Towards the Internet of Safe and Intelligent Postal^{+} Things

Massimo Ancona Viviana Mascardi Nicoletta Noceti Francesca Odone
DIBRIS, University of Genova, Genova, Italy
name.surname@unige.it

Waqas Ahsen Antonino Scribellito
PostEurop, Brussels, Belgium
europeanprojects@posteurop.org, antonino.scribellito@posteurop.org

***Abstract*—SAFEPOST is an FP7 European project which was active from April 2012 to July 2016 aimed at the "reuse and development of Security Knowledge assets for International Postal supply chains", as its full title explains. SAFEPOST addressed threats to postal security by designing and experimenting a sensor network detection system including gas, radiation, Raman spectroscopy and image-based sensors. In 2015, while SAFEPOST was running, the US Postal Service and IBM suggested the idea of applying sensors to the postal infrastructure components to bring the acquired data to the next supply chain level and optimize efficiency and costs, leading to an Internet of Postal Things. Merging the SAFEPOST and Internet of Postal Things approaches and applying the result of their merge to supply chains involving not only postal items, but also logistic infrastructures and business processes, paves the way to an Internet of Safe Postal^{+}Things, IoSP^{+}T. The IoSP^{+}T can be further enriched and made smarter, more flexible, and *intelligent*, by adding agents below, inside, and on top of it.**

In this paper we provide our vision of the *Internet of Safe and Intelligent Postal^{+} Things*, IoSIP^{+}T, highlighting challenges and opportunities.

***Index Terms*—Agents, Multiagent Systems, Internet of Intelligent Things, Internet of Postal Things, Safety, Supply Chain**

I. Introduction

As observed by [19], [32], [33] among many others, Postal Services are reporting mounting deficits every year all over the world: in order to survive, they need to redesign their business. In particular, first-class mail undergoes e-mail, sms, chat and other forms of electronic replacements. "The worse news is the Postal Service expects first-class mail volume to continue dropping by nearly 50% over the next decade" [19]. If they want to survive, they must exploit the most recent technological advances: sensors within the Internet of Things [6], Cloud Computing [51], Big Data technologies [73] and, above all, *Artificial Intelligence*. Based on these observations, the US Postal Service (USPS) and IBM recently proposed to take advantage of the dramatic decline of the cost of sensors and wireless data connectivity, and push the Internet of Things (IoT) into the postal domain.

In 2015, the USPS RARC Report [69] and Marsh and Piscioneri [49] presented the Internet of Postal Things (IoPT) vision: applying sensors to the various component of the Postal infrastructure (vehicles, mailboxes, machines, letter carriers etc.) for bringing data management to the next level. In almost the same years, the notion of Internet of Intelligent Things [5], [18] as a network of "intelligent devices that are capable of communicating with each other, making certain decisions based on local information, and taking autonomous and coordinated actions", to quote [18], was born. In the community working on agents and multiagent systems (MAS), such intelligent devices would be named "agents", and a network consisting of them, would be named "MAS". And in fact, even if using a different terminology, the idea of making IoT smarter and more intelligent by exploiting methodologies and approaches coming from the agent community, also started to flourish in those years [15], [26], [27], leading to many initiatives including the special session on "Internet of Things and Internet of Agents (ITIA)" at the IDC 2019 conference [30], and the explicit reference to IoT as a topic of interest in the PRIMA 2019 call for papers [7].

Despite intelligence on board of the interconnected devices, a wide adoption of Internet and IoT, with a consequent widespread dissemination of sensors, greatly amplifies security and efficiency problems. In such a context, the experience gathered in recent EU projects provides fundamental insights for future developments of e-logistic projects based on Machine-To-Machine (M2M) and IoT. On this respect we mention three recent EU e-logistics projects, SAFEPOST[1], iCargo[2], and e-Freight[3] which aimed at developing frameworks, reference models, and demonstrators to improve, via technologies at the state of the art, a safe and efficient transport of, respectively, postal items, cargo, and containers, throughout the EU. When in Europe these three projects were still active or just closed, in the US, USPS and IBM envisioned the Internet of Postal Things. By generalizing USPS vision, we might consider the "Internet of Safe Postal^{+} Things" (IoSP^{+}T), where by "Postal^{+}" we mean Postal items and

[1] https://www.posteurop.org/SAFEPOST, start: 01/04/2012; end: 30/07/2016.

[2] https://cordis.europa.eu/project/rcn/100869/factsheet/en, start: 01/11/2011; end: 30/04/2015.

[3] https://cordis.europa.eu/project/rcn/94475/factsheet/en, start: 01/01/2010; end: 30/06/2013.

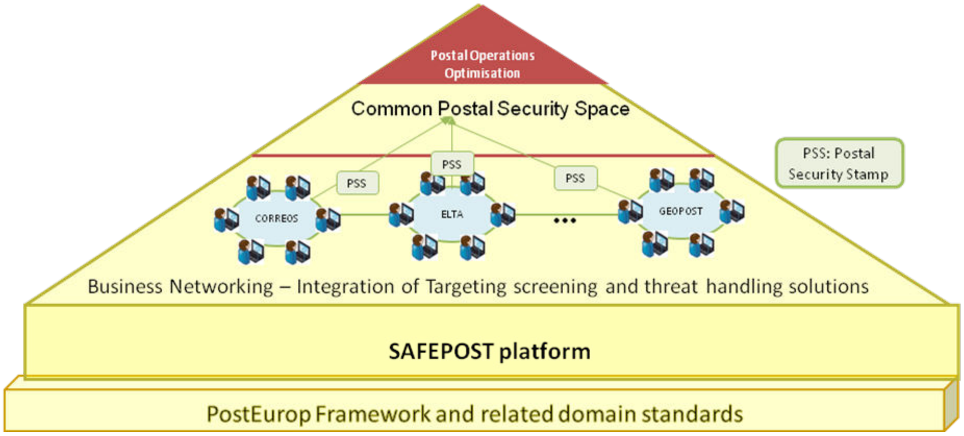
Postal Operations Optimisation
Common Postal Security Space
PSS
PSS
PSS
CORREOS
ELTA
GEOPOST
PSS: Postal Security Stamp
Business Networking – Integration of Targeting screening and threat handling solutions
SAFEPOST platform
PostEurop Framework and related domain standards

