Research Article

Modeling cooperative behavior for resilience in cyber-physical systems using SDN and NFV

Jose Moura[1,2] · David Hutchison[3]

Received: 9 May 2020 / Accepted: 12 August 2020 / Published online: 19 August 2020

Abstract
Cyber-Physical Systems (CPSs) are increasingly important in everyday applications including the latest mobile devices, power grids and intelligent buildings. CPS functionality has intrinsic characteristics including considerable heterogeneity, variable dynamics, and complexity of operation. These systems also typically have insufficient resources to satisfy their full demand for specialized services such as data edge storage, data fusion, and reasoning. These novel CPS characteristics require new management strategies to support the resilient global operation of CPSs. To reach this goal, we propose a Software Defined Networking based solution scaled out by Network Function Virtualization modules implemented as distributed management agents. Considering the obvious need for orchestrating the distributed agents towards the satisfaction of a common set of global CPS functional goals, we analyze distinct incentive strategies to enact a cooperative behavior among the agents. The repeated operation of each agent's local algorithm allows that agent to learn how to adjust its behavior following both its own experience and observed behavior in neighboring agents. Therefore, global CPS management can evolve iteratively to ensure a state of predictable and resilient operation.

Keywords Cyber-physical systems · Internet of things · Software-defined networking · Game theory · Network function virtualization · Threats and cyber-attacks · Algorithms · Resilience · Resilient systems · Cooperation · Orchestration · Robustness

1 Introduction

A Cyber-Physical System (CPS) is essentially a physical facility with embedded sensors and actuators that can be remotely monitored and controlled by computerized systems [1], which we assume here are distributed virtualized agents implemented by Virtual Network Functions (VNFs), most of them located at the network edge. The monitoring and control of CPS are made by logical control loops over physical communication channels. These channels are established between the sensors/actuators and the VNFs. The channels transfer data representing the facility status and control messages to change the operation mode. CPSs are increasingly found in diverse applications areas such as power grids [2, 3], smart buildings [4, 5], next-generation mobile communication systems [6, 7], healthcare systems [8, 9], and also in precision farming systems [10, 11].

Recent years have shown the increasing relevance of CPSs in every day of our lives. In this way, the reliable acquisition and processing of the data originated at the physical part of each CPS become very important. To support the efficient extraction of useful knowledge from the processed CPS data, we argue that, in the current work, several research areas and techniques need to be combined. These are Software Defined Networking (SDN) [12] and Network Function Virtualization (NFV) [13], edge

✉ Jose Moura, jose.moura@iscte-iul.pt; David Hutchison, d.hutchison@lancaster.ac.uk | [1]School of Technology and Architecture, ISCTE-Instituto Universitário de Lisboa, 1649-026 , Lisbon, Portugal. [2]Instituto de Telecomunicações, 1649-026, Lisbon, Portugal. [3]School of Computing and Communications, InfoLab21, Lancaster University, Lancaster LA1 4WA, UK.

SN Applied Sciences (2020) 2:1534 | https://doi.org/10.1007/s42452-020-03335-4

computing [14], system modeling [15], and machine learning [16]. The extraction of useful knowledge can hopefully enable a CPS proactive management [17] by either a high-level layer [18] or even a cross-layer [19] system functionality responsible to enforce the fulfilment of orchestrated management policies in federated use cases [20], involving diverse administrative domains. Due to the non-centralized design of a CPS, there are several virtualized (i.e. VNF) agents managing that CPS. In this way, each VNF agent is responsible for the supervision and control of a specific part of the CPS. Consequently, a specific VNF agent should take individual decisions based on some local system contextual information. Nevertheless, each VNF agent has unique contextual information which, due to reasons including locality, may be different from what is available to others. Consequently, each VNF agent could make management decisions conflicting with the decisions of others. Thus, counter-balancing the flexibility of a distributed NFV approach, the CPS may have a sub-optimal performance when compared to centralized decision-making. This optimization inefficiency of the distributed management is like a system cost, representing a degradation of the CPS performance. To mitigate this performance degradation, we argue in favor of the utilization of a system mechanism to incentivize cooperation and to support orchestration amongst VNF agents [21]. This orchestrated management among the agents is a key feature to ensure the main functional objectives of the associated CPS. Following this, we study the agents' evolving behavior in support of the optimized global operation of the CPS. We consider the learning capability in each VNF agent that adjusts its behavior following both its own experience and the observed behavior from others, by repeated operation of the agent's local algorithm. Thus, the global CPS management can evolve in a consistent way (much like a centralized design), converging to the expected operation of that CPS.

The paper has the following structure. Section 2 discusses related work. The design of a software-defined resilient CPS is described in Sect. 3. Section 4 outlines the implementation details of our proposal. An analysis of the proposed approach is presented in Sect. 5. Section 6 concludes the paper and outlines future research directions. The paper's logical organization is illustrated in Fig. 1. This paper builds on unpublished online material from the same authors, available at [22].

2 Review of literature

A considerable amount of work has recently been done in each of the major areas addressed by our current paper. The contribution in [18] presents a fundamental and updated background in resilience and related concepts. It also offers a comprehensive discussion on diverse relevant scenarios for CPSs and on foundational technologies to enforce resilience in CPSs. Specifically, the authors of [23] discuss the state of the art in resilient networked systems.

Modern CPSs can be treated as large-scale heterogeneous distributed systems. In this context, when adequate supervision and control are also required for network-wide resilience, it is crucial to study the efficient

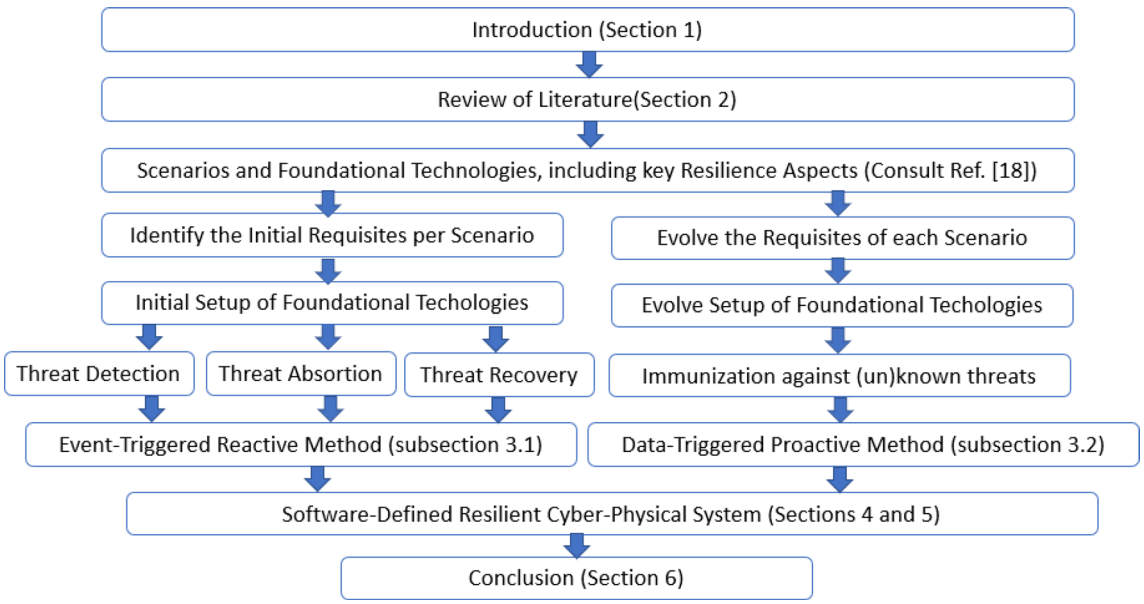

Fig. 1 Structure of the paper

orchestration [24] of a set of software-based services that must cooperate among themselves to fulfil the global resilience requirements [25]. Some software-based services that are pertinent to enforce wide-area resilient networked systems are pointed out in [25], such as traffic classification, anomaly detection, or traffic shaping. In addition, the mobile network edge access should be investigated in novel ways, e.g. ubiquitous access, supported in previous related work [26]. Further, legacy networking techniques for achieving end-user QoS are still relevant, such as the notion of filters as originally proposed in [27].

