeled as a stochastic process with a delay in the signal. In [24], both DoS and deception attacks are considered to be randomly occurring and they are modeled as two sets of Bernoulli distributed white sequences. Let us consider a discrete-time stochastic system with multiplicative noises affecting the system and the measurement as follows:

\[
\begin{align*}
x_{k+1} &= (A_0 + \sum_{i=1}^{r} \omega_{i,k}A_i)x_k + Bu_k \\
\hat{y}_k &= (C_0 + \sum_{i=1}^{s} \tilde{\omega}_{i,k}C_i)x_k
\end{align*}
\]

(8)

where \( x_k \in \mathbb{R}^{n_x} \) is the state vector, \( \hat{y}_k \in \mathbb{R}^{n_y} \) is the sensor measurement, and \( u_k \in \mathbb{R}^{n_u} \) is the controller input. \( A_i(i = 0,1,\cdots,r) \), \( B \) and \( C_i(i = 0,1,\cdots,s) \) are known constant matrices with appropriate dimensions. \( \omega_{i,k} \in \mathbb{R}(i = 1,2,\cdots,r) \) and \( \tilde{\omega}_{i,k} \in \mathbb{R}(i = 1,2,\cdots,s) \) are multiplicative
noises with zero means and unity variances, and are mutually uncorrelated in $k$ and $i, r$ and $s$ are
known positive integers. The rank of $B$ is assumed to be $n_u$.

The following attack model is applied in order to study such problems:

$$y^t_{k_s} = \alpha^t_{k_s}(\tilde{y}^t_{k_s} + \gamma^t_{k_s}v^t_{k_s}) + (1 - \alpha^t_{k_s})y^t_{k_{s-1}}$$

where $y^t_{k_s}$ is the data received by the controller and $v^t_{k_s} \in \mathbb{R}^{n_v}$ stands for the signals injected by
attackers which is described by:

$$v^t_{k_s} = -\tilde{y}^t_{k_s} + \xi^t_{k_s}$$

where $\xi^t_{k_s}$ is an arbitrary bounded energy signal satisfying

$$\|\xi^t_{k_s}\| \leq \delta_2$$

The stochastic variables $\alpha_{k_s}$ and $\gamma_{k_s}$ are Bernoulli distributed white sequences with values of 0 or 1
and with probabilities as follows:

$$\text{Prob}\{\alpha_{k_s} = 0\} = 1 - \bar{\alpha}, \quad \text{Prob}\{\alpha_{k_s} = 1\} = \bar{\alpha}$$
$$\text{Prob}\{\gamma_{k_s} = 0\} = 1 - \bar{\gamma}, \quad \text{Prob}\{\gamma_{k_s} = 1\} = \bar{\gamma}$$

where $\alpha \in [0, 1)$ and $\gamma \in [0, 1)$ are two known constants. The stochastic approach is applied and
some sufficient conditions are obtained to ensure the security requirements of the above system and
by solving certain LMIs with nonlinear constraints for calculating the desired controller gain.

7. Potential Suggestions

Unlike standard control applications, security control techniques for CPSs is still at its fancy. Due to
the core of critical infrastructures, the effects of successful attack on networked systems are generally
more damaging and this presents a major problematic of how to mitigate the impact of cyber-attacks
along with the other imperfections of the NCS.

Design a secure filter based on attacked measurement outputs so as to achieve acceptable index of
security performance [18] is by all means a significant research area. The existing filtering schemes are
not effectively capable of guaranteeing the security. The celebrated Kalman filter has the capability
of achieving the minimal variance of the filtering errors by considering exact knowledge of noise
statistics, however this assumption is usually not true for CPSs since statistical information of
transmitted signals are not readily captured [18].

The combined filtering and control problem with security constraints is an emerging and challenging
problem of research. In [19], a security-guaranteed estimation strategy has been formulated against
integrity attacks by using the minimax optimization technology, where the estimator optimally
minimizes the “worst-case” of the expected cost considering all possible attacks launched by the
adversary [18].

