Trust, Reputation, and Risk in Cyber Physical Systems

Elizabeth Chang, Tharam Dillon

Trust, Reputation, and Risk in Cyber Physical Systems

Elizabeth Chang[1], Tharam Dillon[2]

[1] Chair IFIP WG2.12/12.4 on web semantic
Elizabeth.chang@cbs.curtin.edu.au
[2] Chair IFIP TC12 on Artifical Intelligence Latrobe University,
Digital Ecosystems & Business Intelligence Institute Pty. Ltd, Australia
Tharam.dillon7@gmail.com

Abstract. Cyber Physical Systems (CPS) involve the connections of real world objects into networked information systems including the web. It utilises the framework and architecture for such CPS systems based on the Web of Things previously developed by the authors. This paper discusses the provision of Trust, Reputation and determination of Risk for such CPS systems.

Keywords: Cyber Physical Systems, Trust, Risk, Web of Things, Architecture

1 Introduction

The National Science Foundation (NSF) CPS Summit held in April 2008 [4] defines CPS as "physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core". Researchers from multiple disciplines such as embedded systems and sensor networks have been actively involved in this emerging area.

Our vision of CPS is as follows: networked information systems that are tightly coupled with the physical process and environment through a massive number of geographically distributed devices [1]. As networked information systems, CPS involves computation, human activities, and automated decision making enabled by information and communication technology. More importantly, these computation, human activities and intelligent decisions are aimed at monitoring, controlling and integrating physical processes and environment to support operations and management in the physical world. The scale of such information systems range from micro-level, embedded systems to ultra-large systems of systems. Devices provide the basic interface between the cyber world and the physical one.

The discussions in the NSF Summit [4] can be summarized into eleven scientific and technological challenges for CPS solutions. These

challenges constitute the top requirements for building cyber-physical systems and are listed below.

- Compositionality
- Distributed Sensing, Computation and Control
- Physical Interfaces and Integration
- Human Interfaces and Integration
- Information: From Data to Knowledge
- Modeling and Analysis: Heterogeneity, Scales, Views
- Privacy, Trust, Security
- Robustness, Adaptation, Reconfiguration
- Software
- Verification, Testing and Certification
- Societal Impact

Based on the challenges listed above, a new unified cyber-physical systems foundation that goes beyond current computer mediated systems needs to be developed. We explain how this can be achieved, inline with the challenges to CPS identified by the NSF summit report.

CPS need to stay in constant touch with physical objects. This requires: (1) models that abstract physical objects with varying levels of resolutions, dimensions, and measurement scales, (2) mathematical representation of these models and understanding of algorithmic, asymptotic behavior of these mathematical models, and (3) abstractions that captures the relationships between physical objects and CPS.

Humans have to play an essential role (e.g. influence, perception, monitoring, etc.) in CPS. This requires: (1) seamless integration and adaptation between human scales and physical system scales. (2) support for local contextual actions pertinent to specific users, who are part of the system rather than just being the "users" of the system, (3) new theories on the boundary (e.g. hand-over or switch) between human control and (semi-) automatic control.

Many CPS are aimed at developing useful knowledge from raw data[21]. This requires (1) algorithms for sensor data fusion that also deal with data cleansing, filtering, validation, etc. (2) data stream mining in real-time (3) storage and maintenance of different representations of the same data for efficient and effective (e.g. visualization) information retrieval and knowledge extraction.

CPS needs to deal with massive heterogeneity when integrating components of different natures from different sources. This requires

(1) integration of temporal, eventual, and spatial data defined in significantly different models (asynchronous vs. synchronous) and scales (e.g. discrete vs. continuous), (2) new computation models that characterize dimensions of physical objects such as time (e.g. to meet real-time deadline), location, energy, memory footprint, cost, uncertainty from sensor data, etc., (3) new abstractions and models for cyber-physical control that can deal with - through compensation, feedback processing, verification, etc. - uncertainty that is explicitly represented in the model as a "first-class citizen" in CPS, (4) new theories on "design for imperfection" exhibited by both physical and cyber objects in order to ensure stability, reliability, and predictability of CPS, (5) system evolution in which requirements and constraints are constantly changing and need to be integrated into different views of CPS, and (6) new models for dealing with issues in large-scaled systems such as efficiency trade-offs between local and global, emergent behavior of complex systems, etc.

