New approach based on control theory to secure gas pipeline transportation system under cyber vulnerability

Dr. DJERIDANE Badis
Sonatrach, Midstream Activity
SidiArcine BP 08, Baraki, Algiers, ALGERIA
badis.djeridane@sonatrach.dz

Abstract— **In this work we propose new approach to address the problem of dealing with threats by making the controller more clever to detect any threat might come from the IT infrastructure of gas facility. Here we developed a new framework based on viability, for identifying the impact that an intrusion might have at central dispatch center, which regulates a flow to the specified nominal value and maintain the suction pressure, discharge pressure and discharge temperature in safe area. The numerical results reveal the weaknesses of the system and indicate that a possible policies to attack that an attacker could use to disturb it.**

I. INTRODUCTION

Electrical production utilities and home users are increasingly dependent on the proper functioning of the gas pipeline transportation system. Gas pipeline transportation system malfunction might lead to instability on Gas prices on international energy markets and expensive damage to equipment and economic effects, as well as harm to the population.

In order to operate effectively the energy supply chain systems today are highly dependent on an Information and Communication Technology (ICT) infrastructure with control and DCS (Distributed Control System) systems. Also these control systems have ever since their birth been designed for high reliability and availability. On the other hand, security was never an issue when these systems were designed. During the last decade these system have been interconnected to many other types of IT systems and, in many installations, with direct or indirect connections to external network. In the last years, because of this interconnection, much attention has been toward the threat coming from direct and undirect cyber-attacks towards control systems. For example, the spread of the Stuxnet malware specifically targeting a Siemens PLC for critical infrastructure, the cyber threat has gone from theoretical speculations to a present risk for critical infrastructure operators.

The purpose of this work has been to investigate and to better understand vulnerabilities in DCS and to combine this knowledge with the consequences in the gas pipeline transportation system if theses vulnerabilities indeed are exploited. With this knowledge the work has also been suggesting a countermeasures for identified weaknesses.

Here we investigate the impact of a cyber-attack on the DCS in compressor stations of gas pipeline transportation system. The primary objective of the DCS is to regulate a flow to the specified nominal value and maintain the suction pressure, discharge pressure and discharge temperature in safe area. DCS actions are usually determined for each compressor station at a central dispatch center. Measured flow at each compressor station is sent to this center and then a feedback signal that regulates the generated flow is sent back to the compressor station, participating in the DCS, through the Dispatching Center.

In order to demonstrate possible cyber-attacks and their consequences on the DCS system, in the gas pipeline transportation system a gas pipeline benchmark model is used. This model comes from numerical optimization of gas pipeline model of south gas of Algeria, this model is composed of pipeline line of length of 1000 Km and five compressor stations, also there exist a dispatching center located at the end of the pipeline. Each compressor station is controlled and supervised by DCS ABB of type AC 800 Freelance with redundant architecture and Plantguard triple redundant is used as ESD (Emergency ShutDown). A simulation of gas pipeline is used under Matlab environment in order to proof vulnerability of DCS system at some conditions.

II. PROBLEM STATEMENT

A. *viability formulation problem*

In order to determine whether there exists a signal for the attacker that could irreversibly disturb the the

gas pipeline, we perform an analysis based on viability methods. A viability for continuous and hybrid systems has been an important topic of research in the dynamics and control literature. This approach is widely used in air transportation management system, and also this methodology was used successfully to tackle the problem flight control. All thoses problems are viewed as a classic problem of viability framework. To the best our knowledge the problem of using viability formulation problem is used for the first time to underlying the problem of securing gas pipeline from cyber vulnerabilities.

The characterization of viability concepts can be formulated as optimal control or game theory problems [1], whose solution can be characterized using variants of the Hamilton-Jacobi-Bellman equations. Efficient algorithms developed to solve such PDE [2] can then be used to solve the viability problem numerically. In theory, this numerical tools is appropriate for systems of any state dimension. However the computational cost of higher than four dimension viability analysis is no practical options. The main reason is the exponential increase in computing time and resource requirements which clearly limits the use of these tools. Some efforts have been done to extend the use of continuous system viability tools to six dimensions, thus making them applicable to a number of interesting case studies in the area of aeronautics [3], but we still limited in the dimension size of the problem to be treated.