The analysis of a resilient CPS can be made using a theoretical model. A very popular tool to perform system analysis is Game theory (GT) [15]. It is very useful for analyzing the diverse situations that could impair the system's normal operation. GT also enables the building of automatic models with either bounded rationality or decision uncertainty to safeguard the system's key functionalities in spite of the occurrence of serious threats [28]. In addition, the diverse model players should not only optimize their individual outcomes, but they should also coordinate among themselves towards the fulfilment of common global system goals. In our research experience, the efficient coordination among players can be globally guaranteed by correct incentives endorsed by the system model towards the system players cooperate among themselves. Aligned with these ideas, we have reviewed the literature for theoretical models in CPSs that incentivize cooperation among the players. This cooperation is fundamental to resilient CPSs, and it is discussed below.

The authors of [29] provide an in-depth literature review in viable incentives for mobile crowdsensing, discussing lotteries, auctions, trust and reputation proposals. In contrast, [30] introduces a novel approach for mobile crowdsensing, viz. a social incentive mechanism that enforces the coordinated positive contributions of mobile users sensing their context via their smartphones towards some global system goals. In [29] the authors discuss the relevance of contract theory to design incentive mechanisms for use cases in wireless networks such as traffic offloading, spectrum trading, or mobile crowdsourcing.

We have found a considerable number of contributions addressing incentive models for cooperation among players in Vehicular Ad Hoc Networks (VANETs) to study the evolution of players' behavior (selfish vs. cooperative) under different network conditions [31, 32], to motivate nodes to act as communication relays [33, 34], and to influence nodes to support QoS-based communications [35]. A related survey is available in [36], which discusses several mechanisms to enforce cooperation. These mechanisms are based on punishment, detection of incorrect behavior, and mobile social networking.

Further models to enforce cooperation within a system are as follows: (i) hierarchical model [37–39]; (ii) evolutionary model [40]; (iii) cluster-based model [41]; and (iv) potential game model [42, 43]. In addition to these games, there is a mechanism design (or reverse GT) solution normally designated as auction model [44, 45], which finds the optimum system status with a convergence time lower than that of a theoretical game [46]. Alternatively to the previous mechanisms that are based on (reverse) GT, [47] proposes an incentive mechanism based on both the anchoring effect and loss aversion of Behavioral Economics to stimulate data offloading in IoT use cases. The anchoring effect can be particularly useful, in the start of model game, when the players have not yet learned more suitable choices. In this way, the players are initially attracted to select a choice that optimizes the system operation (e.g. enforce nodes to perform data offloading across the existing edge computational resources, considering also the energy consumption/availability in each node).

The authors of [48] propose a virtualized architecture (based on NFV/VNF) and dynamic control (based on SDN). They deploy, at the SDN controller, a centralized non-cooperative incomplete information game. This enables the SDN controller to decide how the virtual (VNF) sensors are organized in clusters and to identify the more suitable sleep mode for each sensor. The final aim is to extend the lifetime of a software-defined CPS. Our current work is similar to [48] except the latter is concerned with energy efficiency and the former is towards the more efficient coordination among virtualized agents for supporting the CPS resilience in a more generic way. In addition [49], is about a software-defined solution but without NFV. The authors of [50] revise the literature on software-based (i.e. SDN/NFV) proposals to manage and control IoT use cases. In addition [51], proposes a taxonomy of the evolution of the NFV/SDN relationship. Further, [52] reviews the literature on emerging NFV and SDN mechanisms for IoT-based scenarios but mainly focused on security and not addressing the resilience feature.

The next section debates the design for a software-defined resilient CPS. It also discusses two design options to orchestrate agents running over the SDN controller. The first option offers a short-term reactive agent orchestration, and the second one a long-term proactive agent orchestration.

3 Design of a programmable hierarchical architecture for resilient CPS

This section presents and discusses the design of a CPS to enhance this with extra capabilities to detect, absorb and recover, and adapt against threats against the normal

Table 1 Hierarchical architecture of a software-defined resilient cyber-physical system [18]

Layer	Plane	Domain	CPS Activity [53]	Goals	Tools
4	Intelligent management	Inter/Intra	Adapt	Reasoning, orchestration, full abstraction, adjust management policies or intents	NFV, SDN, GT, Intent Engine, ML/AI
3	Control	Intra	Adapt, recover	Partial abstraction, topology, traffic	Software-defined controller with link layer discovery, forwarding, and feedback loop
2	Switching	Edge	Detect, absorb, recover	Decision about next link decision, traffic mirroring, discard packet	Openflow rules in local device tables, queues
1	Physical communications	IoT	Detect, absorb	Accept or discard received message	Interface chip programming

operation of each CPS [53]. We also debate event-triggered (i.e. reactive) (Sub-Sect. 3.1) and data-triggered (i.e. proactive) (Sub-Sect. 3.2) management mechanisms among the several CPS entities towards the resilient operation of that CPS.

3.1 Event-triggered management mechanism

The current sub-section presents some design aspects that are important to consider in an event-triggered Software-Defined resilient CPS. Table 1 presents a four-layered hierarchical architecture [18], which can detect, absorb and recover, and adapt to threats made against CPSs [53]. The current system architecture is formed by management entities that immediately reacts to a relevant system event by executing a management action on the system. In this way, we can classify this as a short-term reactive management solution. Further details on this architecture are available in [18].

The next sub-section presents the basic design of a proactive software-defined resilient CPS management mechanism.

3.2 Data-triggered management mechanism

This sub-section briefly debates how data analysis can also proactively influence the CPS operation in a longer time perspective than the other design discussed in Sub-Sect. 3.1. This occurs because the current system architecture is formed by management entities that need to observe the system operating during some time interval to learn about the more convenient behavior they need to adopt. In this way, we can classify this as a long-term management solution Fig. 2 visualizes the CPS flowchart, showing the major functional phases of gathering data about the CPS operation (status), analyzing data, selecting a management decision, and applying the management decision on the CPS. After this iteration, more CPS data is gathered again, and the previous functional phases are repeated. We assume that data analysis can be performed using a machine learning algorithm to boost the system management [54]. In addition, the management decision of this data model should be conveniently matched with the event-triggered management decision of the agent discussed in Sub-Sect. 3.1. The orchestration among the two management methodologies (reactive vs proactive) can be made using a Blockchain solution [55–57], using a suitable consensus algorithm. Consensus algorithms, such as Kalman-based distributed algorithms [58], can provide interesting distributed functionalities of both filtering the menaces and manage CPSs to mitigate them (or even avoid them in the future). In this way, important network functions, e.g. firewall or Intrusion Detection/Prevention or honeypots, can be deployed pervasively within large networking edge domains, embedding a considerable number of sensors, actuators, or data aggregators. The authors of [58] discuss key recent results in the field of industrial CPSs modeled by differential dynamic equations, and they further discuss what issues should be addressed. These issues are analyzed from three distinct aspects: distributed filtering, distributed control and, distributed security control and filtering.

