2019

Agent-based IoT Coordination for Smart Cities Considering Security and Privacy

Iván García-Magariño

Geraldine Gray

Rajarajan Muttukrishnan

See next page for additional authors

Authors
Iván García-Magariño, Geraldine Gray, Rajarajan Muttukrishnan, and Waqar Asif

Agent-based IoT Coordination for Smart Cities Considering Security and Privacy

Iván García-Magariño*, Geraldine Gray†, Rajarajan Muttukrishnan‡,Waqar Asif‡
*Dept. of Software Engineering and Artificial Intelligence
Complutense University of Madrid
Madrid, Spain
Email: igarciam@ucm.es
†Dept. of Informatics
Technological University of Dublin
Dublin, Ireland
Email: geraldine.gray@itb.ie
‡Dept. of Electrical and Electronic Engineering
City University of London
London, United Kingdom
Email: {waqar.asif,r.muttukrishnan}@city.ac.uk

***Abstract*—The interest in Internet of Things (IoT) is increasing steeply, and the use of their smart objects and their composite services may become widespread in the next few years increasing the number of smart cities. This technology can benefit from scalable solutions that integrate composite services of multiple-purpose smart objects for the upcoming large-scale use of integrated services in IoT. This work proposes an agent-based approach for supporting large-scale use of IoT for providing complex integrated services. Its novelty relies in the use of distributed blackboards for implicit communications, decentralizing the storage and management of the blackboard information in the smart objects, which are accessed by nearby requests. This avoids (a) the common bottlenecks of implicit communications based on centralized blackboards and (b) the overload of bandwidth due to explicit peer-to-peer communications. This solution raises challenges in privacy and security, and some potential solutions are discussed in this paper. Simulations based on a region in Dublin city shows the potential utility of this approach illustrated in the domain of coordination of electric vehicles in selecting paths and charging stations.**

***Index Terms*—Internet of Things; multi-agent systems; distributed blackboard; agent-based simulation; electric vehicle; smart city**

I. Introduction

Lifestyles are continuously evolving and citizens are demanding more and more complex composite services from their cities and homes. In this context, smart cities [1] and smart homes [2] are usually proposed as solutions for these up-growing demands of people. In different scales, both technologies are usually supported by the inclusion of smart objects connected to Internet, within the up-growing field of Internet of Things (IoT). Smart objects can belong to a wide range of types, such as sensors for reporting the fill-levels of waste bins [3], smart grids for proper distribution of electricity in cities [4], and road-side units (RSUs) for vehicle-to-infrastructure (V2I) communications for supporting many applications such as measurement of traffic [5].

For a customized experience of citizens and inhabitants in smart cities and smart homes, service composition [6] usually integrates the management and processing of the information from different smart objects. The scalability of composite services from IoT can become a challenge if these are widespread, assuming that smart objects may have multiple purposes. In fact, the survey of Asghari et al. [6] indicate that many of the existing composite service solutions of IoT have low scalability. In general, there are IoT solutions that depend on centralised servers [7] or require from a replicated structure with a high cost per transaction like in the existing applications of blockchain to IoT [8]. In general, there are some privacy and security challenges in IoT, as detected in the application of IoT for different purposes such as supply chains [9].

In this context, the current work proposes to use multi-agent systems (MASs) for supporting a decentralized and efficient coordination of these smart objects. In the literature, several agent-based simulators (ABSs) have shown the utility of multi-agent approaches for coordinating certain aspects of IoT. For instance, an ABS implemented a mechanism for coordinating smart vehicles with IoT guaranteeing the security with prioritization rules, vehicle certificates and trust management [10]. In addition, another ABS showed the utility of using smart beds with IoT, in which the sensors coordinated to detect sleeping postures [11]. However, none of these approaches considered a distributed blackboard for implicit communications between smart objects.