Another approach to compute a viability set is based on valued theory and viability theory [4]. The basic idea is to compute the value function by determining a viability kernel instead of solving a Hamilton-Jacobi-Belman's equation. The development of computational tools to support the numerous viability theory concepts is an ongoing effort [5]. Hence, this numerical tools based on set valued analysis used for viability computations come with theoretical proofs of convergence, but we have a few results about the numerical accuracy of the computations.

It's well known that, frequently, the complexity for computing the viability kernel even for lower dimensions. Hence, it appears natural to seek approximate method involving suitable discretization to facilitate computer work. Then the full discretization of state space always was an eternal challenge for the computational complexity for researchers for many decades. To overcome this difficulty, for example [6] propose a multi-grid method to a class of discrete time, continuous state, discounted, infinite horizon dynamic programming problems to improve the computational complexity for this class of system.

And another method called cell-mapping method using the basic idea to consider the state space not as continuous but rather as a collection of large number of state cells with each cell being taken as a state entity [7] [8]. This method has been successfully applied to optimal control problem [9], by representing all the admissible controls and their duration application as finite set. Then, the process of extracting optimal control results from the family of controlled mappings becomes a matter of systematic search.

However, all these methods suffer from an exponential computational complexity. Recently, new idea have emerged that could find solution at "most of time" for particular problem with "high confidence" that the candidate solution is the true solution. Randomized algorithms are gaining popularity among control theory community [10], and have been applied successfully to compute a reachable set using neural networks [11] and to system identification of ARMA Model [12]. Another application is the identification of a piecewise affine system presented in [13].

In this paper, we present the initial steps of an approach motivated by the theory of learning theory [14] that aims to beat the curse of dimensionality for viability kernel computation by generating points randomly instead of gridding over the whole state-space. Once we have all sample points, we start by ordering our sample points according to lexicographical scheme and afterwards all our operations will be based on this new representation of our points, with this scheme we took the advantage to be able to use efficient algorithms for searching inside a set, such as list algorithm.

Consider a continuous time control system,

$$\dot{x} = f(x,u) \tag{1}$$

with $x \in \mathbb{R}^n$, $u \in U \subseteq \mathbb{R}^m$ and $f(\cdot,\cdot) : \mathbb{R}^n \times U \to \mathbb{R}^n$. We assume that U is compact and f is bounded and Lipschitz continuous. Under these assumptions, for any $t \in \mathbb{R}^+$, $x \in \mathbb{R}^n$ and $u(\cdot) \in U$ system (1) admits a unique solution, we denote this solution by $\phi(t,x,u(\cdot))$ with $t \in \mathbb{R}^+$.

Given a set of states $K \subseteq \mathbb{R}^n$ the viability set we would like to compute is the set of states $x \in \mathbb{R}^n$ for which there exists a control input $u(\cdot) \in U$ that keeps the solution $x(\cdot)$ in K.

In other words,

$$Viab(K) = \{x \in \mathbb{R}^n | \exists u(\cdot) \in U, \forall \tau \in \mathbb{R}^+ \ \phi(\tau,t,x,u(.))\}$$

In the literature, this set has been characterized indirectly, based on optimal control [1], and indirectly, using non-smooth analysis tools [4]. Here we adopt the latter approach.