CPS in general reveal a lot of physical information, create a lot of data concerning security (e.g. new types of attacks), privacy (e.g. location), and trust (e.g. heterogeneous resources). This requires: (1) new theories and methods on design principles for resilient CPS, threat/hazard analysis, cyber-physical inter-dependence anatomy, investigation/prediction of gaming plots at different layers of CPS, (2) formal models for privacy specification that allow reasoning about and proof of privacy properties, (3) new mathematical theories on information hiding for real-time streams, (4) light-weight security solutions that work well under extremely limited computational resources (e.g. devices), (5) new theories on confidence and trust maps, context-dependent trust models, and truth/falseness detection capabilities.

Due to the unpredictability in the physical world, CPS will not be operating in a controlled environment, and must be robust to unexpected conditions and adaptable to subsystem failures. This requires: (1) new concepts of robust system design that deals with and lives on unexpected uncertainties (of network topology, data, system, etc.) occurring in both cyber and physical worlds, (2) the ability to adapt to faults through (self-) reconfiguration at both physical and cyber levels, (3) fault recovery techniques using the most appropriate strategies that have been identified, categorized, and selected, (4) system evolvement through learning faults and dealing with uncertainties in the past scenarios, (5) system evolvement through run-time reconfiguration and hot deployment.

One important omission from the above requirements is the need for semantics. In particular semantics that are capable of bridging the real physical world and the virtual world. This is addressed in our earlier paper.[IIS Keynote Ref Here]

CPS has recently been listed as the No.1 research priority by the U.S. President's Council of Advisors on Science and Technology [2]. This led the US National Science Foundation to organize a series of workshops on CPS [3]. The CPS framework has the capability to tackle numerous scientific, social and economic issues. The three applications for CPS are in future distributed energy systems, future transportation systems and future health care systems [1,4,14]. We have also investigated their use in collecting information and the control of an offshore oil platform. These applications will require seamless and synergetic integration between sensing, computation, communication and control with physical devices and processes.

In each of the above application areas Trust, Reputation, Security, Privacy and Risk Play a crucial role as they each involve the transfer and utilization of highly sensitive data. This provides the motivation for this paper.

2 Brief Overview of Architectural Framework for CPS Systems

We have previously proposed a Web-of-Things (WoT) framework for CPS systems [1, 20] that augments the Internet-of-Things in order to deal with issues such as information-centric protocol, deterministic QoS, context-awareness, etc. We argue that substantial extra work such as our proposed WoT framework is required before IoT can be utilized to address technical challenges in CPS Systems.

The building block of WoT is Representational State Transfer (REST), which is a specific architectural style [4]. It is, in effect, a refinement and constrained version of the architecture of the Web and the HTTP 1.1 protocol [5], which has become the most successful large-scale distributed application that the world has known to date. Proponents of REST style argue that existing RPC (Remote Procedure Call)-based Web services architecture is indeed not "Web-oriented". Rather, it is merely the "Web" version of RPC, which is more suited to a closed local network, and has serious potential weakness when deployed across the Internet, particularly with regards to scalability, perfor-

mance, flexibility, and implementability [6]. Structured on the original layered client-server style [4], REST specifically introduces numerous architectural constraints to the existing Web services architecture elements [19, 20] in order to: a) simplify interactions and compositions between service requesters and providers; b) leverage the existing WWW architecture wherever possible.

The WoT framework for CPS is shown in Fig 1, which consists of five layers – WoT Device, WoT Kernel, WoT Overlay, WoT Context and WoT API. Underneath the WoT framework is the cyber-physical interface (e.g. sensors, actuators, cameras) that interacts with the surrounding physical environment. The cyber-physical interface is an integral part of the CPS that produces a large amount of data. The proposed WoT framework allows the cyber world to observe, analyze, understand, and control the physical world using these data to perform mission / time-critical tasks.