For practical applications, it is significant to address the scenario of facing multiple attacks at the
same time. An adaptive strategy defending against different types of attacks has not received much
attention industrial CPS and lacked the quality of service (QoS). Additionally, security requirements
and resource constraints in practical systems usually need to be considered simultaneously.

Finally, one of the important topic still not covered is to study the secure control systems in the
internet of things (IoT) applications. More examples and problems in this topic could be found in
[23].
8. Conclusions

In this paper, we reviewed the basics of cloud-based control system as a natural extension of networked control systems. Then we focused on the ingredients of the secure control problem. The problem is treated as a multi-tasking optimal control problem for a class of NCS in simultaneous presence of DoS attacks, deception attacks and physical attacks.

Acknowledgment

This work is supported by the deanship of scientific research (DSR) at KFUPM for support through distinguished professorship award project No. IN-161065.

[1] P. Antsaklis, and J. Baillieul, “Special issue on technology of networked control systems,” Proc. the IEEE, vol. 95, no. , pp. 5–8, 2007.
[2] M. S. Mahmoud, “Networked control systems analysis and design: An overview,” Arabian Journal for Science and Engineering, vol. 41, no. 3, pp.711–758, 2016.
[3] M. S. Mahmoud, “Architecture for cloud-based industrial automation”, Proc. the Third International Congress on Information and Communication Technology (ICICT 2018), London, UK, February 27–28, 2018, Paper 19.
[4] Yuanqing Xia, “From networked control systems to cloud control systems”, Proceeding of the 1st Chinese Control Conference, pp. 5878–5883. 2012.
[5] D. Bakken, ed., “Smart Grids: Clouds, Communications, Open Source, and Automation,” CRC Press, 2014.
[6] Wang, X.; Jia, D.; Lu, C.; Koutsonkos, X., “DEUCON: Decentralized End-to-End Utilization Control for Distributed Real-Time Systems”, IEEE Trans. Parallel and Distributed Systems , vol. 18 , no. 7, 2017, pp. 996–1009.
[7] Kaikhura, Bhavya, Yungshiang S. Han, Swastik Brahma, and Pramod K. Varshney, “Asymptotic analysis of distributed Bayesian detection with Byzantine data,” IEEE Signal Processing Letters, vol. 22, no. 5, 2015, pp. 608–612.
[8] Kaikhura, Bhavya, Yungshiang S. Han, Swastik Brahma, and Pramod K. Varshney, “Distributed Bayesian detection in the presence of Byzantine data,” IEEE Trans. Signal Processing, vol. 63, no. 19, 2015, pp. 5250–5263.
[9] Rawat, Ankit Singh, Priyank Anand, Hao Chen, and Pramod K. Varshney, “Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks,” IEEE Transactions on Signal Processing, vol. 59, no. 2, 2011, pp. 774–786.
[10] E. Mousavinejad, F. Yang, Q. L. Han, L. Vlacic, “A novel cyber attack detection method in networked control systems”, IEEE Trans. cybernetics, vol. 99, 2018, pp. 1-11.
[11] Hoque, N., H. Kashyap, and D. K. Bhattacharyya, “Real-time DDoS attack detection using FPGA,” Computer Communications, vol. 110, 2017, pp. 48-58.
[12] Semerci, Murat, Ali Taylan Cemgil, and Bulent Sankur, “An Intelligent Cyber Security System Against DDoS Attacks in SIP Networks,” Computer Networks, 2018.
[13] Ali, Yasir, Yuanqing Xia, Liang Ma, and Ahmad Hammad, “Secure design for cloud control system against distributed denial of service,” Control Theory and Technology, vol. 16, no. 1, 2018, pp. 14–24.
[14] Srikantha, Pirathayini, and Deepa Kundur. “Denial of service attacks and mitigation for stability in cyber-enabled power grid,” Innovative Smart Grid Technologies Conference (ISGT), IEEE Power & Energy Society, 2015, pp. 1–5.
[15] Beitolahi, Hakem, and Geert Deconinck, “A dependable architecture to mitigate distributed denial of service attacks on network-based control systems,” Int. J. Critical Infrastructure Protection, vol. 4, no. 3-4, 2011, pp. 107–123.
[16] Sarker, Jahangir H., and Ahmed M. Nahhas, “Mobile RFID System in the Presence of Denial-of-Service Attacking Signals,” IEEE Trans. Automation Science and Engineering, vol. 14, no. 2, 2017, pp. 955–967.
[17] Tagra, Deepak, Musfiq Rahman, and Srinivas Sampalli, “Technique for preventing DoS attacks on RFID systems,” Int. Conf. Software, Telecommunications and Computer Networks (SoftCOM), 2010, pp. 6–10.
[18] Z. Wang, D. Wang, B. Shen, F. E. Alsadi, “Centralized security-guaranteed filtering in multirate-sensor fusion under deception attacks,” J. the Franklin Institute, vol. 355, no. 1, 2018, pp. 406–420.
[19] Y. Mo, B. Sinopoli, “Secure estimation in the presence of integrity attacks,” IEEE Trans. Automatic Control, vol. 60, no. 4, 2015, pp. 1145–1151.
[20] H. Bekizadeh, H. J. Marquez, “Multirate observers for nonlinear sampled-data systems using input-to-state stability and discrete-time approximation,” IEEE Trans. Automatic Control, vol. 59, no. 9, 2014, pp. 2409–2474.
[21] H. Tan, B. Shen, Y. Liu, A. Alsadi, B. Ahmad, “Event-triggered multi-rate fusion estimation for uncertain
system with stochastic nonlinearities and colored measurement noises,” Information Fusion, vol. 36, 2017, pp. 313–320.