In the non-smooth analysis they used differential inclusion representation of the dynamical system described by (1)

$$\dot{x}(t) \in F(x(t))$$

where $F : \mathbb{R}^n \to \mathbb{R}^n$ is the set-valued map defined by

$$\forall x \in \mathbb{R}^n, F(x) := \{f(x,u), u \in U\}$$

Assume that the set K is closed and the set-valued map F is bounded. Namely

$$\exists M \geq 0, \forall x \in \mathbb{R}^n, \forall y \in F(x), \|y\| \leq M$$

And also assume that a set-valued map $F : \mathbb{R}^n \to \mathbb{R}^m$ is said to be lipschitz on $\mathbb{R}^n$ if there exists a positive real l satisfying

$$F(x_1) \in F(x_2) + l\|x_1 - x_2\|B \quad \forall (x_1, x_2) \in \mathbb{R}^n \times \mathbb{R}^n$$

where B denotes the closed unit ball of $\mathbb{R}^m$

To approach the viability kernel, we first replace the initial differential inclusion system by a finite difference inclusion. Let's consider F_ε an approximation of F satisfies the following properties:

1) upper semi-continuous with convex compact nonempty values.
2) $Graph(F_\varepsilon(.)) \in Graph(F(.)) + \phi(\varepsilon)B$ where $lim_{\varepsilon \to 0^+} \phi(\varepsilon) = 0^+$
3) $\forall x \in X, \cup_{\|x-y\| \leq M\varepsilon} F(y) \in F_\varepsilon(x)$

Let's construct a discretization F_ε which satisfies the above assumptions, then a natural choice of discretization is

$$F_\varepsilon(x) := F(x) + \varepsilon M l B$$

where B is unit ball in $\mathbb{R}^n$. Then, the discretized dynamic corresponding to Euler scheme is

$$x_{k+1} \in x_k + \varepsilon F_\varepsilon(x_k)$$

The approximation of the viability kernel is divided in two steps:

1) discretization over the time through the use of Euler scheme
2) discretization over the state-space (full discretization)

Then, the viability kernel computation can be determining by the following decreasing sequence of closed sets K^n defined by

Algorithm 1 Computation of the viability kernel: Partial discretization

$K^0 := K$
$K^{p+1} := \{x \in K^p | [x + \varepsilon F_\varepsilon(x)] \cap K^p \neq \emptyset\}$

In this algorithm 1 we are checking wether or not the successor of x_k still inside the set K at each iteration. Then the viability kernel is defined for partial discretization by

$$Viab(K) = \cap_{p=0}^{\infty} K^p$$

In full discretization we are dealing with finite systems, hence we should associate to each set K its projection onto the grid defined by

$$K_h := (K + hB) \cap X_h$$

and the viability kernel computation could be summarized for the case of full discretization at the following algorithm

Algorithm 2 Computation of the viability kernel: Full discretization

$K^0_{\varepsilon,h} := K_h$
$K^{p+1}_{\varepsilon,h} := \{z_h \in K^p_{\varepsilon,h}$ such that : $\left[z_h + \varepsilon F_{\varepsilon,h}(z_h)\right] \cap K^p_{\varepsilon,h} \neq \emptyset\}$

where z_h is a collection of finite points in the set K_h. We should notice that in [5] they have apply the refinement principle which allows to avoid redoing computation over all the initial domain at each change of discretization step.

B. Framework of central dispatch center

The continuous flow of natural gas in a pipeline is facilitated by the help of compressor stations which boost the pressure at predetermined intervals along a pipeline. These stations are generally made up of basic components such as compressor and driver units, scrubber/filters, cooling facilities, emergency shutdown systems, and an on-site computerized flow control- Distributed Control System (DCS) and dispatch systems that maintains the operational integrity of the station [15].

The compressor stations add energy to the gas to overcome frictional losses and maintain the required delivery pressure and flow. Compressor station design has been essential over the years because it is very important in the successful implementation of natural gas pipeline transportation [**?**]. The pressure difference between the discharge side of one station and the suction into another station is responsible for the gas Let us consider the a gas pipeline transportation system described in Fig. 1 which consists of two interconnected compressor station, each one equipped with its own Distributed Control System DCS, connected by gas pipeline.