Fig. 1. The layered architecture of the SAFEPOST project.

components together with more general logistic processes and infrastructural architectures. And by exploiting agents, IoSP^{+}T could move towards the IoSIP^{+}T, namely, the "Internet of Safe *and Intelligent* Postal^{+} Things".

SAFEPOST, iCargo, and e-Freight could naturally evolve into IoSIP^{+}T projects.

In the IoSIP^{+}T context, safety and security are so closely intertwined to be no longer considered two separate concerns: any system interfaced with the outside world has the potential to expose security vulnerabilities. In particular, systems connected to the Internet and the IoT need to be protected against specialized targeted malware attacks and against a whole world of hackers. This paper deals with safe and secure IoSIP^{+}T, grounding its root into the authors' experience in SAFEPOST and in Artificial Intelligence in general, and agents and MAS in particular. After presenting the state of the art in postal security - mainly represented by the results achieved by SAFEPOST - in Section II, we analyse new research directions towards intelligent, dependable and resilient supply chains development with the adoption of agents together with IoT and cloud computing in Section III. Section IV is left to conclusions and final remarks.

II. SAFEPOST AND THE STATE OF THE ART IN POSTAL SECURITY

"SAFEPOST: reuse and development of Security Knowledge assets for International Postal supply chains" is an FP7 European project which spanned the period from April 2012 to July 2016, involving 20 partners for a total cost of nearly 15 million euros. Its main design principles are:

- The introduction of safety sensors, i.e. sensors expressly designed for augmenting knowledge about safety and security information on parcels.
- A well defined hierarchical organization based on (i) the sensing layer, implemented by the Targeting and Threat Handling component and devoted to the safety sensors management and data acquisition; (ii) the network layer, implemented by the Common Postal Security Space (CPSS); (iii) the application layer, composed by the e-logistic (service oriented) optimization code.
- The treatment of security performed in each architectural layer.

The layered architecture shown in Figure 1 simplifies the development of certified code while providing high levels of assurance, and makes this process practical and affordable. It also simplifies code and artefact reuse to leverage investments. A Postal Security Stamp (PSS) connects the SAFEPOST components together. It identifies postal items and associates place of origin, destination, content information, screening history, image comparison data, track and trace mechanisms with them. The information can be traced in real time by authorized stakeholders.

SAFEPOST implementation is centered on a D2D (Door-To-Door) delivery mechanism completely controlled by human operators performing H2M (Human-To-Machine) & M2H (Machine-To-Human) communication. Replacing (part of) a H2M mechanism by a direct M2M communication in an IoT environment, besides optimizing efficiency and costs of delivery, remarkably increases security problems. This is why SAFEPOST has been conceived to be secure by design: SAFEPOST implements a security level able to satisfy evolving international regulations and standards while efficiently supporting the complexity of postal services market across Europe, without increasing costs. Also, and more important for its implications in the development of an IoSIP^{+}T, SAFEPOST could be adopted as the minimum kernel in the development of future safe and dependable intelligent supply chain systems.

A. The Screening System and Safety Sensors

The SAFEPOST Screening System is a hardware-software infrastructure consisting of D-Tube, Raman and Radiak sensors, and an image recognition system[4].

[4] The information related to some sensors is confidential so just a short overview of their specifications and functionalities can be published.

1) The D-Tube: The D-tube is used for detecting explosives or narcotics in real time; the prototype developed within the SAFEPOST project uses a multi-element detector for the generation of the chemical profiles and is suitable for integration into the sorting facility conveyor belt flow. It operates in near real time with high precision and specificity by examining vapor substances. The system also takes into account the varying background vapors ubiquitously present in the air. This D-Tube system consists of three different sub-systems:

- The Breathing Sub-system
- The Air Supply Sub-system
- The eNose Gas Sensor Sub-system

The Breathing Sub-system is positioned over the conveyor belt. It uses a device to compress the packages in order to press out air from the inside of the packages. This procedure makes packages emit as much of the enclosed molecules as possible for further detection. This “active breathing” is key to make the system work consistently on a wide range of different packaging types. The Breathing System is designed to stay within the envelope of specifications for proper handling of the packages.

The Air Supply System is a “sniffer” system positioned after the breathing device to “sniff” any molecules being emitted from the packages. It consists of several silicon hoses and acts as a “vacuum cleaner” to vacuum the packages on its side and on the top. This is being done just after the breathing system has compressed the package. The hoses in the “sniffer” system are then connected and lead the air flow to the Gas Sensor Sub-system, also called the eNose. The eNose chamber consists of 18 separate electronic sensors (“noses”) capable of detecting different molecules such as explosives and narcotics.

2) Radiak and Raman Sensors: The radiation sensor is based on a semiconductor detector of High Purity germanium (HPGe detector) which measures ionizing radiation by means of the number of charge carriers set free in the detector material, which is arranged between two electrodes, by the radiation. Ionizing radiation produces free electrons and holes. Under the influence of an electric field, electrons and holes travel to the electrodes, where they result in a pulse that can be measured in an outer circuit.