Data-driven proactive management will be essentially supported by ML/AI techniques. These techniques, once deployed in future networked systems, should offer a new range of networking-based services such as smart routing in networks with a cross-layer design [59], task offloading and resource allocation [60], optimized operation of next-generation mobile networks [61], distributed storage and computation at the network edge [62], and accurate localization estimation of mobile robots

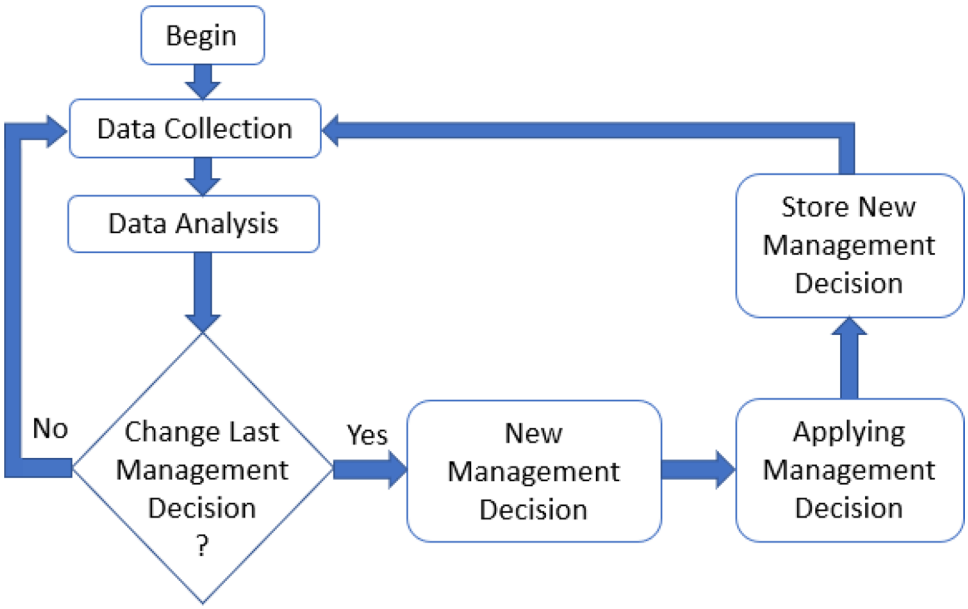

Fig. 2 Data-triggered Management Model of a Cyber-Physical System

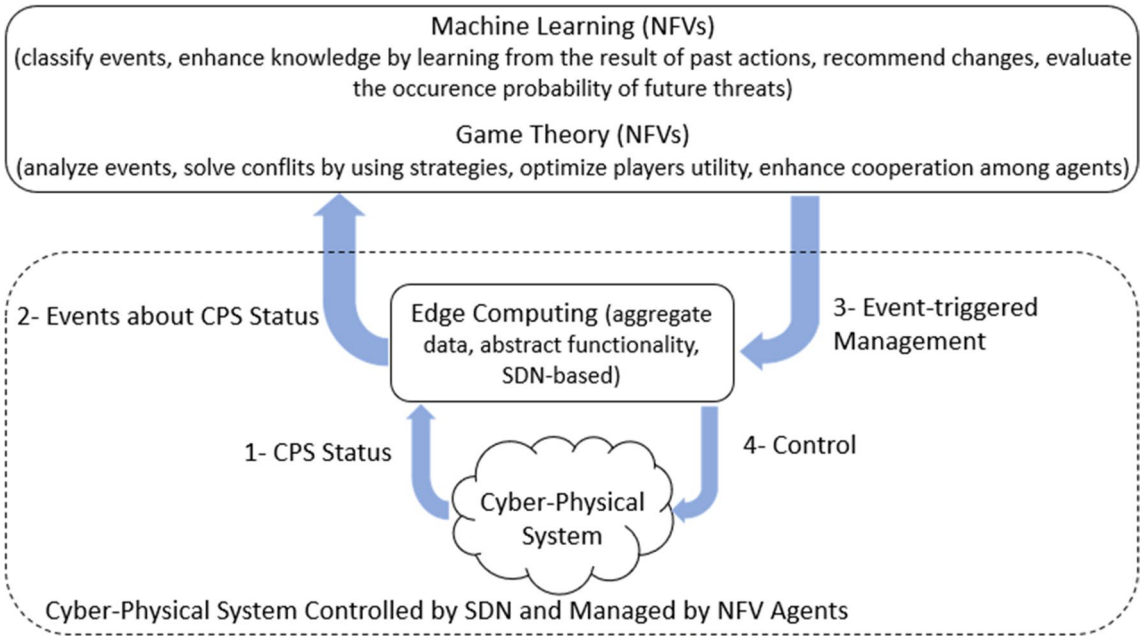

Fig. 3 Reactive system functional blocks with monitor, classify, manage, and control phases

[63]. In parallel with this expected network evolution, novel challenges such as privacy, e.g. in smart contracts [64], or IoT data trustfulness [65] should be successfully guaranteed.

The next section debates the modeling of a proposal to manage a software-defined resilient CPS in a reactive way by each agent.

4 Implementation of a programmable solution for managing resilient CPS

We discuss here the deployment of a programmable proposal to manage a resilient CPS in a reactive way. This solution has a four-layered design (see Table 1). In addition, Fig. 3 presents the key functional blocks of the system under investigation. Analyzing this, one can conclude that the CPS status is being supervised in a periodic way by the SDN controller via a Southbound API protocol such as OpenFlow (see Fig. 3, message 1). Then, the SDN controller, acting as an intermediary, exchanges REST messages via Northbound API with the topmost level system VNF agents (see Fig. 3, message 2). Using these messages, the SDN controller reports status events associated with the CPS operation. These events are analyzed, classified and processed by top-level VNF agents running distinct algorithms (e.g. GT-based, ML-based). At this layer, we expect there to be some coordination mechanisms (e.g. consensus-based) among the distributed agents to guarantee that the CPS is managed in a coherent and efficient way. Subsequently, the final management decision is transferred to the SDN controller (see message 3, Fig. 3). Finally, the SDN controller converts the received management decision into flow rules that control the CPS's physical infrastructure, also commonly referred to as the CPS data plane (see message 4, Fig. 3).

An example of agent processing represented in Fig. 3 at the top-layer, and shown in Table II, it is now briefly explained. This agent estimates the system status from received event messages. The system status is evaluated as the ratio between the *Quantity_good_events* and the *Quantity_total_events*, both collected in a periodic way. There is also the estimator S_n, which is the system status at instant "n". This agent system status estimator with memory (i.e. configurable parameter $\alpha \in [0, 1]$) enables that agent to identify in the best way possible an eventual system anomaly and, after that, to react in a cooperative way to that issue. This means that the recover or adapt algorithm is executed by a specific agent if that agent decides to cooperate and if that choice has been randomly sorted out by the same agent – like tossing a coin. In addition, all the previous goals should be achieved by minimizing the usage of (heterogeneous) system resources (e.g. energy, bandwidth). Alternatively, the agent can selfishly select the 'defect' strategy. As the players select their strategies to optimize the system status, they then verify how the system behaves by evaluating the subsequent value for the local estimator of the system status, and the local processing in each agent is repeated as already explained. In parallel, the global system management is hopefully enhanced, increasing its robustness against any outcoming menace.