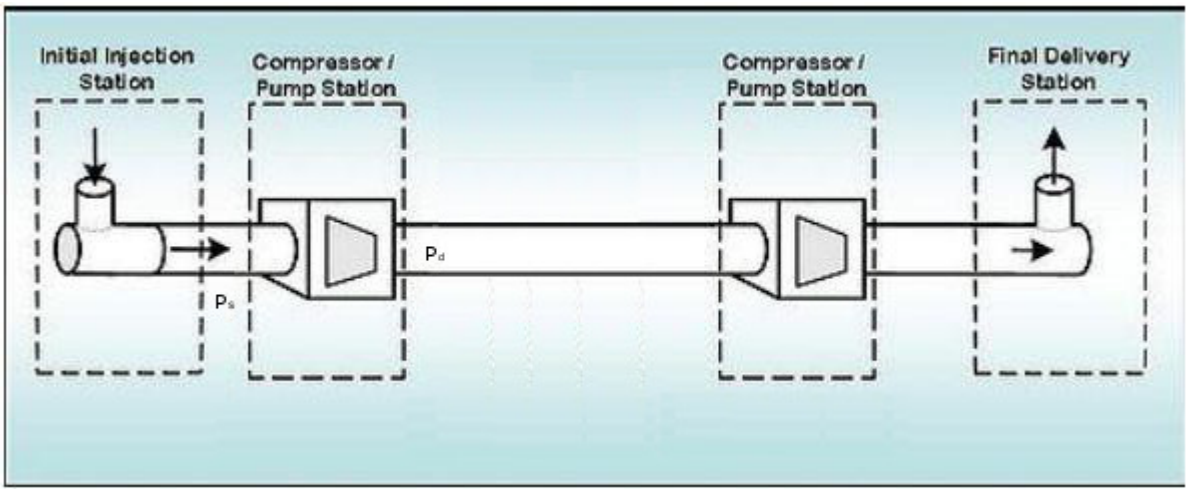
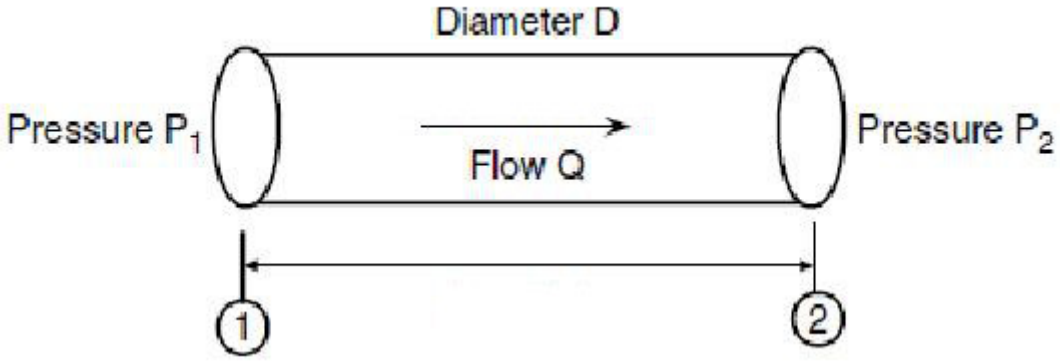


Fig. 1. A typical compressor station model



Each compressor station can be modeled as nonlinear function related to suction pressure P_s, discharge pressure P_d and mass flow rate Q. A compressor station can be disabled which mean that the pressure of discharge is equal to the pressure of suction $P_d = P_s$. Also, the compressor station can be enabled which make that the pressure of discharge is greater than the pressure of suction $P_d > P_s$, then we can write:

$$P_d = f_P(P_s, Q) \tag{2}$$

In order to overcome the complex mathematical models, we are assuming that each compressor station is approximated by the equivalent linear model.

On other hand, the behavior of pipeline can be modeled by the pressure at both ends and the gas flow. The model is based on piecewise linear function that integrate pressures P_1, P_2at the both side of pipeline and flow as stated below:

$$P_1 = a(Q)P_2 + b(Q) + c(Q)Q \tag{3}$$

where a, b and c are parameters depending on mass flow Q. Those parameters are highly related to each specification of pipe.