3) Image Recognition System: The role of the Image Recognition System in SAFEPOST (see a sketch in Figure 2) is to allow postal operators to screen the exterior of the parcels in order to detect damages and signs of tampering [58]. The Image Recognition System provides information to the CPSS as well as to the human postal operator. Information sent to the CPSS can be integrated with the results of other sensors or with previous scans of the same parcel in order to compare if and how the parcel changed over time and better evaluate its tampering risk. At the same time, as the system performs the parcel analysis on the fly, human operators can be immediately informed of suspicious parcel’s features and can intervene on the parcel, according to the risk management policies implemented by the postal operator.

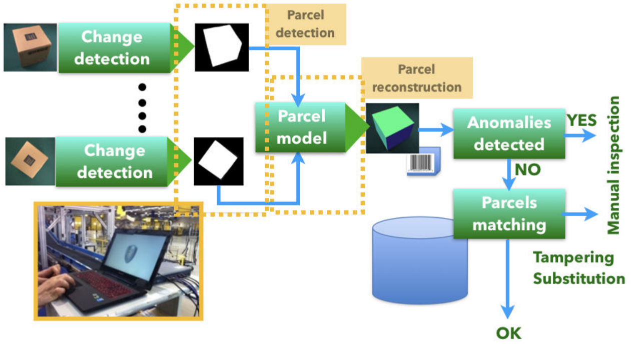

Fig. 2. The image recognition system.

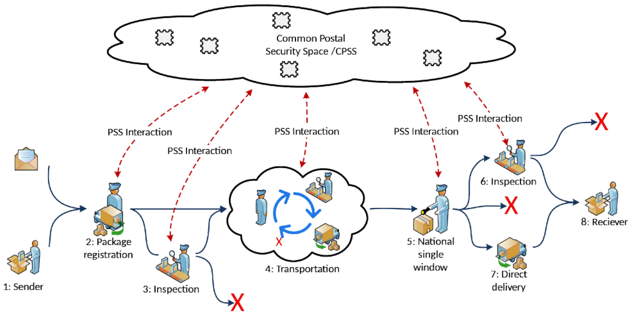

Fig. 3. Package handling work-flow.

B. The Targeting and Threat Handling Reasoning System

The Targeting & Threat Handling Reasoning System is a high level decision support system which combines information from both the SAFEPOST sensors and other sources to conduct risk assessments. Risk assessment is driven by the work-flow of the package handling represented, in a simplified way, in Figure 3. Information gathered from sensors and from the stakeholders involved in the process is used to assess the risk that a parcel is a potential threat throughout the entire D2D postal delivery supply chain. The system discovers potential threats in real-time and assesses those not detectable by physical screening. When a threat is detected, the system helps users decide on which plan to follow based upon the threat, time and resources available. The Targeting and Treat Handling Reasoning System operates at the intermediate level and performs different fusion services onto data in the CPSS to address different phases of the risk management process as follows:

- A risk assessment sub-system fuses all available information regarding letters and parcels to determine which parts of the sorting facility convey or belts should be subject to additional screening on top of the mandated ones. This step of the process uses available information from, e.g., alert levels set by security agencies, intelligence databases, information from cargo operators and customs, besides the information coming from SAFEPOST sensors.

- The results of the detection are combined with other available data to determine what should be done with the suspicious parcels. In particular, using information about the uncertainties in the detection result and combining these with other available information enables the system to choose different handling strategies (with associated different delays in cycle time) for different risks.

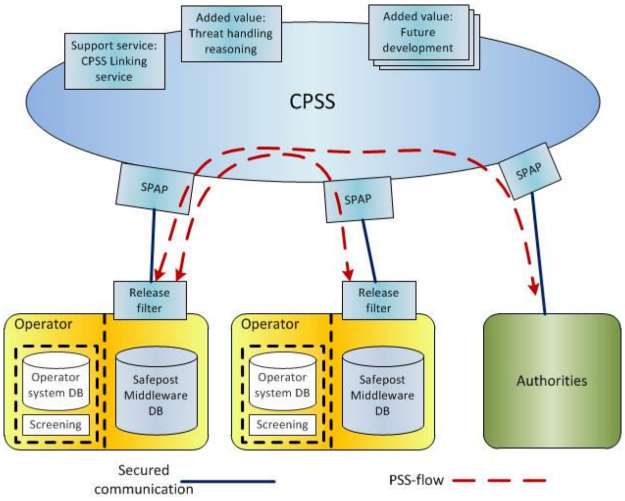

Fig. 4. The Common Postal Security Space.

C. The Common Postal Security Space (CPSS)

The CPSS is shown in Figure 4 and is based on the PostEurop framework[5] as operating model, which aligns EU Policy and Legislation with IT security management and industry wide best practice processes, through a shared network. The CPSS is integrated with the screening systems, target and threat handling reasoning and information sharing via the universally trusted Postal Security Stamp.

D. The Optimization Component

This component consists of a real-time logistics optimization system that automatically reads GPS tracking data and updates the logistics plan accordingly. This is more than simply updating the Estimated Time of Arrival (ETA) of a vehicle, as the system automatically fixes resulting logistics problems using intelligent optimization algorithms. For example, if a vehicle is delayed so that it will not arrive at its destination in time to undertake the next planned work, the optimization component automatically reassigns the work to the next best resource available. The real-time rescheduling means that the logistics plan is constantly updated (working within operational constraints and rules) so that at any point in time the system "knows" what should be happening next, even if this is now different from the original plan at the start of the day.