5 Analytic study of a CPS aimed at resilience enhancement

This section studies a CPS that is managed by a set of distributed agents. Among these agents, some of them could assume incorrect behavior, which needs to be detected and retaliated against; otherwise, the efficient and resilient operation of the CPS could be jeopardized. For ensuring the CPS' global performance and resilience, we initially analyze a non-cooperative model among distributed agents with an External Retaliation Mechanism, which is controlled by a Model Discounted Factor. Then, we carry on an evolution study among the independent agents, which can select, among several options, a retaliation strategy against undesired actions observed from others, aiming to fulfil a global system objective (e.g. resilience).

In this first part, we present and debate some analytic results of a non-cooperative model enhanced by an external mechanism that reactively enforces cooperation among players through infinitely iterated repetitions of the model algorithm which is running in each player. We have selected a non-cooperative model to the detriment of others, namely Stackelberg or cooperative, because each one of these alternatives has important limitations. In fact, the first alternative, i.e. the Stackelberg game, has a centralized operation based on the master player. This master node takes, at the beginning of each iteration, the first management decision, followed by individual decisions made in each follower node that has previously observed the initial master decision. The Stackelberg model presents the classical problems of a centralized design: low scalability, no system operation if the master node fails, or a high probability of the master node being subjected to cyber-attacks.

The second possible alternative based on a cooperative model has the drawback of inducing a very high network overhead. This network overhead is due to the high amount of signaling traffic used in the formation and maintenance of clusters, essentially in a large and high-complexity scenario such as the emerging scenario of vehicular networks in operation within a very busy city.

Considering a non-cooperative model, we avoid the limitations explained in the previous paragraphs, but we should be aware that some players could assume decisions, which in turn could penalize the system's global performance. Assuming this, and to assure a global system optimization, we should guarantee that most of the distributed players become coordinated together, towards the fulfilment of a common system goal. In this way, the cooperation among players is very important for achieving reliable system operation with a limited set of resources.

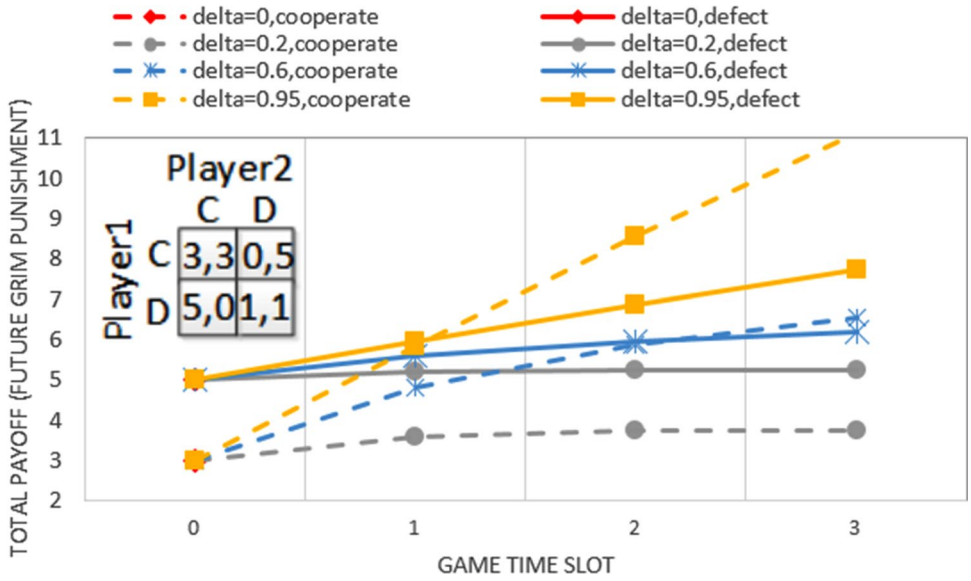

Fig. 4 Total Payoff Trend for a specific player involved in an Infinitely Repeated PD Game with a Grim Punishment Mechanism (Tit for Tat) and Diverse Discounted Factors

To support the next debate, we consider the well-known infinitely repeated Prisoner's Dilemma (PD) game between *N* non-cooperative agents. These *N* players are functional entities of a CPS and IoT system, e.g. containers, or specialized VNF agents located at the topmost layer of the software-defined resilient CPS. By specialized agents we mean that, as the system overlaps a specific threshold, each system agent detects it and cooperatively reacts, selecting either 'absorb' or 'adapt to' the problem. Alternatively, the agent can be selfish by doing nothing to mitigate the problem.

Next, we analyze a model involving two ($N=2$) topmost layer management agents that can either cooperate or defect. In the current game, the discounted factor combined with a mechanism that is triggered by a player´s defection can enforce cooperation throughout players. The discounted factor ($<=1$) multiplies the payoffs of the current stage, meaning that in future game stages the payoffs of previous rounds have less relevance. In this way, each player gets an accumulated reward during all the game iterations in which that player was involved.

Figure 4 shows the payoff matrix of an infinitely repeated PD game as well as the total (per player accumulated) payoff along the initial four runs of the game, considering distinct values for the discounted factor (i.e. delta = {0,0.2,0.6,0.95}). A Grim Trigger methodology is applied to a player that defects. Two distinct strategies are analyzed. In the first situation, both players cooperate, being rewarded with the social optimum payoff of 3 in every stage of the game, as shown in Eq. (1). In the second situation, one player defects in the first stage to increase its initial payoff from 3 to 5. Nevertheless, the other player at the second stage retaliates against the former defecting player, also defecting. Consequently, both players get a payoff of 1, as shown in Eq. (2), after the initial stage.

$$Coop = 3 + \delta.3 + \delta^2.3 + \cdots = \frac{3}{1-\delta} \tag{1}$$

$$Def = 5 + \delta.1 + \delta^2.1 + \cdots = 5 + \frac{\delta}{1-\delta} \tag{2}$$

$$\frac{3}{1-\delta} \geq 5 + \frac{\delta}{1-\delta} \Leftrightarrow \delta \geq 0.5 \tag{3}$$

The expression (3) evaluates the minimum value (i.e. 0.5) for the discounted factor (delta) to reflect in future a strong enough threat (in terms of payoff decrease) to a deviating player. Comparing the payoff trends of the two cases we have discussed in the previous paragraph, one can conclude for delta values of 0 (i.e. the game has only a single stage) and 0.2, which are both lower than 0.5, then the more convenient strategy for both players is always to defect (see Fig. 4). The mutual defection occurs because the model gives the players solid evidence that they are playing the ultimate round of the game. So, the players are normally tempted to defect as they cannot be punished in the future. Alternatively, analyzing from Fig. 4 the trends associated with the delta values of 0.6 and 0.95, which are both higher than 0.5, one can conclude that in the initial stages both players are tempted to defect; but after a threshold stage of the game is passed, both players should always cooperate in their best interest. This threshold stage depends on the delta value (see Fig. 4). In fact, as the delta value