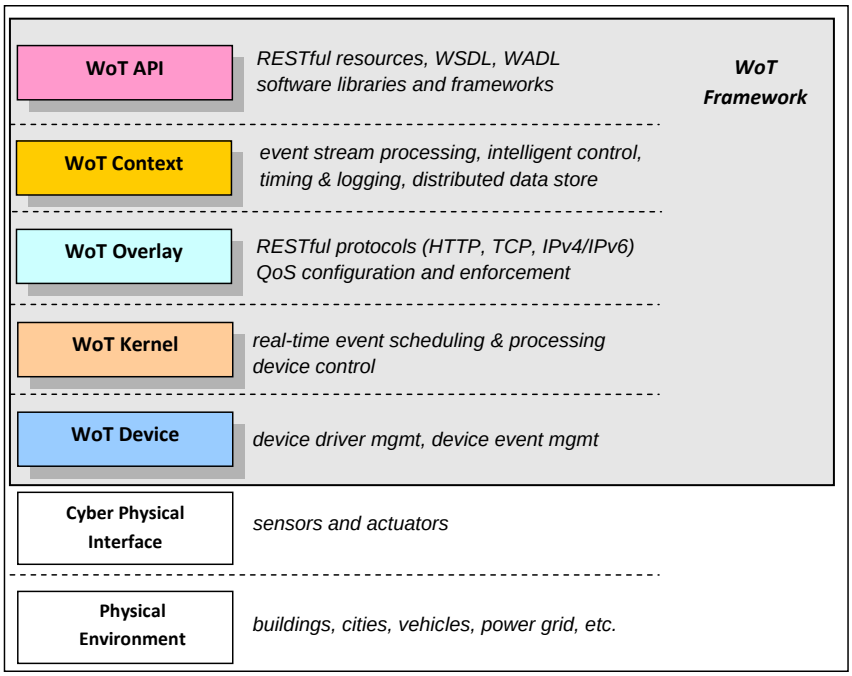

Fig 1. WoT Framework for CPS.

As shown in Fig. 1, the proposed WoT based CPS framework consists of five layers:

1. WoT Device: This layer constitute the cyber-physical interface of the system. It is a resource-oriented abstraction that unifies the management of various devices. It states the device semantics in terms of RESTful protocol.

2. WoT Kernel: This layer provides low level run-time for communication, scheduling, and WoT resources management. It identifies events and allocates the required resources, i.e. network bandwidth, processing power and storage capacity for dealing with a large amount of data from the WoT Device layer.

3. WoT Overlay: This layer is an application-driven, network-aware logical abstraction atop the current Internet infrastructure. It will manage volatile network behavior such as latency, data loss, jitter and bandwidth by allowing nodes to select paths with better and more predictable performance.

4. WoT Context: This layer provides semantics for events captured by the lower layers of WoT framework. This layer is also responsible for decision making and controlling the behaviour of the CPS applications.

5. WoT API: This layer provides abstraction in the form of interfaces that allow application developers to interact with the WoT framework.

Based on the WoT framework in Fig 1, the CPS reference architecture is shown in Fig 2, which aims to capture both domain requirements and infrastructure requirements at a high level of abstraction. It is expected that CPS applications can be built atop the CPS reference architecture.

More details about the CPS Fabric structure and the CPS node structure are given in Dillon et. al. [1].

3 Brief overview of our previous work on Trust, Reputation and Risk

In this section we give a brief description and definitions of the key ideas of Trust, Reputation and Risk defined in our previous work.[15,17]