E. Related Work in Postal Security

After the Yemen bomb plot in 2010[6], the postal security management entered its biggest reform in modern times. In 2012 the Universal Postal Union (UPU), the United Nations (UN) organization coordinating global postal policies, issued two postal security standards binding all of its 192 members countries:

- S58, Postal Security Standards - General Security Measures which defines the minimum physical and process security requirements available to critical facilities within the postal network;
- S59, Postal Security Standards - Office of Exchange and International Airmail Security which defines minimum requirements for security operations relating to the air transport of international mail.

Besides regional legislation in the transportation sector, which have been rapidly evolving as well over the past few years with major implications on postal security[7], also academic literature on security in the supply chain has become huge after September 11, 2001: as observed by Männistö in [50], "The terrorist attacks of September 11, 2001 raised major concerns about the vulnerability of global transportation systems to transnational crime and terrorism. Although the attacks occurred in the context of passenger transport, they spurred unprecedented academic research on supply chain security (SCS)". Männistö defines a supply chain crime taxonomy, carries out a deep literature review showing that the SCS discipline is more empirically grounded and diverse than the previous literature reviews suggest, and discusses a case study in the international postal service from the Swiss perspective. To the best of our knowledge, that work is one of the more recent and complete academic documents dealing with safety and security in the supply chain in general, and in the postal sector in particular. Compared to SAFEPOST[8] it complements its practical results with a strong theoretical underpinning by providing a taxonomy which can serve as a unifying framework in the supply chain crime area, and which can be generalized and adapted to other domains. Although Männistö's work also includes a practical component, leading to concrete suggestions to the Swiss Post and Swiss authorities based on the results of the case analysis, it cannot compete with the practical solutions to threat handling proposed within such a large project as SAFEPOST.

Given that the SAFEPOST approach is fully compliant with the most recent regional and UPU standards, and that the academic literature we are aware of in the postal safety and security areas is connected and complementary to the project, we can assess that SAFEPOST findings are the state of the art in postal security.

[5] http://www.posteurop.org/VisionandMission

[6] https://en.wikipedia.org/wiki/Cargo_planes_bomb_plot

[7] https://ec.europa.eu/transport/modes/air/security/legislation_en;https://www.faa.gov/regulations_policies/faa_regulations/

[8] Männistö's Ph. D. Thesis is not fully disjoint from SAFEPOST: he received funding from SAFEPOST, as stated in his thesis acknowledgments.

III. Beyond SAFEPOST: towards an IoSIP$^+$T

As discussed in Section II, SAFEPOST is a layered, distributed architecture with sophisticated sensors at the lowest level, organizations that must protect their data and privacy on the one hand, and must collaborate to reach a safer management of postal items on the other, complex interactions among the parties involved, reasoning and optimization systems at the top of the architecture. The holonic MAS metaphor [64] is extremely suitable to describe SAFEPOST: some sensors like the image recognition system depicted in Figure 2 are so sophisticated, that may be seen as MASs themselves. The same holds for the different providers of postal services, which could be seen as individual agents if we analyze the high level interactions among them, taking place within the CPSS, but can also be seen as MASs due to the many components they consist of, and their complex dynamics.

More intelligence can be added to SAFEPOST's architecture, both at the sensor level – by making sensors smarter –, and at the global architecture level – by making it more flexible and adaptable, and by improving the existing optimization component, which could be based on agents [8], [29], [61], [70]. The reasoning component could take advantage of agents as well, along the lines of some recent proposals for agent-based distributed reasoning including [9], [38], [54].

But the "SAFEPOST of the future", besides intelligent, must also be resilient.

Resilience is the capacity to quickly recover from difficulties; in a supply chain context, it can be seen as the ability to react in a timely fashion to unexpected external events including delayed delivery, reduced exchange of information with other companies in the chain, hardware/software failures, but also more disruptive ones such as floods, earthquakes, acts of terrorism. Dependability of a system reflects the user's degree of trust in that system: it measures the numerical extent of the user's confidence that the system will operate as expected. Implementing dependable and resilient supply chains is a strategic choice for mitigating the risks [35]. The notion of dependability[9], together with responsiveness, agility, cost, and assets, is one of the five Standard Strategic Metrics of the Supply Chain Operations Reference model, SCOR[10]. Delivery dependability, also known as delivery reliability [63] is the ability, for supply chains,"to exactly meet quoted or anticipated delivery dates and quantities" [72]. Specific sensors and relative fusion algorithms can help extracting several kinds of contextual data, raising the system context awareness which represents a key ingredient of the IoT. Quoting [53], "...smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of IoT. With the growing presence of WiFi and 4G-LTE wireless Internet access, the evolution towards ubiquitous information and communication networks is already evident". Today's companies are already adopting resilience and dependability for obtaining an immediate reaction to unpredictable events through smart organizations: both resiliency and dependability imply safety and security requiring advanced forms of context-awareness. The meaning of context depends on the application domain and may involve many aspects, including location, time of day, emotional state of the user, orientation, and even the preferences or identities of people within an environment. In an IoSIP$^+$T, the context is also represented by data coming from advanced physical sensors. In order to be useful, sensory data need to be located, described, measured, and analysed on the fly in real-time, which requires sophisticated approaches to sensor fusion. SAFEPOST already provides a first answer to the need of dependability, resilience and context awareness; in its current setting, context- and self-awareness are supported by the specific safety sensors discussed in Section II-A whose outputs are fused within the targeting and threat handling reasoning system discussed in Section II-B.

In a more general IoSIP$^+$T perspective, SAFEPOST could be extended to integrate other sensors into a single MAS made secure by design [31] and supporting different levels of awareness operated in an IoT, within a Cloud environment. In the following we discuss approaches, methods and techniques that could be integrated within the existing SAFEPOST framework, to transform it into an IoSIP$^+$T.