The pipe model is connected to the transmission network (nodes and compressor stations) by means of real variables representing the three states defining a pipe (Temperature, pressure and flow). However, for simplification purpose we consider only the case of model depending heavily on flow and pressure. Then, the pressure required to transport a given volume of gas through a pipeline is one of the factors which controls pipe selection. The pipe internal pressure is a parameter that can cause permanent deformation if allowed to reach or exceed the yield strength of the pipe. Obviously, the pipe should have sufficient strength to handle the internal pressure safely.

A dynamic simulator using optimization approach to compute the optimal compressor operating policies so that their energy consumption is minimized, while keeping the system in a safe region in order to protect pipe and compressor to be damaged.

In summary we consider the system to be safe when

the state trajectories of (3) lie inside the following safe set of the state space:

$$P_s \in [P_s min; P_s max] P_d \in [P_d min; P_d max] \qquad (4)$$

Moreover it should be noted that large pressure oscillations in the pipeline could make irreversible damage and can lead to stop the gas pipeline. This potential threat make the gas transmission system vulnerable to disturbance that a cyber attacker could try to excite by his intrusion through Information Technology infrastructure of gas facility.

III. Simulation Results

In this section, we adopt the viability framework of Section II-A to provide answers to some questions concerning the safety of the gas pipeline system. For this purpose, is examined if the attacker, by applying a suitable control policy, is able to violate the safety constraints (4). Considering different bounds on the attack signal, it will be shown that for sufficiently large attack bounds, the gqs pipeline system is vulnerable to such cyber attacks. The case of violating of pressure constraint inside pipe between the two compressor stations is investigated and the analysis proves the existence of an attack strategy that might directly or indirectly lead to a damage of the gas pipeline. The scenarios have been tested numerically by the tools of Randomized Algorithm developed by [11].

In this part, we will examine if the attacker could develop a strategy so as to exceed the pressure bounds (safe region) for the case of gas pipeline GR1 and GR2 Benchmark. This pipeline of 48 inch managed by Sonatrach, length is more than 1000 km, composed by five compressor station, each compressor station supervised by DCS with redundant architecture developed by ABB of type AC800 Freelance.

Therefore, we define K, safe region, as

$$K = \{P \in \mathbb{R}^2 | 40bar < P_s < 45bar, 55bar < P_d < 70bar\} \qquad (5)$$

and the distance function $l(x) = min\{P_s - 40, 45 - P_s, P_d - 55, 70 - P_d\}$.

For the safety analysis, we performed a series of viability computations for different bounds of probable attack input. Through the computation of the volume of safe region for different bounds of flow gas, we can conclude that the attacker would need quantity at least 2 million cubic meter per hour as flow Q. In the case where attacker is able to inject an arbitrary quantity up to 1.5 million cubic meter per hour, we remark that after 30 min it turns out that for this horizon the viability computation has already reached steady state.

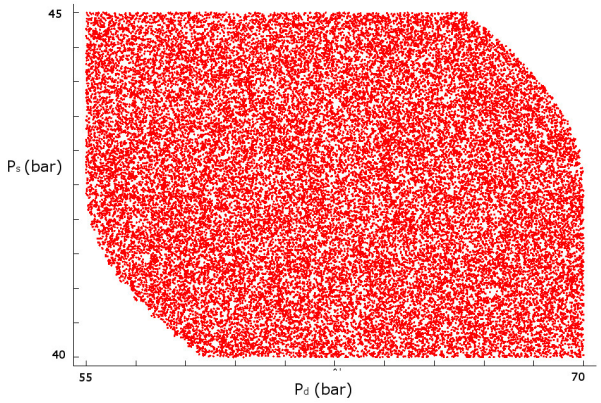


Fig. 2. Safe Region for the controller DCS

IV. Conclusions

A viability framework to perform safety analysis for a two compressor station was developed. This analysis proposed a new methodology so as to identify how an attacker probably could disturb the system by gaining access to the DCS, and determine the policy that he should follow to disrupt the system. Our approach was tested numerically, by using computational tools based on viability. In our work, we assumed the scenario of the worst-case that the attacker has access to all system states, which is might be hardly applicable.

