Modelling Cooperative Control Problems in the Cyber Environment: Introduction to Quasi Consensus Networks

A. Edelmayer[1,2], L. Virág[1], J. Kovács[1]

[1]Systems and Control Laboratory, Institute for Computer Science and Control, Hungarian Academy of Sciences
H-1111, Budapest, Kende u. 13-17, Hungary
e-mail: edelmayer@sztaki.mta.hu

[2]Multidisciplinary School of Technical Sciences
Research Group for Systems and Control Theory
Széchenyi István University, H-9026, Egyetem tér 1, Győr, Hungary

Abstract: The paper introduces the novel idea of the application of quasi consensus networks to modelling networked distributed systems. Quasi consensus networks operate alike standard consensus seeking ones without requesting the information state of the contributing systems to converge to a predetermined value. The quasi consensus-modelling paradigm can be used in modelling cooperative control problems in the cyber environment when the achievement of a common value of the information state is not the ultimate goal of the systems operation.

Keywords: consensus seeking, cooperative systems, detection and estimation of cyber physical systems, distributed systems modelling, networked systems

1. Introduction

An emerging trend in modern control theory that reflects the use of distributed and networked dynamical systems in the information age is called cyber physical systems (CPS). CPSs integrate data acquisition, computation and communication to interact with the physical world and with other systems in an attempt to acquire, distribute and share data around each other. The amount of literature dealing with various categories of cyber physical systems, spanning from distributed robotic microsystems to large-scale networked systems, is wide and varied.

A special operational policy of distributed systems, emerged quite lately in modern control theory, is based on the principle of cooperation. Cooperative systems consists of a set of interacting autonomous agents, interconnected over an information network to achieve a common desired task and enhance operational effectiveness through cooperative teamwork. The agents exchange information over a communication medium, either on wires or wireless. Examples include large-scale mass transport and power (energy, electricity) distribution networks, ad-hoc vehicle networks and others.

A particular policy of operation within cooperative behaviour is called coordination. Coordination is the organisation of the different elements of a complex distributed system so as to enable them to work together in a controlled and supervised way. Potential application of the coordination idea includes formation control of vehicles required to maintain a prescribed shape during travel, or rendezvous problems, where the movement trajectories of two or more autonomous vehicles are required to meet in space and time.

Hence, devices which acquire, process and transfer information from one agent to another are inherent part of the system, and are recognised as critical infrastructure of the distributed (control) systems based on interconnected information technology, which cannot be disregarded when modelling. Properties of the information exchange process, and so this communication infrastructure (which is frequently referred to cyber infrastructure), is inseparable part of systems operation.

Due to the largely fragmented nature of CPSs and the cyber infrastructure itself, this specific architecture is exposed to the possibility of being harmed by environmental effects or attacked maliciously. As most CPSs, especially those consisting of mobile autonomous agents, such as vehicle and robotic networks, are based on wireless communication, communication links have to be assumed insecure. Information coded radio waves are potentially subject of interception. By obtaining trustful network information the attackers are able to bypass intrusion prevention techniques. Fake and malicious nodes e.g., may be able to hacked into the network by eavesdropping on network traffic acquiring network information for launching attacks. Therefore, vulnerability of cyber physical systems has received increasing attention in the past years and security has to be addressed as a primary concern.

As vulnerability is an engineering principle that cannot be securely avoided CPSs have to use proper protection techniques as precautionary measure. First of all it is absolutely necessary to know at each time instant if the system is intact, i.e., it is complete and not damaged or impaired in any way. Therefore, timely detection and identification of intrusions and other malicious actions is of a primordial design goal.

Existing techniques of fault detection and identification may provide standard means for the implementation of this protection mechanism for CPSs as attacks can be thought as faults. One difficulty with this analogy is that faulty behaviours caused by malicious actions may be very difficult to detect as the attacker have knowledge on the system itself and thus could be able to use masking techniques to conceal the action. Model-based fault detection is one of the most powerful methods to the solution of this problem, as it possesses information on the system as well.

Using model-based detection, however, necessitates the availability of a system model. Due to the crucial role of distributed and networked systems, including CPSs, in advanced engineering systems modelling of these type of systems have received much attention lately. Recent modelling approaches are motivated by existing CPS use cases and attack experiences basically relying on representation of the complex CPS as a single, homogeneous entity of interconnected dynamical systems with special focus on the modelling of the interconnection scheme, while the behaviour of the cyber infrastructure is not explicitly treated by the theory.