In order to achieve scalability in composite services, this work presents a solution based on applying MASs in the coordination of composite services with IoT. This solution uses implicit coordination to avoid overloading the bandwidth with peer-to-peer (P2P) communications. Instead, it only uses implicit communications with the relevant information based on edge computing for coordination using a distributed black-

We acknowledge the support from grants with references IT1/18, EP/N028155/1, 518RT0558 and TIN2017-88327-R, introduced in the acknowledgement section.

board model for avoiding the bottlenecks of centralised blackboards. This blackboard is stored and managed in IoT smart objects, which is novel to the best of authors' knowledge. In addition, this work discusses some potential solutions for maintaining security and privacy.

The remainder of this paper is organized as follows. Next section presents some works related to this research field. Section III introduces the novel approach for coordinating composite services with IoT. Section IV discusses how to maintain security and privacy in the proposed approach. Section V shows the experimentation of the current approach illustrated in the specific domain of coordination of electric vehicles (EVs) that intelligently collaborate for selecting their paths and charging stations for improving their trip time by reducing the waiting time in the queues of charging stations. Section VI mentions the conclusions and future research lines.

II. Related work

In IoT, one of the main challenges is to provide joined services by coordinating several physical things connected to Internet. This challenge is usually known as service composition, and Asghari et al. [6] presented a systematic review about possible existing solutions for this challenge. In service composition, there were usually interactions between user requirements and smart objects. Their review showed that most existing works provide ad-hoc solutions for specific applications. Embedded platforms had the highest usage, although wireless sensor network (WSN) platforms and cloud platforms were also highly used. The most common simulation environments were Eclipse platform, Matlab toolkit and Petri-net environments. MASs were useful in service composition, especially for reinforcement learning, evolutionary computation and Nash equilibrium.

In service composition, Wang et al. [12] proposed an agent-based approach for addressing service composition in an adaptive way. Their approach applied a multi-agent Q-learning algorithm for service composition, and they showed their benefits and their improvement of the Q-learning method. They used coordination equilibrium from game theory. This work assumed that all services were aimed at providing a common task ignoring the possible hindering of quality of service (QoS) when simultaneously attending several tasks. However, this system focused on composing web services rather than services of IoT smart objects.

In the field of MASs deployed with IoT, Nascimento [13] proposed the problem of addressing self-configurable systems for determining the behaviours of agents in IoT systems with environmental variability. They stated that the challenge was to predict the appropriate subset of agents that adapted not only to common feature changes but also possible unpredicted feature changes. They already had defined the Framework of IoT (FIoT) that handled IoT agents, with which they had defined four agent-based IoT applications. They were in working progress for actually solving the self-configurable approach, and their approach was presented in a doctoral consortium.

Many works support the coordination of MASs. For instance, Perez-Diaz et al. [14] proposed several game-based approaches for addressing the reduction of electricity costs in the context of EVs. Their most effective approach was based on a payment mechanism provided by the least-core. Their experimental simulated results departing from real market and driver data about Iberian Peninsula showed the feasibility of their approach.

Several platforms focus on the seamless interoperability between IoT smart devices thus proposing integration solutions for providing customized services by different sets of IoT smart objects. Some examples of these platforms are UniversAAL IoT, BodyCloud and OpenAAL. The ongoing INTER-IoT (Horizon 2020) European project is aimed at bridging the gap between some IoT platforms for supporting active and assisted living healthcare services [15]. In particular, their goal is to come up with a solution for integrating BodyCloud and UniversAAL. Their members have already developed the system INTER-Health for the rapid detection and correction of inappropriate lifestyles or critical situations.

Abtoy et al. [16] presented a survey about the platforms of IoT that are specifically aimed at supporting ambient-assisted living (AAL), considering reference models and reference architectures. In particular, they compared Amlra, Contina, FeelGood, MPOWER, OpenAAL, Persona, RAFAALS, SOPRANO, and UniversAAL. They concluded that most available platforms lacked standardization, which was considered as crucial in these kinds of infrastructure. These platforms omitted specifically dealing the data flow. They highlighted the challenge of integrating and managing all the data collected from AAL systems with their given heterogeneity.