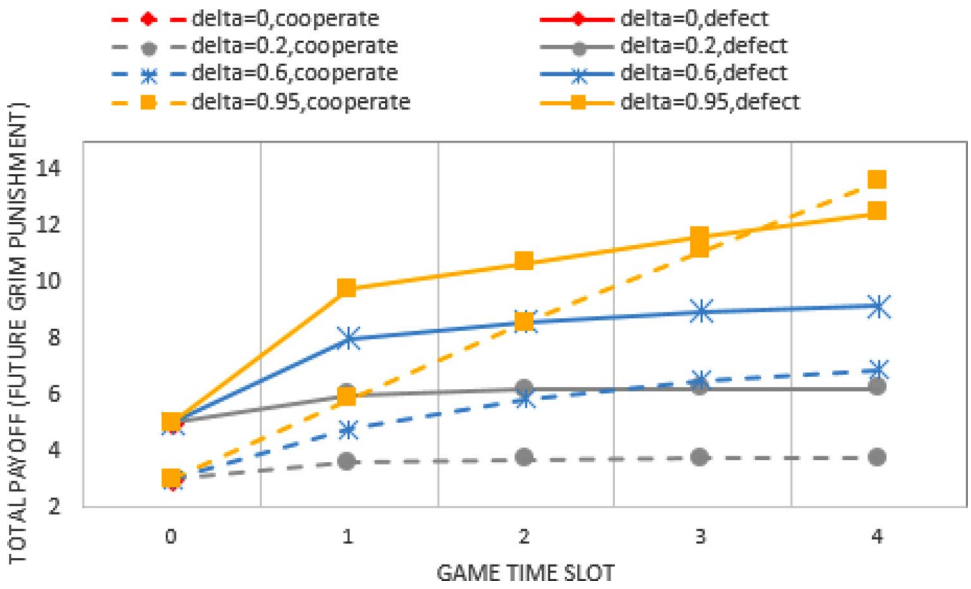

Fig. 5 Total Payoff Trend for a specific player involved in an Infinitely Repeated PD Game with a Grim Punishment Mechanism (Slow Tit for Two Tats) and Diverse Discounted Factors

increases towards one that means the player (with that perspective of the game) learns it is better to cooperate instead defecting faster, i.e. after fewer stages counted from the game's start.

The opposite happens if for the same game the strategy is changed from Tit for Tat (Fig. 4) to Slow Tit for Two Tats (Fig. 5). From Fig. 5 it is evident that the need to cooperate occurs in later stages of the game when compared with the trend of Fig. 4. The last difference in behavior occurs because Tit for Two Tats is a forgiving strategy by which a player only defects after the opponent has defected twice in a row. This behavior is fairer than Tit for Tat in scenarios where the player, due to a network communication error or any limitation imposed by other system operational constrain, erroneously perceived the previous opponent's choice.

For validating the key conclusions extracted from the previous analytical comparison made between the two cooperative strategies, we have also performed some additional simulations to study how the distribution of the two studied types of cooperative behavior evolve along the time, considering a total player population of constant size. In this way,Fig. 6 shows the evolution of a population composed by the two types of players of our study, during one thousand rounds. The Moran process was used to keep the population size always at a constant value of one hundred players. For simulating that situation, we have used the Axelrod Python library.[1] The winning management strategy was Slow Tit for Two Tats, suggesting Tit for Tat has a lower fitness function than the former one, confirming our analytical conclusions.

There are still a considerable open research challenges in discounted repeated games, such as: (i) coping with incomplete available information; (ii) controlling defectors; (iii) considering an individual delta for each player; (iv) triggering punishment only during a limited set of stages after an incorrect behavior; and finally (v) studying scenarios where a serious system threat stops the system's operation and the game. Also, the authors of [66] investigate the more suitable values for the parameters of a repeated game to guarantee cooperation among the majority of the players is still guaranteed in spite of some uncertainty about the strategy selection. Another recent contribution [67] suggests the usage of statistical physics to understand human cooperation better. We think that this research direction is very interesting, by transposing it to an investigation on how to design and deploy systems used by diverse players, which need to be more cooperative and fairer in the mutual interaction within each system. Further, the cooperation and fairness should be obtained not by centralized policies that can often be either unoptimized or be easily deceived by (some) players, but simply by the coordinated effort of most players that can create a high level of collective intelligence.

In this section we have used static rewards for the strategies each player is able to select. It is also possible to analyze a more dynamic game, where the reward of each player is a function of the estimator S_n used by the algorithm of Table 2.

[1] https://github.com/Axelrod-Python/Axelrod (Verified in 2019/04/21).

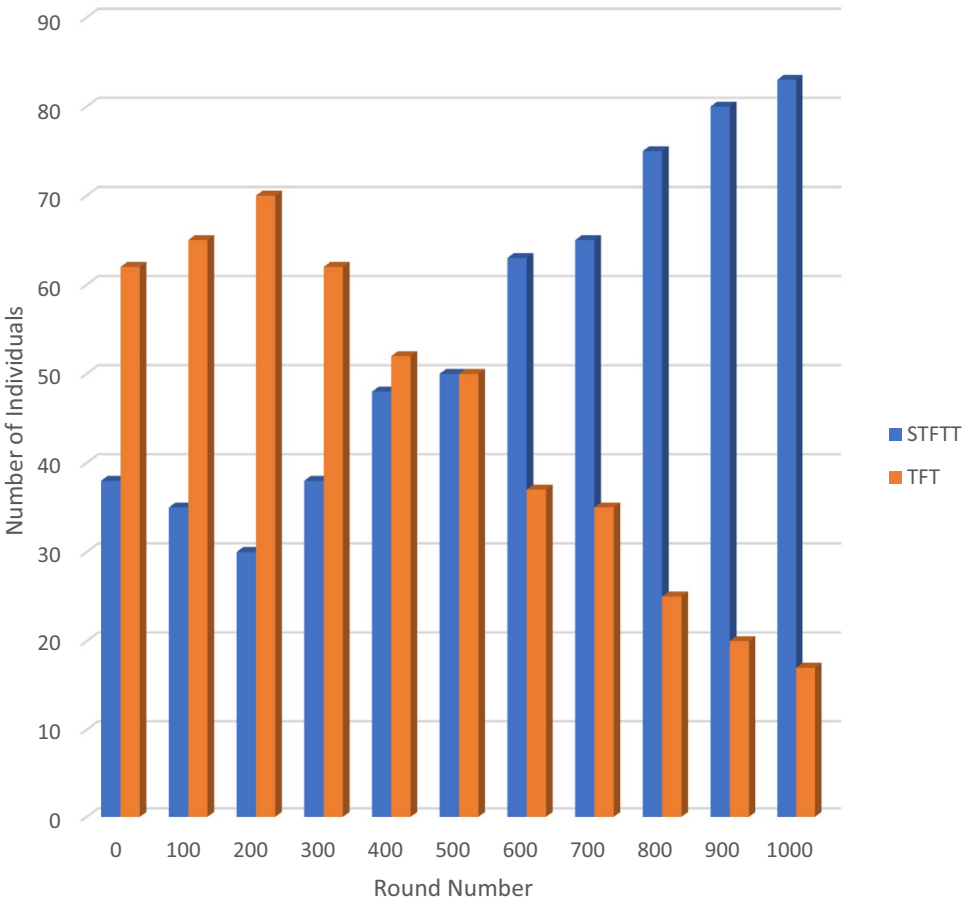

Fig. 6 Distribution of the Two Studied Types of Cooperative Behavior in a Constant Population of 100 Players during 1,000 Rounds (*STFTT* Slow Tit for Two Tats; *TFT* Tit For Tat)

Table 2 Agent Event-Triggered Management Algorithm

$S_0 = 1; \alpha = 0.8;$ n = 1
While True do
Collect, analyze, and classify CPS events occurred within last time slot
$S = \frac{Quantity\_good\_events\_within\_last\_time\_slot}{Quantity\_total\_events\_within\_last\_time\_slot}$
$S_n = S_{n-1} * \alpha + S * (1 - \alpha)$
if $S_n > threshold$ ***then***
CPS system is ok; do nothing different from last action
else
CPS system is not ok; play the cooperate / defect game
end if
n = *n* + 1
end for

6 The main results of our work

The main contributions of this work, including its major analytic evaluation results, are summarized as follows: (i) it presents the perspective that upcoming services for resilient CPSs require the implementation flexibility of SDN and NFV, theoretical modeling, and machine learning; (ii) it discusses both short and long term CPS orchestration mechanisms among the agents, towards the fulfilment of global system goals; (iii) it describes a distributed algorithm to implement the proposal for resilient CPSs; (iv) it analyzes results of a non-cooperative model, enhanced by an external mechanism, that reactively enforces cooperation among players through iterations of the model algorithm running in each agent; (v) it compares cooperation strategies in an evolution scenario with two distinct agent types belonging to a population with a global constant number of agents across the diverse generations. We conclude that a higher-level strategy by which an initial cooperative agent defects only after the opponent has defected twice in a row seems a more promising policy than other concurrent

strategies where the initial cooperative agent reacts more promptly to defective behavior observed in others.