This paper, instead of committing itself to the discussion of the detection problem as a whole, addresses the modelling issue only. A novel modelling paradigm i.e., the concept of quasi-consensus networks is introduced that can be useful in the description of the cyber infrastructure in cases when some conditions, posed by the standard consensus seeking operation, can be resolved. This specific system model, analogously to [9], allows the introduction of misbehaving agents for the modelling of faulty and/or changed behaviour of the system without taking particular restrictions on the way the consensus seeking is made.

The layout of the paper is as follows. In Section 2 the techniques that have been recently used for modelling CPSs are briefly reviewed. Based on this knowledge this is followed by the introduction of quasi consensus networks in Section 3. A brief section of conclusions on future works closes the paper.

2. Modelling Cyber Physical Systems

Living with the constructive assumption that cyber physical systems can be thought of like a set of interconnected dynamical systems, which are modelled by linear time invariant (LTI) dynamics the approach of [10] became quite common in the synthesis and analysis of large-scale CPSs. This approach considers the set of connected subsystems

$$\begin{aligned} x_i(t) &= A_i x_i(t) + B_i u_i(t), \\ y_i(t) &= C_i x_i(t) + D_i u_i(t) \end{aligned} \qquad (1)$$

with the state $x_i(t) \in \mathbb{R}^n$, input $u_i(t) \in \mathbb{R}^m$ and measurement $y_i(t) \in \mathbb{R}^p$ vectors of the individual subsystems. The matrices A_i, B_i, C_i and D_i are given in the appropriate dimensions. These can be combined by taking interconnections among subsystems into consideration to produce the overall system equations by the time invariant descriptor system [5] in the form

$$\begin{aligned} E\dot{x}(t) &= Ax(t) + Bu(t), \\ \mathrm{y}(t) &= Cx(t) + Du(t), \end{aligned} \qquad (2)$$

where $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^p$ are the state, input and measurement vectors of the combined system, respectively. $E \in \mathbb{R}^{n \times n}$ is called the connectivity matrix of the system, which encodes the interconnection structure of the networked subsystems. For practical reasons E is generally required to be singular. The input $u(t)$ can be thought quite generally, it can be composed and extended arbitrarily, representing unknown inputs, failures and other incipient effects depending on the purpose of modelling, which affect the plant in predetermined directions.

An obvious shortcoming of this modelling approach comes from the assertion that subsystems dynamics is viewed to be homogeneously LTI, which may prove to be a very strong assumption in modelling of complex, large-scale CPSs. For the difficulties of the use of nonlinear descriptor systems, see [6]. The use of heterogeneous or hybrid system models (containing LTI and nonlinear subsystems jointly) is not a viable modelling option neither.

The classical modelling approach, which is based on the composition of the set of autonomous systems (2) that perform and are modelled individually then connected together as in (2), is useful in modelling large-scale CPSs. Examples can be cited from mass transport and power distribution networks.

A somewhat different approach is needed to CPSs, where compared to the previous approach, the emphasis of operation (and thus, modelling) is not on individual system dynamics but the quality of information acquisition and exchange, moreover, the devices which transmit and process information, i.e., the principles of communication and networking. This is a modelling approach where the performance of the cyber-infrastructure of the network gets in the forefront. Cyber-infrastructure is considered the enabling body of CPS functionality and viewed as the medium in which the input acquisition, processing and transmission of information occurs. Control and detection of cyber-infrastructure that must ensure that the global CPS are kept in an operating condition as expected is therefore of primary importance.

A particular class of advanced CPS applications is based on the principle of cooperation. In the modern theory of decentralised and distributed control, cooperative systems are thought to be as composed of multiple dynamic entities that share and exchange information or tasks among each other to support a common effort. The shared information among contributing parties of the overall system, which may take the form of common objectives, common control algorithms or common data is a necessary condition for cooperation [13]. Performing in the cyber environment in an attempt to align a common objective requires among coordinated systems to share a consistent view of the goals and other control specific data that is critical to the accomplishment of that objective. The instantaneous value of that information is called the information state [12].