In the context of modelling IoT, self-organizing and other complex adaptive communication networks, Laghari and Niazi [17] proposed an exploratory agent-based modelling approach that used the Cognitive Agent-based Computing (CABC) framework. Their experimental results advocated that CABC was effective for modelling complex problems in the domain of IoT. They also proposed a solution for the problem of managing carbon footprint with their approach.

There is an agent-based IoT platform for distributed real-time machine control [18]. However, this model did not included the possibility of using distributed blackboards for avoiding the bottleneck of coordination when several entities need to coordinate based on information remotely collected by sensors.

None of the aforementioned works proposed to use distributed blackboards stored and managed in IoT smart objects for achieving scalable composite services with an agent-based approach. The current work covers this gap of the literature.

III. Multi-agent approach for coordination in service composition from IoT

The challenge of comprehensively coordinating the IoT objects of a whole smart city includes solving many related problems such as scalability, security, privacy and analysis

of big data from sensors. This article proposes an agent-based solution for handling the management of IoT data in smart cities with the proper feasible coordination and adaptive learning for improving the behaviour of the whole city. In order to present this approach, section III-A presents the coordination approach with implicit communication through blackboards distributed in IoT objects, and section III-B briefly mentions other considerations related to edge computing and big data analytics for making this approach more scalable.

A. Coordination with distributed blackboards in IoT smart objects

In order to solve the coordination problem, we propose a distributed blackboard system in which the common public knowledge is distributed among the city IoT objects. In this way, IoT objects not only provide real-time and historic data from their sensors, but also allow agents to write or alter certain information with serialized synchronized access.

From a formal viewpoint, smart objects could be defined as $o_1, o_2, ..., o_N$, and these objects belong to the whole set of objects $\boldsymbol{O}$. In addition, the types of objects are defined as $t_1, t_2, ..., t_M$ and the set of types is defined as $\boldsymbol{T}$. Each object is assumed to be of one type or several types defined with the relation "is". This is formally expressed with the following equation:

$$(\forall o \in \boldsymbol{O} : (\exists t \in \boldsymbol{T} : is(o, t))) \tag{1}$$

Every type is defined with a set of properties $p_1, p_2, ..., p_N$ and a set of functionalities $f_1, f_2, ..., f_M$, and these set are available through the functions "p" and "f", so in the definition of each smart object type t_x, one would have the following definitions with equations:

$$p(t_x) = \{p_1, p_2, ..., p_N\} \tag{2}$$

$$f(t_x) = \{f_1, f_2, ..., f_M\} \tag{3}$$

In this approach, we define that the coordination is performed by a reduced set of smart object types denoted as $\boldsymbol{B} = \{b_1, b_2, ..., b_N\}$, and the developer has to select this reduced set of types from the smart object types for supporting the distributed blackboard, where consequently $\boldsymbol{B} \subset \boldsymbol{T}$.

The condition of $\boldsymbol{B}$ is that their elements have a subset of properties denoted as p_B that can be accessed by other smart object types through certain synchronized functions of the blackboard f_B for accessing and changing these properties, formalized as follows:

$$\begin{aligned}(\forall b \in \boldsymbol{B} : p_B(b) \subset p(b) \wedge p_B(b) \neq \emptyset \wedge f_B(b) \subset f(b) \wedge \\ (\forall p \in p_B(b) : (\exists f_c \in f_B(b) : change(f_c, p)) \\ \wedge (\exists f_r \in f_B(b) : return(f_r, p)))\end{aligned} \tag{4}$$

where "$change(f, p)$" indicates that the f function changes the p property in a synchronized way, and "$return(f, p)$" determines that the f function returns all or some information of the p property

In addition, the current approach proposes that some smart objects are related to the final users denoted as the set of clients $\boldsymbol{C} = \{c_1, c_2, ..., c_N\}$ so that $\boldsymbol{C} \subset \boldsymbol{O}$ for providing some composed service from several smart objects. The coordination among clients uses the distributed blackboard.