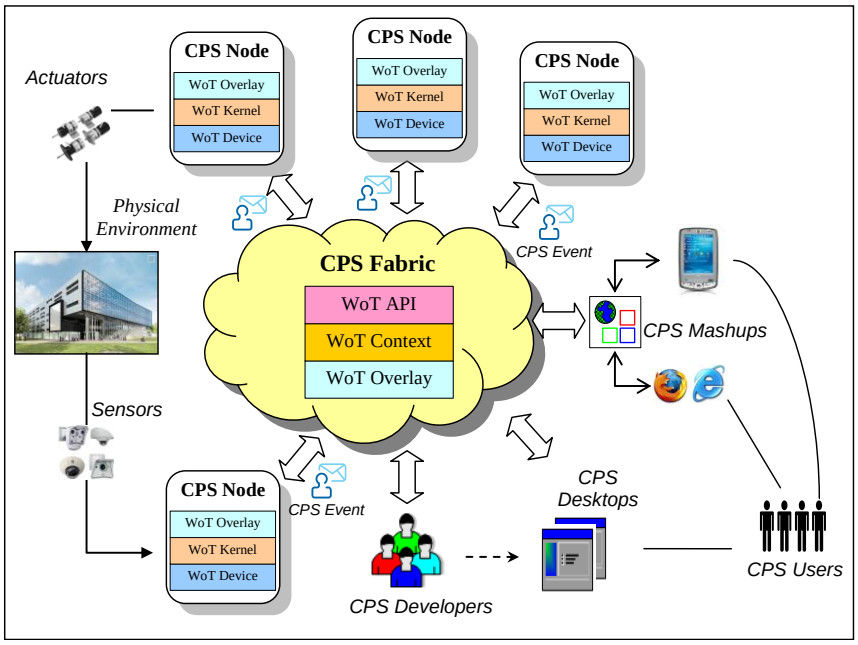

Fig 2. CPS Reference Architecture

Thus Trust is defined in

Definition: Trust is defined as *the belief* the *trusting agent* has in the *trusted agent's willingness*

and *capability to deliver a mutually agreed service* in a given *context* and in a given *timeslot.*

The term *willingness* captures and symbolises the trusted agent's will to act or be in readiness to act

honestly, truthfully, reliably and sincerely in delivering on the mutually agreed service

The term *capability* captures the skills, talent, competence, aptitude, and ability of the trusted agent

in delivering on the mutually agreed behaviour. If the trusting agent has low trust in

the trusted agent, it may signify that the trusting agent believes that the trusted agent does not have

the capability to deliver on the mutually agreed service.

In contrast, if the trusting agent has a high level of trust, then it signifies that the trusting agent

believes that the trusted agent has the capability to deliver on the mutually agreed behaviour.

The term *context* defines the nature of the service or service functions, and each *Context* has

a name, a type and a functional specification, such as ‘rent a car’ or ‘buy a book’ or ‘repair a

bathroom’. Context can also be defined as *an object* or *an entity* or a *situation* or a *scenario.*

Definition 1 – Basic Reputation Concept

Definition 1a: In service-oriented environments, we define *agent reputation* as an aggregation of

the recommendations from all of the third-party recommendation agents, in response to the trusting

agent’s reputation query about the *quality* of the trusted agent.

The definition also applies to the reputation of the *quality of product* (QoP) *and quality of*

service (QoS).

Definition 1b: In service-oriented environments, we define *product reputation* as an aggregation of

the recommendations from all of the third-party recommendation agents, in response to the trusting

agent’s reputation query about the Quality of product (QoP).

Definition 1c: In service-oriented environments, we define *service reputation* as an aggregation of

the recommendations from all of the third-party recommendation agents, in response to the trusting

agent’s reputation query about the Quality of the Service (QoS).

Definition 2 – Advanced Reputation Concept

Definition 2a: In service-oriented environments, we define *agent reputation* as an aggregation of

the recommendations from all of the third-party recommendation agents and their first-, second- and

third-hand opinions as well as the trustworthiness of the recommendation agent in giving correct

recommendations to the trusting agent about the quality of the trusted agent.

Definition 2b: In service-oriented environments, we define *service reputation* as an aggregation of

the recommendations from all of the third-party recommendation agents and their first-, second- and

third-hand opinions as well as the trustworthiness of the recommendation agent in giving correct

recommendations to the trusting agent about the Quality of the Product (QoP).

Definition 2c: In service-oriented environments, we define *product reputation* as an aggregation of

the recommendations from all of the third-party recommendation agents and their first-, second- and

third-hand opinions as well as the trustworthiness of the recommendation agent in giving correct

recommendations to the trusting agent about the Quality of the Service (QoS).