Cooperative systems collect and exchange information by communication and sensing, and as such, are ultimately based on the quality and performance of the cyber-infrastructure. Coordinated control and filtering (targeting vehicle formation control, rendezvous and attitude alignment problems, flocking, foraging, payload transport and enhanced position estimation just to mention a few) are typical applications of the cooperating idea [1, 8, 14].

Consensus seeking cooperation algorithms are best known from coordinated control problems. In classical coordination systems, the goal is the zeroing of the difference of the value of the information states around all the contributing systems. To achieve a successful coordination, the contributing systems have to agree (i.e., have to have information consensus) over the objective value of the information state. In coordinated control scenarios, therefore, the goal is to design a control law so that the information states of the coordinated systems converge to a common value in time (*cf.* rendezvous problem) [2, 3].

This control law can be implemented by means of consensus iterations, where, at each iteration, the contributing actors get closer to the implementation of the common objective. In classical consensus iterations, at each time instant, a contributing system update its state as a weighted combination of its own value and also those received from the partners. As a result of this procedure the information state may converge to the objective value in case stability can be ensured.

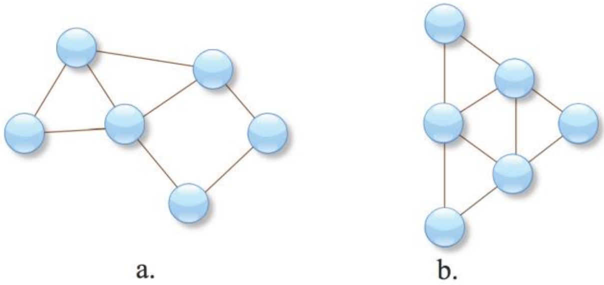

Figure 1. The initially unordered structure of vehicle topology (see Fig. 1/a) is made structured and ordered (Fig. 1/b) by selecting the distance between immediate neighbours as information state and applying a consensus algorithm to iteratively modify the value of this state as long as the desired formation is reached, i.e., until all the information states are equal

The most typical application of the consensus algorithm is in vehicle formation control, see Fig. 1, when onboard vehicle controllers manoeuver each vehicle to the equidistant locations which satisfy the geometric criteria of the formation. In the next section the consensus-based modelling is reviewed briefly and the idea of quasi-consensus networks is introduced.

3. Linear quasi-consensus networks

Standard consensus problems assume similar dynamics on the information state of each subsystems (*cf.* the assumption made in system models (2) for the system state dynamics). Apart from all the works which tend to model CPSs as linear descriptor systems it is a common approach to model information exchange among dynamical subsystems by means of graph theory. Team's communications topologies can be represented with directed or undirected graphs. This modelling technique became very popular as it fits to the description of complex networked system structures.

Consider the pair (N, E) denoting a directed graph with vertex set $N = \{1, \dots, n\}$ and edge set $E \subset N \times N$. The edge $(i, j) \in E$ indicates that the node (or agent) j can obtain information from node i. As the graph is directed, this is not necessarily vice versa and i is called the parent node and j is the child node. Undirected graphs are considered a special case of undirected ones where the edge (i, j) in the undirected graph corresponds to (j, i) in the directed one. The physical meaning of directed graph representation is that information flow is considered unidirectional between nodes, while undirected graph may represent bidirectional flow of information.

For the representation of the interconnection structures one needs to introduce the so called adjacency matrix that describes the structure of neighbourhood connections. The adjacency matrix $A = [a_{ij}] \in \mathbb{R}^n$ of the node set $N = \{1, \dots, n\}$ is defined such that a_{ij}

is a positive weight if $(j,i) \in E$, while $a_{ij} = 0$ if $(j,i) \notin E$. If weights are not relevant in the model, then $a_{ij} = 1, \forall\, (j,i) \in E$.

Based on the linear graph theoretic notions defined above the most common continuous time consensus seeking problem, similarly to [4] [11], can be represented by the linear system

$$\dot{x}_i(t) = -\sum_{j=1}^{n} a_{ij}(t)\big(x_i(t) - x_j(t)\big), \quad i = 1, \ldots, n, \tag{3}$$

where $a_{ij}(t)$ is the (i,j) entry of the adjacency matrix of the associated communication graph at time t and x_i is the information state of the i^{th} subsystem (node). Setting $a_{ij} = 0$ means that subsystem i cannot receive information from subsystem j. Realize that the dynamics of system (3) is determined by the difference of the information state of the neighbouring subsystems.