There can be exclusive conditions denoted as $\boldsymbol{E}$ that must satisfied for a given place or service managed by any $b \in \boldsymbol{B}$, then any $c \in \boldsymbol{C}$ must book the service for a given time slot $[t_i, t_f]$. The exclusive condition is guaranteed by the following formula:

$$needs(c, b, t_i, t_f) \rightarrow (invokes(c, f_x) : f_x \in f_B(b)) \tag{5}$$

where "needs" means that c needs b in the time slot $[t_i, t_f]$, and "invokes" determines that c asks for access with function f_x.

Each blackboard object must guarantee that it does not provide access to so many elements that E is not satisfied for a given time, denoted with the following equation:

$$(\nexists t' : \neg E(c \in \boldsymbol{C} : access(b, c, t_i, t_f) \wedge t' \in [t_i, t_f])) \tag{6}$$

where t' denotes any time, and $E(C')$ is evaluated as the exclusive conditions over a C' subgroup of clients and "access" indicates that a b blackboard has granted access to a c client in the $[t_i, t_f]$ time interval.

In this way, the coordination is distributed among the existing IoT smart objects, so not any single centralized point can become overloaded with considerable waiting time for synchronized writing access.

B. Edge computing and big data analytics

This approach proposes to use edge computing to avoid overloading the systems with processing units that can become bottlenecks, and limit communication payloads. For this purpose, each agent is implemented in each IoT device, and performs all the processing that can be performed locally.

To illustrate this approach, smartbands could report accidents in AAL environments, by measuring rapid decreases of altitude or acceleration peaks. In this case, neither the acceleration nor the altitude values need to be transmitted. Instead, only the fall reports would be transmitted.

In addition, more advanced customized learning processes could be implemented using parallelizable machine learning algorithms customized for machine learning in a distributed, big data environments. Each node contributes to model training, and the final, summarized learned model (represented with low amount of information) is propagated to each node for local analysis complying with an edge-based architecture [19].

IV. Security and Privacy

The proposed approach raises many security and privacy challenges, since the information is distributed among the IoT objects. These IoT objects usually lack of the appropriate firewalls and antivirus because of either their limited computing resources or their high dependency with the manufacturer, which does not include all the the necessary security measures. In addition, the privacy is challenging to be preserved since the information is continuously shared among the different devices. This work proposes some mechanisms to ensure privacy and avoid the common attacks.

A. Privacy of users

In most domains, when a user (or their agent) asks for a service in either a smart city or a smart home, they can usually reveal their location or whether they are at home. This fact implies two risks which are (a) to rob or attack the person in the most convenient circumstances, or (b) burglar their house when the user is not at home.

In order to avoid the lack of privacy, in this approach the information is pseudo-anonymised, and the IoT objects only save a value obtained with a hash function from certain user features including some information only known by the user as a part of their password. In this way, when a user requests and claims their service, they send this hash value. However, any IoT object or any man-in-the-middle attack in communications cannot know the identity of the user, since the hash value is not useful for getting back to the original values [20].

In addition, all the communications are recommend to be encrypted with asymmetric encryption for establishing a secure channel for exchanging a shared key. Then, IoT objects can use symmetric encryption with this shared key for each session.

B. DoS attacks

The Denial of Service (DoS) is one of the most common attacks. In this approach, DoS would be to request a service more than necessary so that an IoT object gets overloaded, and other users cannot get the service. For example, in the case of electric vehicle (EV) charging stations, this approach could be very vulnerable, because if a user books all the slots of a day, then no one would be able to use this charging station for the whole day.

In order, to avoid this attack, we propose that each person can be only registered once. Thus, every time a user wants to start using this framework, they first have to start a session in a trusted service indicating its valid identification, and the system would store the corresponding hash value without any link to the original user. In this way, every charging station can corroborate the real identity of a user, but we avoid that a person can use different identities to overload a charging station.