Fundamentally, reputation is an aggregated value of the recommendations about the trustworthiness

of a *trusted agent* (such as a trusted agent or QoP and services). The reputation value is not

assigned but only aggregated by the trusting agent.

There are four primary concepts that should be clearly understood in the reputation definition:

(1) *Reputation*: aggregation of all the recommendations from the third-party recommendation agents

about the quality of the trusted agent.

(2) *Recommendation (including opinion and recommendation value)*: submitted by the third-party

recommendation agents (recommenders).

(3) *Recommendation agent*: submit the recommendation or opinion to the trusting agent or respond to a reputation query.

(4) *Reputation query*: a query made by the trusting agent about the trusted agent in a given context

and timeslot.

The terms ‘reputation query’, ‘third-party recommendation agents’, ‘first-, second- and third-hand

opinions’, ‘trustworthiness of recommendation agent’, ‘trusting agent’, ‘trusted agent’ are essential

when defining reputation. These new terms can be regarded as the building blocks of reputation,

particularly in service-oriented environments. These new terms introduced in the definition of

reputation make a fundamental distinction between trust and reputation.

In contrast to Trust and Reputation,when assessing Risk it is important to take into account :[16]

1. The likelihood of an event taking place
2. The impact of the event.

   Thus it is not only important to calculate a failure probability but also the the likely financial or other cost of the failure.

We have previously designed a risk measure that takes both of these into account.

In addition , we have developed ontologies for Trust, Reputation and Risk [15,16,18] and Data Mining techniques for analyzing this[21].

4 Extensions of Trust , Reputation and Risk For CPS

In CPS systems we have several issues in relation to Trust and Reputation that have to be addressed.

1. Previously we determined , forecast , modelled and predicted the Trust and Reputation of a single agent, service or service provider. In CPS systems we frequently are collecting information from a number of sensors, agents, heterogeneous resources and synthesizing or fusing the information to find out the system state, condition and to provide situation awareness. We need to extend the previous ideas on Trust and Reputation to groups of Agents and Services.
2. The agents in CPS could also be functioning as members of a virtual community which seeks to bargain on their behalf collectively for instance in a smart grid situation. Then the other members of the community need to be able to evaluate and feel confident that any individual member of the community will play their part so as not to jeopardize the community as a whole. This will need not only Trust evaluation but also mechanisms for rewarding good behaviours and penalizing aberrant behaviours.
3. The notion of Trust and Reputation discussed in the previous section essentially dealt belief with the willingness and capability of the agent, service, and service provider to fulfil their commitment. In CPS systems the situation is complicated by the fact that the Data being generated could be noisy and have limi-

tations on its accuracy. This has to be modelled in the Trust models.

4. The Real world environment also has a degree of uncertainty associated with the occurrence of different

   Events. This uncertainty has to be modelled.

   Issues 3. and 4. above will provide qualifiers on the evaluation of Trust. Namely The value of Trust will have certain accuracy and confidence level associate with it.
5. The uncertainty in the real world environment also has a major impact on the calculation of Risk.

5 Conclusion

In this keynote we will explain the extensions necessary to apply the concepts of Trust, Reputation and Risk for Cyber Physical Systems in detail. These extensions are of major significance for CPS systems.

References

1. Dillon, T. S., Zhuge, H., Wu, C., Singh, J., Chang, E.: Web-of-things framework for cyber–physical systems. Concurrency and Computation: Practice and Experience. vol. 23. Issue 9. pp. 905, 923. (2011)
2. President's Council of Advisors on Science and Technology (PCAST), Leadership under challenge: Information technology r&d in a competitive world, http://www.nitrd.gov/pcast/reports/PCAST-NIT-FINAL.pdf August (2007)
3. National Science Foundation, Cyber-physical systems (CPS) workshop series, *http://varma.ece.cmu.edu/Summit/Workshops.html*,
4. National Science Foundation, Cyber-physical systems summit report, http://precise.seas.upenn.edu/events/iccps11/_doc/CPS_Summit_Report.pdf, Missouri, USA 24-25 April (2008)
5. Lee, E.: Cyber physical systems: Design challenges. in *IEEE Object Oriented Real-Time Distributed Computing*, pp. 363-369. , (2008)
6. Lee, E.: Computing needs time. Communications of the ACM. vol. 52, No. 5, pp. 70-79. (2009)
7. National Science Foundation. Cyber-physical systems executive summary, *http://varma.ece.cmu.edu/Summit/CPS_Summit_Report.pdf*, (2008)
8. Dillon, T., Talevski, A., Potdar, V., Chang, E.: Web of things as a framework for ubiquitous intelligence and computing. In The 6th International Conference on Ubiquitous Intelligence and Computing, p. 13 in Ubiquitous Intelligence and Computing. vol.5585, ed. Zhang, D., Portmann, M., Tan, A.-H., Indulska, J., (2009)