Another direction of research concerns the determination of the most appropriate structure of pipeline gas to approximate the system. Work is in progress to nd out the most efcient structure for our problem. We will also work on fault detection schemes to determine whether it is possible to diagnose the attackers action sufficiently fast before he disturbs the system.

Finally, we are working to test and verify the computation of the 'safe region' by using real-time simulations of process-models build in Matlab, and controller implemented in Control Builder. The connection between them is made by OPC Server.

V. Acknowledgments

The author gratefully acknowledge to Prof. John Lygeros, Head of Automatic Laboratory at Federal Polytechnic of Zurich for all gaining access to technical reports.

References

[1] J. Lygeros, "On reachability and minimum cost optimal control," *Automatica*, vol. 40, pp. 917–927, 2004.

[2] I. Mitchell, A. Bayen, and C. Tomlin, "Validating a hamilton jacobi approximation to hybrid reachable sets," in *Hybrid systems: Computation and Control*, M. DiBenedetto and A. Sangiovanni-Vincentelli, Eds. Springer-Verlag, 2001, pp. 418–432.

[3] I. Kitsios and J. Lygeros, "Aerodynamic envelope computation for safe landing of the hl-20 personnel launch vehicule using hybrid control," in *Mediterranean Conference on Control and Automation*, Limassol, June 2005.

[4] J. P. Aubin, *Viability theory*. Boston: Bikhauser, 1991.

[5] P. Cardaliaguet, M. Quincampoix, and P. Saint-Pierre, "Stochastic and differential games: Theory and numerical methods," in *Annals of the International Society of Dynamic Games*. Birkaser, 1999.

[6] C. Chow and J. Tsitsiklis, "An optimal multigrid algorithm for continuous state discrete time stochastic control," in *Conference on Decision and Control*, Austin, Texas, December 1988, pp. 1908–1912.

[7] C. Hu and H. Chiu, "A cell mapping method for nonlinear deterministic and stochastic systems -part i: The method of analysis," *Trans. ASME J. Appl. Mech.*, vol. 53, no. 3, pp. 702–710, 1986.

[8] ——, "A cell mapping method for nonlinear deterministic and stochastic systems -part ii: Examples of application," *Trans. ASME J. Appl. Mech.*, vol. 53, no. 3, pp. 695–701, 1986.

[9] F. Bursal and C. Hsu, "Application of a cell-mapping method to optimal control problems," *International Journal of Control*, no. 5, pp. 1505–1522, 1989.

[10] M. Ariola, C. Abdallah, and V. Koltchinskii, "Applications of statistical-learning control in system and control," in *IFAC Workshop*. Villa Erba, Cernobbio-Como: on Adaptation and Learning in Control and Signal Processing, Agust 29-31 2003.

[11] B. Djeridane, E. Cruk, and J. Lygeros, "A learning theory approach: to the computation of reachable sets," in *European Control Conference*, Kos, July 2007.

[12] M. Vidyasagar and R. Karandikar, "A learning theory approach to system identification," in *Technical committe on robust control*. Portugal: Workshop of IFAC, July 2002.

[13] M. Prandini, "Priecewise affine systems identification: a learning theoretical approach," in *Conference on Decision and Control*, Bahamas, December 2004, pp. 3844–3849.

[14] M. Vidyasagar, "Statistical learning theory and randomized algorithms for control," *IEEE Control Systems*, pp. 69–85, December 1998.

[15] R. Carter, "Pipeline optimization: Dynamic programming after 30 years," in *Proceedings of the 30th PSIG Annual Meeting*, San Diego, December 1998.

[16] S. P. S. S. Mokhatab and T. Cleveland, "Compressor station design criteria," *Pipeline and Gas Journal*, 2007.