A. *CPS, Spimes and Smart Objects*

SAFEPOST safety sensors operate in real-time and are designed with the dependable and resilient architecture of fully-protected Cyber Physical System (CPS). Safety and security are design dimensions of a CPS: safety is aimed at protecting the systems from accidental events while security is limited to hostile actions, and both share the goal of protecting a CPS from failures. As pointed out in [62] when safety and security are aligned, namely when actions performed for enforcing safety do not contrast with actions performed for enforcing security, they make the enclosing CPS almost inviolable. A theoretical concept which has recently emerged as an evolution of CPS and sensors in the direction of real time and context-aware tracking, is that of the spime[11] a uniquely identifiable object whose real-time attributes can be continuously tracked. Smart objects [39], namely computers equipped with sensors and/or actuators, and a communication device, are examples of spimes. They are described as the building blocks for the IoT [43] and can be embedded in cars, light switches, thermometers, billboards, or machinery. The gap between a smart object and an intelligent software agent is very small: the smarter the object, the closer to an agent [60]. The integration of smart objects in SAFEPOST would definitely increase not only its context awareness, but also its ability to self-adapt and self-repair thanks to the smart objects actuators which can play an active role, differently from traditional, passive sensors. The ability to manage itself is a "must" for the SAFEPOST of the future, given that SAFEPOST should be able to survive

[9] Named "reliability" and meaning "Perfect Order Fulfillment".

[10] http://www.apics.org/apics-for-business/products-and-services/apics-scc-frameworks/scor

[11] Spime is a neologism introduced by B. Sterling (2005) as the contraction of space and time.

to disasters, to continue keeping the infrastructure as safe as possible. The opportunities to increase SAFEPOST reliability thanks to self* approaches are huge: self-adaptive and self-organizing MASs [1], [28], [55], [65] are very close to autonomic computing systems, namely systems that "manage themselves according to an administrators goals. New components integrate as effortlessly as a new cell establishes itself in the human body" [41]. An "autonomic SAFEPOST" would give many advantages, but would also raise many challenges. In particular, autonomy in self-adapting, self-organizing and self-repairing should balance compliance to existing technical, legal, and even ethical constraints. To reach this goal, designers should be able to verify in advance (at design time, when the system is still under test) as many properties of the "autonomic SAFEPOST" as possible via traditional techniques based on model-checking. At runtime, when the system has been deployed, it should undergo a continuous monitoring to early detect those anomalies that static verification techniques could not capture, and report them to a human controller. While these problems are far to be solved, in particular for large and complex systems as an "autonomic SAFEPOST" would be, some results achieved within the MAS community seem to go in the right direction. Model checking MASs has a long tradition which dates back to the beginning of the millenium [11], [12], [47], [74] and, although not scaling well to large systems, could be used for the design-time static verfication. Recently, runtime verification mechanisms suitable for MASs in particular, and for distributed system in general, have been proposed [2], [4], [23]. Attempts to integrate static and runtime verification techniques in the MAS domain are discussed in [3] and in [24], [25]: while the first work deals with the relationships between Linear Temporal Logic and the trace expression formalism used for MAS runtime verification, the last ones address the problem of validating an abstract environment designed for model checking purposes, at runtime.

B. Real-Time Data Mining

A real-time management of threats, like in SAFEPOST's Targeting and Threat Handling Reasoning System, requires a real-time analysis of the acquired data and new forms of dependable data mining algorithms. As observed in [68], "data mining has typically been applied to non-real-time analytical applications. Many applications, especially for counter-terrorism and national security, need to handle real-time threats. [...] This means that the data mining algorithms have to have the ability to recover from faults as well as maintain security, and meet real-time constraints all in the same program." Real time data mining is a hot research topic, as witnessed by many existing tools [10], [56], papers [22], [37], [44], [71], and even patents [20]. In the same way as massive data generated by the IoT can be analysed and managed with data mining techniques adapted to cope with big data and data streams [17], existing data mining algorithms operating in real-time could be adopted to manage data generated by an IoSIP$^+$T system, in order to cope with its complexity and to increase its dependability, in particular when boosted by agents [46]. A challenging research direction is "real-time weak signal detection mining", and its integration with the results obtained by a more traditional mining of IoT data. In fact, a really safe logistic system, should also take weak signals of threats coming from news, social networks, the web, into account. As observed in [14], "Lone wolf terrorists pose a large threat to modern society. The current ability to identify and stop these kinds of terrorists before they commit a terror act is limited since they are hard to detect using traditional methods. However, these individuals often make use of Internet to spread their beliefs and opinions, and to obtain information and knowledge to plan an attack. Therefore there is a good possibility that they leave digital traces in the form of weak signals that can be gathered, fused, and analyzed". An agent-based approach might turn useful to tackle the last tasks, as discussed for example in [57], [76].

C. Integrating IoT and Cloud Computing for Logistics

Although IoT and cloud computing are different paradigms, they play complementary roles in tackling emerging needs of the current world, and both are recognized as being extremely suitable to supply chain management. While the IoT mainly consists of device connections via the Internet, the role of the cloud is to deliver data, applications, streams, images, and other digital objects in a distributed context. The huge implications of IoT for logistics have been explored by Cisco and DHL [48] among the others and are raising more and more attention [40], [52], [66], mainly when combined with big data management [42]. A similar or maybe even greater interest can be observed for the adoption of cloud computing for logistics and supply chain management, which - besides many scientific and popular articles (see for instance the recent works [16], [67]) - also lead to patents [36]. The integration of IoT with cloud computing [13] offers an additional potential benefit to significantly reduce costs on a pay-per-use base and with an improved customer service based on rationalization of operations, through optimization and increased operating and economic efficiencies and supporting the development of new services and business models. Several postal and logistic companies are already offering their service from the cloud and the combination of IoT with intelligent CPSs makes them accessible anytime and anywhere. This combination will be a key enabler of the IoSIP$^+$T, and agents will play a relevant role to add intelligence, security, and flexibility to it, as discussed for example in [45], [75], [77].