In addition, each charging station only allows that each person can have an active booking, so if someone tried to perform a second booking before actually using the first booking, the system would ignore the second request.

Moreover, each IoT object will have a record to establish trust on each person. If someone books a time slot and then it does not use it without a justified reason, then the IoT object decreases the trust on this person. On the contrary, if a person uses its booked slot, then the IoT object increases its trust on them. From time to time, the IoT objects will share their trust values of users so that the whole distributed system considers the reputation of the users. In this way, if a person starts trying performing DoS attacks, the system will detect them by this trust and reputation mechanism.

C. DDoS attacks

The Distributed DoS (DDoS) is a variant of the DoS attacks, in which several attackers coordinate to simultaneously request a service to a given target. The security measures indicated in the previous section can prevent most of these attacks by for example eventually detecting the common attackers with the trust mechanism. The proposed authentication mechanism also reduces the possibility of creating many identities to perform this attack.

Nevertheless, we could assume that an attacker may achieve a high number of identities and these can be coordinated to ask for a given service. For example, the attacker could compromise several objects (e.g. EVs) and then use these objects to perform the attack. They could also steal the pseudonym identities (i.e. hash values), and use these to perpetrate the attack.

In order to defend from DDoS, we recommend to analyse the patterns of service requests with artificial intelligence (AI) techniques, when there is a dataset of known attacks, in which the corresponding machine learning (ML) algorithms will train with the existing attacks and normal activity to learn to classify the requests. In particular, neural networks, support-vector machines and k-nearest neighbours are examples of ML algorithms that can work properly.

Since, each IoT object only has a very partial information and to be able to apply ML techniques, the IoT objects will share summarised information to collectively conform datasets that can properly train ML algorithms.

This approach also recommends to use novelty detectors, which are able to detect novel patterns when using a service, even when knowing a very partial observable environment [21]. In this way, the IoT objects can detect strange patterns of requesting services and mark them as possible attacks.

D. Thief of identity

Another attack can be to steal pseudonym identities by intercepting the corresponding hash value, and using them without the authorisation of the owner. This could be done by either compromising the communications or hacking into one of the IoT service provider. The attacker could use this for later performing a DDoS attack for example or any other attack covering their traces.

This approach proposes to apply two security measures. First, all the communications will be encrypted using asymmetric encryption for establishing the channel and then the symmetric encryption as previously introduced before in section IV-A.

Another possibility to prevent this attack is to use a hash function instead of a hash value for the authentication. In this way, the service provider will indicate a value and then the user will return the transformed value returned by the hash function. It would be like a table of keys, in which the identity thief would only able to steal a key in each communication interception, but could not use the service unless they have a representative group of keys, so in this way identity thief could be further prevented.