7 Some assumptions and limitations of our work

We finalize this section with some assumptions and limitations of our current work, projecting several possible future work directions. Our theoretical model assumes the distributed agents act as rational players, and they should be coordinated to support cooperation among themselves towards the resilient operation of CPSs. Nevertheless, in more realistic scenarios, the previous assumptions could be difficult to attain. In fact, the agents could be non-rational players or even the extra control and signaling traffic could incur non-negligible overheads (e.g. the cost of incentivized cooperation) on the network infrastructure. Consequently, when we are interested to enable cooperation among the agents, it is fundamental to infer what are the system gains from that cooperation—and balancing these gains against the associated cost. On one hand, to accommodate the non-rationality of players we pointed out the use of probabilistic tools, such as Bayesian prediction in theoretical games [68]. On the other hand, to infer correctly the usefulness of establishing (or not) the cooperation among agents, some machine learning techniques [16] can be used to deploy a smart adaptation of the level of cooperation necessary to manage the CPS's available resources as efficiently as possible. Other interesting aspects for future study include addressing the problem of maintaining a resilient CPS in the presence of system agents infected such that that they assume non-cooperative decisions to undermine the CPS operation. To avoid this, new management solutions should be investigated to detect and remove those malicious agents as quickly as possible from the CPS's operational domain.

Communication networks form a crucial part of a CPS. Consequently, it is very important to guarantee their resilient and stable operation in the presence of cascading failures / attacks through the entire CPS [69]. Aligned with this goal, previous work [70] has investigated a network formation game that incorporates an adversarial attack, as well as immunization or protection against that attack at some additional cost. Nevertheless, they assume the attack spreads deterministically. However, in real-world scenarios, e.g. the diffusion of contagious disease over the network of people, this is not deterministic. So, novel complementary research is needed, for cases when the network threat is propagated over the network topology not only in a probabilistic static way [71], but in a variably probabilistic way or even assuming imperfect (i.e. parts of) system immunization against that threat.

8 Conclusion and future work

Cyber-Physical Systems (CPSs) are increasingly deployed in critical areas of our society, but they are subject to new challenges to their optimum and reliable operation, which strongly suggests the need for innovative management strategies to achieve resilience in these systems. To this end, we have outlined in this paper a programmable (SDN- and NFV-based) solution using distributed Virtual Network Function (VNF) modules. These VNF modules take orchestrated management decisions among themselves to guarantee a resilient operation of the CPSs. In the paper, we design, model and analyze two different strategies to impose cooperation among the VNFs.

Future work will involve studying data-triggered management models for building programmable and flexible resilient CPSs [72]. In addition, the dynamic movement of processes and data in (edge) cloud-based systems may compromise their resilience, unless steps are taken to recognize the problem and modify anomaly detection components appropriately [73]. Further investigation in complex networking environments is needed by using distributed consensus mechanisms among management agents that incentivize honest behavior towards a well-identified system operation goal, with low complexity and high fault-tolerance [74].

Acknowledgements Jose Moura acknowledges the support given by Instituto de Telecomunicações, Lisbon, Portugal. David Hutchison is grateful to colleagues in EU COST Action RECODIS (CA15127) for discussions about the resilience of communication systems.

Funding The work of Jose Moura is funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/EEA/50008/2020.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Da Xu L, Duan L (2019) Big data for cyber physical systems in industry 4.0: a survey. Enterp Inf Syst 13(2):148–169. https://doi.org/10.1016/j.ijepes.2017.12.020.
2. Sun CC, Hahn A, Liu CC (2018) Cyber security of a power grid: state-of-the-art. Int J Electrical Power Energy Syst. https://doi.org/10.1016/j.ijepes.2017.12.020
3. Eder-Neuhauser P, Zseby T, Fabini J (2016) Resilience and security: a qualitative survey of urban smart grid architectures. IEEE Access 4:839–848. https://doi.org/10.1109/ACCESS.2016.2531279