IV. Conclusions and Future Work

In its most recent mobility report, Ericsson forecasts that around 29 billion connected devices will be available by 2022, of which around 18 billion related to IoT. Connected IoT devices will include cars, machines, meters, sensors, point-of-sales terminals, consumer electronics and wearable [34]. Between 2016 and 2022, IoT devices are expected to increase at a compound annual growth rate of 21 percent, driven by new use cases. In [21] the author discusses seven ways the IoT will change our lives. Besides boosting remote work and increasing speed, accessibility, efficiency, and productivity, he points out that IoT will transform how companies track and manage their inventory, since smart devices will be able to keep tabs on inventory changes completely automatically, moving from "smart homes" to "smart offices" and "smart warehouses". According to [59], companies in the 2016 Fortune 500 list[12] are implementing real-time resilient and dependable supply chain IoT platforms able to solve key questions pertinent shipment's context-awareness, like continuous knowledge of its space-temporal position and precise forecasting of delivery time. Many companies are already boosting their business thanks to IoT and/or cloud computing, and the others will follow. For those working in the logistic sector, moving to an IoSIP$^+$T would require investments in new intelligent safety sensors, an infrastructure supporting not only communication among these sensors, but also the possibility to verify their behaviour (including communicative behaviour) at runtime, a shift in the business process to include some "security stamp" à la SAFEPOST, attached to physical objects, and an injection of intelligence in all of those processes which are not routinary, and require to perform some reasoning or other sophisticated tasks. Moving to this new setting would be worth the costs, since the integration of security sensors in CPSs connected in an IoT network as smart objects (or agents) and operating in a cloud environment in real time seems one of the most promising approaches for realizing dependable, resilient, and intelligent supply chains.

References

[1] D. Ancona, D. Briola, A. Ferrando, and V. Mascardi. Global protocols as first class entities for self-adaptive agents. In *AAMAS*, pages 1019–1029. ACM, 2015.

[2] D. Ancona, S. Drossopoulou, and V. Mascardi. Automatic generation of self-monitoring MASs from multiparty global session types in Jason. In *DALT*, volume 7784 of *Lecture Notes in Computer Science*, pages 76–95. Springer, 2012.

[3] D. Ancona, A. Ferrando, and V. Mascardi. Comparing trace expressions and Linear Temporal Logic for runtime verification. In *Theory and Practice of Formal Methods*, volume 9660 of *Lecture Notes in Computer Science*, pages 47–64. Springer, 2016.

[4] D. Ancona, A. Ferrando, and V. Mascardi. Parametric runtime verification of multiagent systems. In *AAMAS*, pages 1457–1459. ACM, 2017.

[5] A. Arsénio, H. Serra, R. Francisco, F. Nabais, J. Andrade, and E. Serrano. Internet of intelligent things: Bringing artificial intelligence into things and communication networks. *Inter-cooperative Collective Intelligence: Techniques and Applications*, page 1, 2014.

[6] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[7] M. Baldoni, Y. Sakurai, M. Dastani, B. Liao, and R. Zalila-Wenkstern. The 22nd international conference on principles and practice of multi-agent systems (PRIMA), 2019.

[8] M. Barbati, G. Bruno, and A. Genovese. Applications of agent-based models for optimization problems: A literature review. *Expert Systems with Applications*, 39(5):6020–6028, 2012.

[9] I. Benelallam, Z. Erraji, G. E. Khattabi, and E. H. Bouyakhf. Dynamic JChoc: A distributed constraints reasoning platform for dynamically changing environments. In *International Conference on Agents and Artificial Intelligence*, pages 20–36. Springer, 2015.

[10] A. Bifet, G. Holmes, R. Kirkby, and B. Pfahringer. MOA: Massive Online Analysis. *J. Mach. Learn. Res.*, 11:1601–1604, Aug. 2010.

[11] R. H. Bordini, M. Fisher, C. Pardavila, W. Visser, and M. Wooldridge. Model checking multi-agent programs with CASP. In *International Conference on Computer Aided Verification*, pages 110–113. Springer, 2003.

[12] R. H. Bordini, M. Fisher, W. Visser, and M. Wooldridge. Verifying multi-agent programs by model checking. *Autonomous agents and multi-agent systems*, 12(2):239–256, 2006.

[13] A. Botta, W. de Donato, V. Persico, and A. Pescapé. On the integration of cloud computing and Internet of Things. In *Proceedings of the 2014 International Conference on Future Internet of Things and Cloud*, FICLOUD '14, pages 23–30, Washington, DC, USA, 2014. IEEE Computer Society.

[14] J. Brynielsson, A. Horndahl, F. Johansson, L. Kaati, C. Mårtenson, and P. Svenson. Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Security Informatics*, 2(1):11, Jul 2013.

[15] D. Calvaresi, M. Marinoni, A. Sturm, M. Schumacher, and G. Buttazzo. The challenge of real-time multi-agent systems for enabling IoT and CPS. In *Proceedings of the international conference on web intelligence*, pages 356–364. ACM, 2017.

[16] R. Cao, D. G. Schniederjans, and M. Schniederjans. Establishing the use of cloud computing in supply chain management. *Operations Management Research*, 10, 02 2017.

[17] F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos, and X. Rong. Data mining for the internet of things: Literature review and challenges. *Int. J. Distrib. Sen. Netw.*, 2015:12:12–12:12, Jan. 2015.