Ensuring stability the information state $x_i(t)$ of subsystem i is driven toward the state of its immediate neighbours. Obviously, the critical question is, if under what conditions the information states of all nodes in the connected network converge to a common predetermined value and, in what time. This is the point when traditional consensus algorithms become problematic. Even in fixed, time invariant topologies, it is possible to guarantee only that the common value of the negotiated information state is a convex combination of the initial ones. However, topologies are more frequently dynamic and satisfying conditions under which the consensus is stable during random switching of the communication topologies is not trivial. As an additional difficulty, consensus making must satisfy certain requirements for performance criteria such as convergence time.

Now let the linear iteration over the adjacency matrix A be defined in terms of the matrix Laplacian. The Laplacian matrix $L = [\ell_{ii}] \in \mathbb{R}^{n\times n}$ of a directed graph, similarly to [7] is defined such that $\ell_{ij} = \sum_{j\neq i} a_{ij}$ and $\ell_{ij} = -a_{ij}$ for all $i \neq j$. If $(j,i) \notin E$ then $\ell_{ij} = -a_{ij} = 0$ to satisfy the conditions

$$\ell_{ij} \leq 0 \quad i \neq 1,$$

$$\sum_{j=1}^{n} \ell_{ij} = 0 \quad i = 1, \ldots, n.$$

Based on the above the consensus algorithm [9] can be written in matrix form as

$$\dot{x}(t) = -L(t)x(t), \tag{4}$$

where $x = [x_1, \ldots, x_n]^T$ is the information state and $L(t) = [\ell_{ij}(t)] \in \mathbb{R}^{n\times n}$ is the Laplacian of the interconnection graph that serves for the update rule of the information state $x(t)$. We say that (4) is consensus seeking if, for all initial information state $x_i(0)$ and all $i,j = 1, \ldots, n$ the state difference $\tilde{x}_{ij} = |x_i(t) - x_j(t)|$ disappears i.e., it converges to zero as $t \to \infty$.

While the consensus paradigm discussed above is useful for many coordinated control applications, the assumptions might not be appropriate when each agent's information state evolves in an uncoordinated fashion and the objective of the control problem is different than zeroing out the state differences.

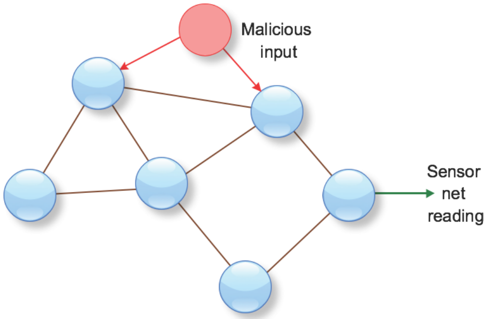

Figure 2. Sensor network under cyber attack

There are problems, however, when posing conditions for the information state convergence is overly restrictive and simply not necessary.

Consider, for example, the case of distributed sensor networks: the elements of the network provide measurement data at the output of the network which contain measurements slightly different from node to node, even in case we have a homogeneous set of redundant sensors in the network. If the measurement value is considered the information state of the network it is meaningless to require that this value converges to anything. However, the system model (4) still describes the connectivity of the network and provides useful means to model the information exchange around the network elements.

Proposition 1: The system representation (4) is thought quasi consensus network if, for all initial information state $x_i(0)$ and all $i,j = 1, \dots, n$ the state difference $\tilde{x}_{ij} = |x_i(t) - x_j(t)|$ is bounded as $t \to \infty$.

Note that the obvious extension of Proposition 1 includes systems permitting $\tilde{x}_{ij}$ to converge to a bounded constant value. Recall that traditional consensus systems like (3) ensures only that the information state converges to a common value but does not let the specification of a particular value of that state. Many cooperative problem setup in advanced control theory can be represented by quasi consensus system models. Examples are heterogeneous ad-hoc vehicle networks and sensor networks.