4. Kolokotsa D (2016) The role of smart grids in the building sector. Energy Build 116:703–708. https://doi.org/10.1016/J.ENBUILD.2015.12.033.
5. Kumar A, Singh A, Kumar A, Singh MK, Mahanta P, Mukhopadhyay SC (2018) Sensing technologies for monitoring intelligent buildings: a review. IEEE Sens J 18(12):4847–4860. https://doi.org/10.1109/JSEN.2018.2829268.
6. Agiwal M, Roy A, Saxena N (2016) Next generation 5G wireless networks: a comprehensive survey. IEEE Commun Surv Tutorials 18(3):1617–1655. https://doi.org/10.1109/COMST.2016.2532458.
7. Xu Y, Wang J, Wu Q, Du Z, Shen L, Anpalagan A (2015) A game-theoretic perspective on self-organizing optimization for cognitive small cells. IEEE Commun Mag 53(7):100–108. https://doi.org/10.1109/MCOM.2015.7158272
8. Boyi Xu, Li Da Xu, Hongming Cai, Cheng Xie, Jingyuan Hu, Fenglin Bu (2014) Ubiquitous data accessing method in IoT-based information system for emergency medical services. IEEE Trans Ind Informatics 10(2):1578–1586. https://doi.org/10.1109/TII.2014.2306382.
9. Mutlag AA, Abd Ghani MK, Arunkumar N, Mohammed MA, Mohd O (2019) Enabling technologies for fog computing in healthcare IoT systems. Futur Gener Comput Syst 90: 62–78. https://doi.org/10.1016/J.FUTURE.2018.07.049.
10. Ordonez-Garcia A, Siller M, Begovich O (2017) IoT architecture for urban agronomy and precision applications. In: 2017 IEEE International autumn meeting on power, electronics and computing (ROPEC), pp 1–4. https://doi.org/10.1109/ROPEC.2017.8261582.
11. Gómez-Chabla R, Real-Avilés K, Morán C, Grijalva P, Recalde T (2019) IoT applications in agriculture: a systematic literature review. In: 2nd International conference on ICTs in agronomy and environment, pp 68–76. https://doi.org/10.1007/978-3-030-10728-4_8.
12. Mu M et al (2016) (2016) A scalable user fairness model for adaptive video streaming over SDN-assisted future networks. IEEE J Sel Areas Commun 34(8):2168–2184. https://doi.org/10.1109/JSAC.2016.2577318
13. Barakabitze AA, Ahmad A, Mijumbi R, Hines A (2020) 5G network slicing using SDN and NFV: a survey of taxonomy, architectures and future challenges. Comput Netw 167:106984. https://doi.org/10.1016/j.comnet.2019.106984
14. Morabito R, Cozzolino V, Ding AY, Beijar N, Ott J (2018)Consolidate IoT edge computing with lightweight virtualization. IEEE Netw 32(1):102–111. https://doi.org/10.1109/MNET.2018.1700175
15. Moura J, Hutchison D (2019) Game theory for multi-access edge computing: survey, use cases, and future trends. IEEE Commun Surv Tutorials 21(1):260–288. https://doi.org/10.1109/COMST.2018.2863030
16. Xie J et al (2019) A survey of machine learning techniques applied to software defined networking (SDN): research issues and challenges. IEEE Commun Surv Tutorials 21(1):393–430. https://doi.org/10.1109/COMST.2018.2866942
17. Sun N, Zhang J, Rimba P, Gao S, Xiang Y, Zhang LY (2018) Data-driven cybersecurity incident prediction: a survey. IEEE communications surveys & tutorials, p 1. https://doi.org/10.1109/COMST.2018.2885561.
18. Moura J, Hutchison D (2020) Fog computing systems: state of the art, research issues and future trends, with a focus on resilience, pp 1–38. Available: https://arxiv.org/abs/1908.05077.
19. Park P, Di Marco P, Johansson KH (2017) Cross-layer optimization for industrial control applications using wireless sensor and actuator mesh networks. IEEE Trans Ind Electron 64(4):3250–3259. https://doi.org/10.1109/TIE.2016.2631530
20. Cui L, Tso FP, Jia W (2020) Federated srvice chaining: architecture and challenges. IEEE Commun Mag 58(3):47–53. https://doi.org/10.1109/MCOM.001.1900627
21. Vaquero LM, Cuadrado F, Elkhatib Y, Bernal-Bernabe J, Srirama SN, Zhani MF (2019) Research challenges in nextgen service orchestration. Futur Gener Comput Syst 90:20–38. https://doi.org/10.1016/j.future.2018.07.039
22. Moura J, Hutchison D (2020) Resilient cyber-physical systems: Using NFV Orchestration. https://arxiv.org/abs/2003.12401v2. Accessed May 06, 2020.
23. Hutchison D, Sterbenz JPG (2018) Architecture and design for resilient networked systems. Comput Commun 131:13–21. https://doi.org/10.1016/j.comcom.2018.07.028
24. Rotsos C et al (2017) Network service orchestration standardization: a technology survey. Comput Stand Interfaces 54:203–215. https://doi.org/10.1016/J.CSI.2016.12.006
25. Smith P, Schaeffer-Filho A, Hutchison D, Mauthe A (2014) Management patterns: SDN-enabled network resilience management. In: IEEE/IFIP NOMS 2014—IEEE/IFIP network operations and management symposium: management in a software defined world, pp 1–9, https://doi.org/10.1109/NOMS.2014.6838323.
26. Moura J, Edwards C (2016) Efficient access of mobile flows to heterogeneous networks under flash crowds. Comput Netw 107(2):163–177. https://doi.org/10.1016/j.comnet.2016.04.010
27. Yeadon N, Mauthe A, García F, Hutchison D (1996) QoS filters: addressing the heterogeneity gap. Lect Notes Comput Sci 1045:227–243. https://doi.org/10.1007/3-540-60938-5_16
28. Rass S, Alshawish A, Abid MA, Schauer S, Zhu Q, De Meer H (2017) Physical intrusion games—optimizing surveillance by simulation and game theory. IEEE Access 5:8394–8407. https://doi.org/10.1109/ACCESS.2017.2693425
29. Zhang Y, Pan M, Song L, Dawy Z, Han Z (2017) A survey of contract theory-based incentive mechanism design in wireless networks. IEEE Wirel Commun 24(3):80–85. https://doi.org/10.1109/MWC.2017.1500371WC
30. Yang G, He S, Shi Z, Chen J (2017) Promoting cooperation by the social incentive mechanism in mobile crowdsensing. IEEE Commun Mag 55(3):86–92. https://doi.org/10.1109/MCOM.2017.1600690CM
31. Ding Q, Zeng X, Zhang X, Sung DK (2018) A public goods game theory-based approach to cooperation in VANETs under a high vehicle density condition. IEEE Trans Intell Transp Syst, pp 1–11. https://doi.org/10.1109/TITS.2018.2876237.
32. Shivshankar S, Jamalipour A (2015) An evolutionary game theory-based approach to cooperation in VANETs under different network conditions. IEEE Trans Veh Technol 64(5):2015–2022. https://doi.org/10.1109/TVT.2014.2334655
33. Kapade N (2014) TLC: trust point load balancing method using coalitional game theory for message forwarding in VANET. In: IEEE global conference on wireless computing & networking (GCWCN), pp 160–164. https://doi.org/10.1109/GCWCN.2014.7030870
34. Ghorai C, Banerjee I (2018) A robust forwarding node selection mechanism for efficient communication in urban VANETs. Veh Commun 14:109–121. https://doi.org/10.1016/J.VEHCOM.2018.10.003
35. Kadadha M, Otrok H, Barada H, Al-Qutayri M, Al-Hammadi Y (2018) A Stackelberg game for street-centric QoS-OLSR protocol in urban Vehicular Ad Hoc Networks. Veh Commun 13:64–77. https://doi.org/10.1016/J.VEHCOM.2018.05.003
36. Hua LC, Anisi MH, Yee PL, Alam M (2017) Social networking-based cooperation mechanisms in vehicular ad-hoc network—a survey. Veh Commun 10:57–73. https://doi.org/10.1016/J.VEHCOM.2017.11.001