[18] Y. Chen and H. Hu. Internet of intelligent things and robot as a service. *Simulation Modelling Practice and Theory*, 34:159 – 171, 2013.

[19] M. A. Cusumano. Can services and platform thinking help the U.S. Postal Service? *Commun. ACM*, 55(4):21–23, Apr. 2012.

[20] K. Dasgupta, B. Nilanjan, C. Dipanjan, M. Sumit, N. Seema, J. Anupam, and R. Angshu. Real-time data mining, 2017.

[21] J. DeMers. 7 ways the Internet of Things will change businesses in 2017, 2017.

[22] W. Fan and A. Bifet. Mining big data: Current status, and forecast to the future. *SIGKDD Explor. Newsl.*, 14(2):1–5, Apr. 2013.

[23] A. Ferrando, D. Ancona, and V. Mascardi. Decentralizing MAS monitoring with DecAMon. In *AAMAS*, pages 239–248. ACM, 2017.

[24] A. Ferrando, L. A. Dennis, D. Ancona, M. Fisher, and V. Mascardi. Recognising assumption violations in autonomous systems verification. In *AAMAS*, pages 1933–1935. International Foundation for Autonomous Agents and Multiagent Systems Richland, SC, USA / ACM, 2018.

[25] A. Ferrando, L. A. Dennis, D. Ancona, M. Fisher, and V. Mascardi. Verifying and validating autonomous systems: Towards an integrated approach. In *RV*, volume 11237 of *Lecture Notes in Computer Science*, pages 263–281. Springer, 2018.

[26] G. Fortino. Agents meet the IoT: Toward ecosystems of networked smart objects. *IEEE Systems, Man, and Cybernetics Magazine*, 2(2):43–47, 2016.

[27] G. Fortino, A. Guerrieri, W. Russo, and C. Savaglio. Integration of agent-based and cloud computing for the smart objects-oriented IoT. In *Proceedings of the 2014 IEEE 18th international conference on computer supported cooperative work in design (CSCWD)*, pages 493–498. IEEE, 2014.

[28] L. Gardelli, M. Viroli, M. Casadei, and A. Omicini. Designing self-organising environments with agents and artefacts: a simulation-driven approach. *IJAOSE*, 2(2):171–195, 2008.

[29] J. Gjerdrum, N. Shah, and L. G. Papageorgiou. A combined optimization and agent-based approach to supply chain modelling and performance assessment. *Production Planning & Control*, 12(1):81–88, 2001.

[30] V. Gorodetky, V. Maric, and P. Skobelev. Internet of things and internet of agents (ITIA): special session at idc 2019, 2019.

[31] J. Granjal, E. Monteiro, and J. S. Silva. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 17(3):1294–1312, 2015.

[32] F. Guerrini. Achieving high performance in the post and parcel industry, Accenture research and insights. https://www.accenture.com/us-en/insight-achieving-high-performance-post-and-parcel-industry, 2015.

[12] The Fortune 500, http://fortune.com/fortune500/, is an annual list compiled and published by Fortune magazine that ranks 500 of the largest United States corporations by total revenue for their respective fiscal years. The list includes publicly held companies, along with privately held companies for which revenues are publicly available.

[33] F. Guerrini. How big data and the Internet Of Things will change the postal service. http://www.forbes.com/sites/federicoguerrini/2014/07/03/how-big-data-and-the-internet-of-things-will-change-the-postal-service, 2015.

[34] N. Heuveldop. Ericsson mobility report, 2017.

[35] W. Ho, T. Zheng, H. Yildiz, and S. Talluri. Supply chain risk management: a literature review. *International Journal of Production Research*, 53(16):5031–5069, 2015.

[36] P. Jaeger and R. Lindenlaub. Cloud logistics, 2016.

[37] D. Jankov, S. Sikdar, R. Mukherjee, K. Teymourian, and C. Jermaine. Real-time high performance anomaly detection over data streams: Grand challenge. In *Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems*, DEBS '17, pages 292–297, New York, NY, USA, 2017. ACM.

[38] A. Jarraya, A. Bouzeghoub, A. Borgi, and K. Arour. Distributed collaborative reasoning for HAR in smart homes. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, pages 1971–1973. International Foundation for Autonomous Agents and Multiagent Systems, 2018.

[39] M. Kallman and D. Thalmann. *Modeling Objects for Interaction Tasks*. Springer, 1998.

[40] B. Karakostas. *Towards Autonomous IoT Logistics Objects*. IGI Global, 2017.

[41] J. O. Kephart and D. M. Chess. The vision of autonomic computing. *IEEE Computer*, 36(1):41–50, 2003.

[42] N.-H. Kim. Design and implementation of Hadoop platform for processing big data of logistics which is based on IoT. *International Journal of Services Technology and Management*, 23(1-2):131–153, 2017.

[43] G. Kortuem, K. Fahim, S. Vasughi, and F. Daniel. Smart objects as building blocks for the Internet of Things. *IEEE Internet Computing*, 14(1):44–51, 2010.

[44] K. Kwon, D. Kang, Y. Yoon, J.-S. Sohn, and I.-J. Chung. A real time process management system using RFID data mining. *Computers in Industry*, 65:721–732, 05 2014.

[45] P. Leitao, S. Karnouskos, L. Ribeiro, J. Lee, T. Strasser, and A. W. Colombo. Smart agents in industrial cyber–physical systems. *Proceedings of the IEEE*, 104(5):1086–1101, 2016.

[46] G. Lombardo, P. Fornacciari, M. Mordonini, M. Tomaiuolo, and A. Poggi. A multi-agent architecture for data analysis. *Future Internet*, 11(2):49, 2019.