[22] W. Chen, L. Qiu, “Stabilization of networked control systems with multirate sampling,” Automatica, vol. 49, no. 6, 2013, pp. 1528–1537.

[23] F. A. Alaba, M. Othman, I. A. T. Hashem, F. Alotaibi, “Internet of Things security: A survey,” J. Network and Computer Applications, vol. 88, 2017, pp. 10–28.

[24] D. Ding, Z. Wang, G. Wei, F. E. Alsaadi, “Event-based security control for discrete-time stochastic systems,” IET Control Theory & Applications, vol. 10, no. 15, 2016, pp. 1808–1815.

[25] M. Long, C. H. Wu, J. Y. Hung, “Denial of service attacks on network-based control systems: impact and mitigation.” IEEE Trans. Industrial Informatics, vol. 1, no. 2, 2005, pp. 85–96.

[26] C. D. Persis, P. Tesi, “Input-to-state stabilizing control under denial-of-service,” IEEE Trans. Automatic Control, vol. 60, no. 11, 2015, pp. 2930–2944.

[27] Z. H. Pang, G.P. Liu, Z. Dong, “Secure networked control systems under denial of service attacks,” IFAC Proceedings Volumes, vol. 44, Issue 1, 2011, pp. 8908–8913.

[28] Y. Shoukry, P. Tabuada, “Event-triggered state observers for sparse sensor noise/attacks,” IEEE Trans. Automatic Control, vol. 61, no. 8, 2016, pp. 2079–2091.

[29] S. Amin, A. A. Cardenas, S. S. Sastry, “Safe and secure networked control systems under denial-of-service attacks,” Int. Workshop on Hybrid Systems: Computation and Control, pp. 31-45. Springer, Berlin, Heidelberg, 2009.

[30] S. Amin, G. A. Schwartz, S. S. Sastry, “Security of interdependent and identical networked control systems,” Automatica 49, no. 1, 2013, pp. 186–192.

[31] G. K. Bebekadu, V. Gupta, P. J. Antsaklis, “Risk-sensitive control under Markov modulated denial-of-service (dos) attack strategies,” IEEE Trans. Automatic Control, vol. 60, no. 12, 2015, pp. 3299–3304.