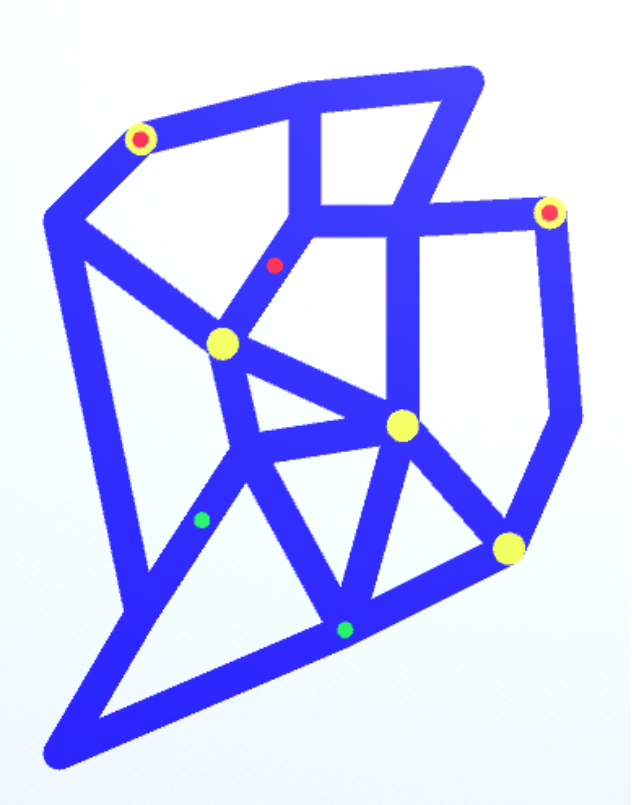

Fig. 1. Simulation of EVs that stop in charging station using a distributed blackboard mechanism

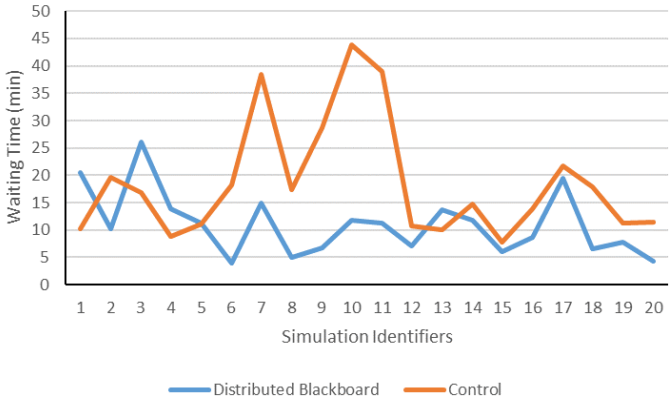

Fig. 2. Comparison of waiting times between the system with the distributed blackboard and the control system

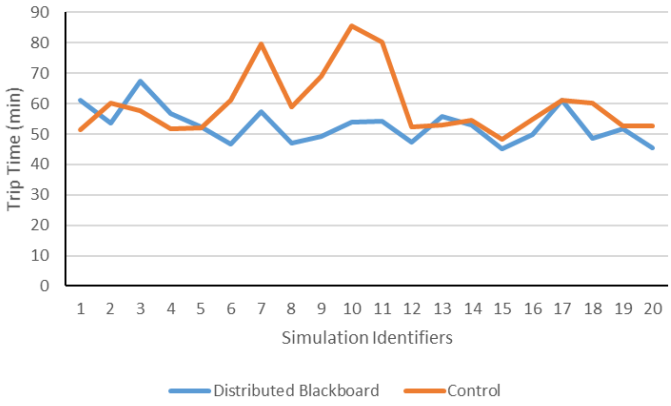

Fig. 3. Comparison of trip times between the system with the distributed blackboard and the control system

V. Experimental evaluation

The current approach is illustrated with the coordination of EVs in which IoT smart objects are placed in charging stations. These smart objects not only have information about whether an EV is currently charging, but also allow EV to book certain time slots in advance. In this manner, charging station smart objects handle bookings indicating available slots to EVs, and ensuring that these booked slots do not overlap in time for the same charging point. In this way, EVs can plan their routes in order to reduce the waiting times. This is achieved by considering available slots on each potential route, and booking the slot that results in minimising total trip time. This application domain is experimented with an ABS.

Figure 1 shows a simulation of the coordination of EVs with a blackboard distributed in the agents representing charging stations. We defined a new map inspired by some of the main streets and charging stations of Dublin. We used our simulator ABSCEV (an ABS about Charging EVs) [22] for illustrating the current approach. In ABSCEV, the lines represent roads, the big circles represent charging stations, and the small circles represent EVs. Red circles represent EVs that have low energy-levels in their batteries, while green circles represent vehicles that have high energy-levels, because they have recently charged their vehicles on their way.

We compared the system with the distributed blackboard coordination system and a similar one where EVs just selected the shortest path without using the distributed blackboard system. We executed 20 simulations with each alternative.