37. Zhang H, Ding W, Song J, Han Z (2016) A hierarchical game approach for visible light communication and D2D heterogeneous network. In: 2016 IEEE global communications conference (GLOBECOM), pp 1–6. https://doi.org/10.1109/GLOCOM.2016.7841505.
38. Zhou Z, Tan L, Gu B, Zhang Y, Wu J (2018) Bandwidth slicing in software-defined 5G: a Stackelberg game approach. IEEE Veh Technol Mag 13(2):102–109. https://doi.org/10.1109/MVT.2018.2814022
39. Li X, Zhang C, Gu B, Yamori K, Tanaka Y (2019) Optimal pricing and service selection in the mobile cloud architectures. IEEE Access 7:43564–43572. https://doi.org/10.1109/ACCESS.2019.2908223
40. Cheng L, Yu T (2018) Nash equilibrium-based asymptotic stability analysis of multi-group asymmetric evolutionary games in typical scenario of electricity market. IEEE Access 6:32064–32086. https://doi.org/10.1109/ACCESS.2018.2842469
41. Li S, Fei F, Ruihan D, Yu S, Dou W (2016) A dynamic pricing method for carpooling service based on coalitional game analysis. In: 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), pp 78–85. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0022.
42. Zhang N, Zhang S, Zheng J, Fang X, Mark JW, Shen X (2017) QoE driven decentralized spectrum sharing in 5G networks: potential game approach. IEEE Trans Veh Technol 66(9):7797–7808. https://doi.org/10.1109/TVT.2017.2682236
43. Zhao X, Li L, Geng S, Zhang H, Ma Y (2019) A link-based variable probability learning approach for partially overlapping channels assignment on multi-radio multi-channel wireless mesh information-centric IoT networks. IEEE Access 7:45137–45145. https://doi.org/10.1109/ACCESS.2019.2908872
44. Chen I, Wu J, Zhang X-X, Zhou G (2018) TARCO: two-Stage auction for D2D relay aided computation resource allocation in HetNet. IEEE transactions on services computing, p 1. https://doi.org/10.1109/TSC.2018.2792024.
45. Zhou Z, Liao H, Gu B, Huq KMS, Mumtaz S, Rodriguez J (2018) Robust mobile crowd sensing: when deep learning meets edge computing. IEEE Netw 32(4):54–60. https://doi.org/10.1109/MNET.2018.1700442
46. Luo T, Kanhere SS, Huang J, Das SK, Wu F (2017) Sustainable incentives for mobile crowdsensing: auctions, lotteries, and trust and reputation systems. IEEE Commun Mag 55(3):68–74. https://doi.org/10.1109/MCOM.2017.1600746CM
47. Liu J, Gao W, Li D, Huang S, Liu H (2019) An incentive mechanism combined with anchoring effect and loss aversion to stimulate data offloading in IoT. IEEE Internet Things J 6(3):4491–4511. https://doi.org/10.1109/JIOT.2018.2883452
48. Wu J, Luo S, Wang S, Wang H (2019) NLES: a novel lifetime extension scheme for safety-critical cyber-physical systems using SDN and NFV IEEE Internet Things J 6(2):2463–2475. https://doi.org/10.1109/JIOT.2018.2870294
49. Kathiravelu P, Veiga L (2017) SD-CPS: taming the challenges of cyber-physical systems with a software-defined approach. In: Fourth international conference on software defined systems (SDS), pp 6–13. https://doi.org/10.1109/SDS.2017.7939133
50. Bizanis N, Kuipers FA (2016) SDN and virtualization solutions for the internet of things: a survey. IEEE Access 4:5591–5606. https://doi.org/10.1109/ACCESS.2016.2607786
51. Matias J, Garay J, Toledo N, Unzilla J, Jacob E (2015) Toward an SDN-enabled NFV architecture. IEEE Commun Mag 53(4):187–193. https://doi.org/10.1109/MCOM.2015.7081093
52. Farris I, Taleb T, Khettab Y, Song J (2019) A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Commun Surv Tutorials 21(1):812–837. https://doi.org/10.1109/COMST.2018.2862350
53. Connelly EB, Allen CR, Hatfield K, Palma-Oliveira JM, Woods DD, Linkov I (2017) Features of resilience. Environ Syst Decis 37(1):46–50. https://doi.org/10.1007/s10669-017-9634-9
54. Frohlich P, Gelenbe E, Nowak MP (2020) Smart SDN management of fog services. TechRxiv-11640162, pp. 1–6. https://doi.org/10.36227/techrxiv.11640162.v1.
55. Dai HN, Zheng Z, Zhang Y (2019) Blockchain for internet of things: a survey. IEEE Internet Things J 6(5):8076–8094. https://doi.org/10.1109/JIOT.2019.2920987
56. Lo SK et al (2019) Analysis of blockchain solutions for IoT: a systematic literature review. IEEE Access 7:58822–58835. https://doi.org/10.1109/ACCESS.2019.2914675
57. Sharma PK, Chen M-Y, Park JH (2018) A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access 6:115–124. https://doi.org/10.1109/ACCESS.2017.2757955
58. Ding D, Han Q-L, Wang Z, Ge X (2019) A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Trans Ind Informatics 15(5):2483–2499. https://doi.org/10.1109/TII.2019.2905295
59. Medhat Salih Q, Rahman MA, Al-Turjman F, Azmi ZRM (2020) Smart routing management framework exploiting dynamic data resources of cross-layer design and machine learning approaches for mobile cognitive radio networks: a survey. IEEE Access, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp 67835–67867. https://doi.org/10.1109/ACCESS.2020.2986369.
60. Alfakih T, Hassan MM, Gumaei A, Savaglio C, Fortino G (2020) Task offloading and resource allocation for mobile edge computing by deep reinforcement learning based on SARSA. IEEE Access 8:54074–54084. https://doi.org/10.1109/ACCESS.2020.2981434
61. Ma B, Guo W, Zhang J (2020) A survey of online data-driven proactive 5G network optimisation using machine learning. IEEE Access, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp 35606–35637. https://doi.org/10.1109/ACCESS.2020.2975004.
62. Zhang W, Chen X, Liu Y, Xi Q (2020) A distributed storage and computation k-nearest neighbor algorithm based cloud-edge computing for cyber-physical-social systems. IEEE Access 8:50118–50130. https://doi.org/10.1109/ACCESS.2020.2974764
63. Zhu Z, Wen Y, Zhang Z, Yan Z, Huang S, Xu X (2020) Accurate position estimation of mobile robot based on cyber-physical-social systems (CPSS). IEEE Access 8:56359–56370. https://doi.org/10.1109/ACCESS.2020.2980558
64. Gupta R, Tanwar S, Al-Turjman F, Italiya P, Nauman A, Kim SW (2020) Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. IEEE Access 8:24746–24772. https://doi.org/10.1109/ACCESS.2020.2970576
65. Fortino G, Fotia L, Messina F, Rosaci D, Sarné GML (2020) Trust and reputation in the internet of things: state-of-the-art and research challenges. IEEE Access 8:60117–60125. https://doi.org/10.1109/ACCESS.2020.2982318
66. Bó PD, Fréchette GR (2018) On the determinants of cooperation in infinitely repeated games: a survey. J Econ Lit 56(1):60–114. https://doi.org/10.1257/jel.20160980
67. Perc M, Jordan JJ, Rand DG, Wang Z, Boccaletti S, Szolnoki A (2017) Statistical physics of human cooperation. Physics Reports, vol. 687. Elsevier, Amsterdam, pp 1–51. https://doi.org/10.1016/j.physrep.2017.05.004.
68. Akkarajitsakul K, Hossain E, Niyato D (2011) Distributed resource allocation in wireless networks under uncertainty and application of Bayesian game. IEEE Commun Mag 49(8):120–127. https://doi.org/10.1109/MCOM.2011.5978425

69. Blume L, Easley D, Kleinberg J, Kleinberg R, Tardos É (2013) Network formation in the presence of contagious risk. ACM Trans Econ Comput 1(2):1–20. https://doi.org/10.1145/2465769.2465771
70. Goyal S, Jabbari S, Kearns M, Khanna S, Morgenstern J (2016) Strategic network formation with attack and immunization. In: Lecture notes in computer science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 10123. LNCS, pp 429–443, https://doi.org/10.1007/978-3-662-54110-4_30.
71. Chen Y, Jabbari S, Kearns M, Khanna S, Morgenstern J (2019) Network formation under random attack and probabilistic spread. IJCAI International joint conference on Artificial intelligence, vol 2019, pp 180–186. Accessed: 24 July 2020. Available: https://arxiv.org/abs/1906.00241.
72. Bures T et al (2017) Software engineering for smart cyber-physical systems. ACM SIGSOFT Softw Eng Notes 42(2):19–24. https://doi.org/10.1145/3089649.3089656
73. Shirazi NUH, Simpson S, Marnerides AK, Watson M, Mauthe A, Hutchison D (2014) Assessing the impact of intra-cloud live migration on anomaly detection. In: 2014 IEEE 3rd international conference on cloud networking, CloudNet 2014, pp 52–57, https://doi.org/10.1109/CloudNet.2014.6968968.
74. Wang L, Bai Y, Jiang Q, Leung VCM, Cai W, Li X (2020) Beh-Raft-Chain: a behavior-based fast blockchain protocol for complex networks. IEEE Transactions on Network Science and Engineering, pp 1–1. https://doi.org/10.1109/tnse.2020.2984490.