[47] A. Lomuscio, H. Qu, and F. Raimondi. MCMAS: A model checker for the verification of multi-agent systems. In *International conference on computer aided verification*, pages 682–688. Springer, 2009.

[48] J. Macaulay, L. Buckalew, and C. Gina. Internet of things in logistics – a collaborative report by DHL and Cisco on implications and use cases for the logistics industry, 2015.

[49] B. Marsh and P. Piscioneri. The Internet of Postal Things. In *2015 International Conference on Collaboration Technologies and Systems (CTS)*, pages 3–4, June 2015.

[50] B. Marsh and P. Piscioneri. The internet of postal things, collaboration technologies and systems conference, 2015.

[51] P. Mell and T. Grance. The NIST definition of cloud computing. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, 2011.

[52] A. Meola. How IoT logistics will revolutionize supply chain management, 2016.

[53] S. Mishra. Design and evaluation of wireless and IoT based healthcare system. *International Journal of Current Engineering and Technology*, 7(2), 2017.

[54] A.-W. Mohammed, Y. Xu, M. Liu, and H. Hu. Semantical markov logic network for distributed reasoning in cyber-physical systems. *Journal of Sensors*, 2017, 2017.

[55] S. Monica, F. Bergenti, M. B. Blake, G. Cabri, and U. Wajid. Adaptive computing (and agents) for enhanced collaboration (ACEC 2018). In *WETICE*, pages 1–2. IEEE Computer Society, 2018.

[56] G. D. F. Morales. SAMOA: a platform for mining big data streams. In *WWW*, 2013.

[58] N. Noceti, L. Zini, and F. Odone. A multi-camera system for damage and tampering detection in a postal security framework. *EURASIP Journal on Image and Video Processing*, 2018(1):11, 2018.

[57] G. Neubert, Y. Ouzrout, and A. Bouras. Collaboration and integration through information technologies in supply chains. *arXiv preprint arXiv:1811.01688*, 2018.

[59] D. Palmquist and T. Leal. The IoT supply chain: 3 things you should know, 2016.

[60] P. Pico-Valencia and J. A. Holgado-Terriza. Agentification of the Internet of Things: A systematic literature review. *International Journal of Distributed Sensor Networks*, 14(10):1550147718805945, 2018.

[61] J. Rouzafzoon and P. Helo. Developing logistics and supply chain management by using agent-based simulation. In *2018 First International Conference on Artificial Intelligence for Industries (AI4I)*, pages 35–38. IEEE, 2018.

[62] G. Sabaliauskaite and A. P. Mathur. Aligning cyber-physical system safety and security. In *Complex Systems Design & Management Asia*, pages 41–53. Springer, 2015.

[63] R. Sarmiento, M. Byrne, L. Rene Contreras, and N. Rich. Delivery reliability, manufacturing capabilities and new models of manufacturing efficiency. *Journal of Manufacturing Technology Management*, 18(4):367–386, 2007.

[64] M. Schillo and K. Fischer. Holonic multiagent systems. *Manufacturing Systems*, 8(13):538–550, 2002.

[65] G. D. M. Serugendo, M.-P. Gleizes, and A. Karageorgos. Self-organization in multi-agent systems. *The Knowledge Engineering Review*, 20(2):165–189, 2005.

[66] J.-P. Su, C.-A. Wang, Y.-C. Mo, Y.-X. Zeng, W.-J. Chang, L.-B. Chen, D.-H. Lee, and C.-H. Chuang. i-Logistics: An intelligent logistics system based on Internet of Things. In *2017 International Conference on Applied System Innovation (ICASI)*, 05 2017.

[67] N. Subramanian and M. D. Abdulrahman. Logistics and cloud computing service providers? Cooperation: a resilience perspective. In *Production Planning and Control*, 2017.

[68] B. Thuraisingham, C. C. Latifur Khan, J. Maurer, , and M. Ceruti. Dependable real-time data mining. In *Proceedings of the Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing*, pages 158–165, 2005.

[69] USPS. The Internet of Postal Things. Report Number RARC-WP-15-013 https://www.uspsoig.gov/sites/default/files/document-library-files/2015/rarc-wp-15-013_0.pdf, 2015.

[70] R. R. van Lon, J. Branke, and T. Holvoet. Optimizing agents with genetic programming: an evaluation of hyper-heuristics in dynamic real-time logistics. *Genetic programming and evolvable machines*, 19(1-2):93–120, 2018.

[71] M. Vanni, S. E. Kase, S. Karunasekara, L. Falzon, and A. Harwood. RAPID: real-time analytics platform for interactive data-mining in a decision support scenario, 2017.

[72] S. K. Vickery, C. Dröge, and R. E. Markland. Dimensions of manufacturing strength in the furniture industry. *Journal of Operations Management*, 15(4):317–330, 1997.

[73] S. J. Walker. Big data: A revolution that will transform how we live, work, and think. *International Journal of Advertising*, 33(1):181–183, 2014.

[74] M. Wooldridge, M. Fisher, M.-P. Huget, and S. Parsons. Model checking multi-agent systems with MABLE. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 2*, pages 952–959. ACM, 2002.

[75] G. Yıldırım and Y. Tatar. Simplified agent-based resource sharing approach for WSN-WSN interaction in IoT/CPS projects. *IEEE Access*, 6:78077–78091, 2018.

[76] Y. Zhang, G. Zhang, J. Wang, S. Sun, S. Si, and T. Yang. Real-time information capturing and integration framework of the internet of manufacturing things. *International Journal of Computer Integrated Manufacturing*, 28(8):811–822, 2015.

[77] S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim, and S. Bianchi. ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures. In *2017 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE, 2017.