9. Dillon, T.: Web-of-things framework for cyber-physical systems. In The 6th International Conference on Semantics, Knowledge & Grids (SKG*)*, Ningbo, China (2010) (Keynote).
10. Talcott, C.: Cyber-Physical Systems and Events. In Software-Intensive Systems and New Computing Paradigms.vol.5380, ed. Wirsing, M., Banâtre, J.-P., Hölzl, M., Rauschmayer, A., pp. 101-115. Springer Berlin, Heidelberg. (2008)
11. Tan, Y., Vuran, M. C., Goddard, S.: Spatio-temporal event model for cyber-physical systems. In 29th IEEE International Conference on Distributed Computing Systems Workshops. pp. 44-50. (2009)
12. Tan, Y., Vuran, M. C., Goddard, S., Yu, Y., Song, M., Ren, S.: A concept lattice-based event model for Cyber-Physical Systems. Presented at the Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, Stockholm, Sweden. (2010)
13. Yue, K., Wang, L., Ren, S., Mao, X., Li, X.: An AdaptiveDiscrete Event Model for Cyber-Physical System. In Analytic Virtual Integration of Cyber-Physical SystemsWorkshop., pp. 9-15. USA (2010)
14. Yu, Xinghuo, Cecati, Carlo, Dillon, Tharam, Godoy Simões, M. : Smart Grids: An Industrial Electronics Perspective. In IEEE Industrial Electronics Magazine IEM-02 (2011)
15. Chang, E., Dillon, T. S., Hussain, F.: Trust and Reputation for Service-Oriented Environments. Technologies For Building Business Intelligence And Consumer Confidence. John Wiley & Sons (2006)
16. Hussain, O, Dillon, T. S., Chang, E, Hussain, F.: Risk Assessment and Management in the Networked Economy. With Risk Assessment and Management in the Networked Economy. Studies in Computational Intelligence , Springer (2012)
17. Chang, EJ, Hussain, FK, Dillon, TS: Fuzzy Nature of Trust and Dynamic Trust Modelling in Service Oriented Environments. Proceedings of the 2005 workshop on Secure web services, 75-83.
18. Wouters, C., Dillon, T, Rahayu, JW, Chang, E: A practical Approach to the derivation of a Materialized Ontology View Web Information Systems, ed. Taniar, D. and Rahayu, J, pp.191-226. Hershey USA: Idea Group Publishing. (2004)
19. Wu, C., Chang., E. J.: Searching services "on the web: A public web services discovery approach. In Third International Conference on Signal-Image Technology & Internet-based Systems, Shanghai, China. IEEE, (2007)
20. Dillon, T. S., Wu, C., Chang, E. J.: Reference architecture styles for service-oriented computing. In Lecture Notes in Computer Science, vol. 4672, Network and Parallel Computing, Li, ed. Keqiu, Jesshope, Chris, Jin, Hai, Gaudiot, Jean-Luc: 543-555. Heidelberg: Springer. (2007)
21. Tan, H., Dillon, T. S., Hadzic, F., Feng, L., Chang, E. J.: MB3-Miner: Efficient mining eMBedded subTREEs using tree model guided candidate generation. In First International Workshop on Mining Complex Data (MCD) in conjunction with ICDM'05, Houston, Texas, USA: IEEE., Nov 27, (2005)