Quasi consensus models allow for some network elements to update their state differently than specified by the update matrix L. This is required for modelling faults and external disturbances or even malicious effects. By adding an exogenous input to the network to model (4) malicious inputs or other cyber attacks can be modelled as depicted in Fig. 2. A quasi consensus network with faulty behaviour can be represented as

$$\dot{x}(t) = -L(t)x(t) + B_v u_v(t), \tag{5}$$

where $u_v(t)$ is the malicious effect, which affects the network in the predetermined direction B_v. Now standard methods of fault detection can be used for the detection and isolation of the attack. This, however, is not in the scope of the paper.

4. Conclusions

This article provided a brief introduction to quasi consensus networks, a modelling paradigm applicable to networked decentralised systems. The approach fits to the description of heterogeneous cyber physical systems subject to faults and other external disturbances or malicious effects. Application of the quasi consensus seeking idea widens the possibility of the application of advanced methods of control and detection in the field of CPSs. More work will be needed to clarify the properties of the matrix Laplacian L in view of the application of particular detection and control problems, moreover, the construction and evaluation of malicious input models in the quasi consensus representation.

Acknowledgement

This work was supported by the project TÁMOP-4.2.2.C-11/1/KONV-2012-0012: *Smarter Transport – IT for cooperative transport systems*, which is supported by the Hungarian Government and co-financed by the European Social Fund. The financial support is gratefully acknowledged by the authors.

References

[1] Caughman, J.S., Lafferriere, G., Veerman, J.J.P., Williams, A.: *Decentralized control of vehicle formations*. Sys. Contr. Lttrs., vol. 54, no. 9, pp. 899-910, 2005

[2] Lin, J., Morse, A.S., Anderson, B.D.O.: *The multi-agent rendezvous problem*. In: Proceedings of 42nd IEEE Conference Decision and Control, vol. 2, pp. 1508-1513, 2003
DOI: 10.1109/CDC.2003.1272825

[3] Lin, J., Morse, A.S., Anderson, B.D.O.: *The multi-agent rendezvous problem - the asynchronous case.* In: Proceedings of 42nd IEEE Conference Decision and Control, vol. 2, pp. 1926-1931, 2003
DOI: 10.1109/CDC.2004.1430329

[4] Jadbabaie, A., Jin, J., Morse, A.S.: *Coordination of groups of mobile autonomous agents using nearest neighbour rules*. IEEE Transaction of Automatic Control, vol. 48, no. 6, pp. 988-1001, 2005

[5] Luenberger, D.G.: *Dynamic equations in descriptor form*. IEEE Transaction of Automatic Control, vol. 22, no. 3, pp. 312-321, 1977

[6] Luenberger, D.G.: *Non-linear descriptor systems.* Journal of. Economic Dynamics and Control, vol. 1, no. 4, pp. 219-242, 1979

[7] Merris, R.: *Laplacian matrices of graphs: a survey.* Linear Algebra and its Applications, no. vol. 197, no. 198, pp. 143-176, 1994

[8] Olfati-Saber, R., Jalalkamali, P.: *Coupled distributed estimation and control for mobile sensor networks.* IEEE Transaction of Automatic Control, vol. 57, no. 10, pp. 2609-2614, 2005

[9] Pasqualetti, F., Bicchi, A., Bullo, F.: *Consensus computation in unreliable networks: a system theoretic approach.* IEEE Transaction of Automatic Control, vol. 57, no. 1, pp. 90-104, 2012

[10] Pasqualetti, F., Dörfler, F. Bullo, F.: *Attack detection and identification in cyber-physical systems.* IEEE Transaction of Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013
DOI: 10.1109/TAC.2013.2266831

[11] Ren, W., Beard, R.W.: *Consensus seeking in multi agent systems under dynamically changing interaction topologies*. IEEE Transaction of Automatic Control, vol. 50, no. 5, pp. 655-661, 2005

[12] Ren, W., Beard, R.W., Atkins, E.M.: *Information consensus in multivehicle cooperative control.* IEEE Control Systems Magazine, vol. 27, no. 2, pp. 71-82, 2007

[13] Ren, W, Beard, R.W., McLain, T.W.: *Coordination variables and consensus building in multiple vehicle systems.* In V. Kumar, N. E. Leonard, and A. S. Morse, editors, Lecture Notes in Control and Information Sciences, pp. 171-188, 2004

[14] Veerman, J.J.P., Lafferriere, G., Caughman, J.S., Williams, A.: *Flocks and formations*. Journal of. Statistical Physics, vol. 121, no. 5-6, pp. 901-936, 2005