Figure 2 represents the comparison of waiting time. The distributed blackboard system obtained 11.0 min in average in comparison with 18.6 min to the control mechanism. This represented a reduction of 40.6% in waiting time. In the worst case, the proposed approach obtained only 26.1 min compared to 43.9 min of the control case.

Figure 3 compares the trip time of the used alternatives. In the simulation with the distributed blackboard, the average trip time was 52.8 min, while the control system averaged 59.9 min. The worst case of the proposed mechanism obtained 67.4 min while the worst case of the control mechanism was 85.5 min, showing a reduction of 21.2% in the worst case.

Therefore, the current approach shows that effectively coordinated EVs with a distributed blackboard for reducing both the waiting times in charging stations and the whole trip time in EVs that need to be recharged.

VI. Conclusions and future work

This work has proposed to exploit a distributed blackboard coordination mechanism for creating scalable agent-based IoT systems. For this purpose, IoT smart objects store blackboards in a distributed way for achieving an effective implicit coordination among agents. One of the keys for achieving successful systems with this approach is to properly distribute the information so that only small group of agents simultaneously access to the same node. This work discussed some mechanisms to ensure security and privacy in the systems following this approach. This work has illustrated this approach with a case study, with an implemented ABS about coordination of EVs for reducing waiting times in charging stations. The experimental results with the case study show the feasibility of the current approach.

Our future work includes to look for European funding for developing fully AAL systems in smart homes with this approach for supporting both the assistance and the continuous evaluation of elderly people, especially the ones with neurological diseases such as Alzheimer‘s disease. In addition, we plan to use this MAS based coordination mechanism of IoT for implementing new mechanisms of human-centric AI techniques to detect cyberattacks over IoT systems automatically generating explanations associated with these detections, so that human can easily understand the reasons and either corroborate or refute the attack detections.

Acknowledgement

This work was mainly done during (a) the research stay of the first author in the Institute of Technology Blanchardstown (now integrated into the Technological University of Dublin) in 2018 with support from “Universidad de Zaragoza”, “Fundación Bancaria Ibercaja” and “Fundación CAI” in the “Programa Ibercaja-CAI de Estancias de Investigación” with reference IT1/18, and (b) the research stay of the first author in the City University of London in 2019, supported by this university with the research budget associated to Rajarajan Muttukrishnan (third author). The latter stay and the presented research were supported through UK Engineering and Physical Sciences Research grant number EP/N028155/1. We also acknowledge “CITIES: Ciudades inteligentes totalmente integrales, eficientes y sotenibles” (ref. 518RT0558) funded by CYTED (“Programa Iberoamericano de Ciencia y Tecnología para el Desarrollo”) and “Diseño colaborativo para la promoción del bienestar en ciudades inteligentes inclusivas” (TIN2017-88327-R) funded by the Spanish council of Science, Innovation and Universities from the Spanish Government.

References

[1] R. W. S. Ruhlandt, “The governance of smart cities: A systematic literature review,” *Cities*, vol. 81, pp. 1–23, 2018.

[2] J. Shin, Y. Park, and D. Lee, “Who will be smart home users? an analysis of adoption and diffusion of smart homes,” *Technological Forecasting and Social Change*, vol. 134, pp. 246–253, 2018.

[3] T. R. P. Ramos, C. S. de Morais, and A. P. Barbosa-Póvoa, “The smart waste collection routing problem: Alternative operational management approaches,” *Expert Systems with Applications*, vol. 103, pp. 146–158, 2018.

[4] M. Faheem, S. Shah, R. Butt, B. Raza, M. Anwar, M. Ashraf, M. A. Ngadi, and V. Gungor, “Smart grid communication and information technologies in the perspective of industry 4.0: Opportunities and challenges,” *Computer Science Review*, vol. 30, pp. 1–30, 2018.

[5] M. Hoeft and J. Rak, “How to provide fair service for v2i communications in vanets?” *Ad Hoc Networks*, vol. 37, pp. 283–294, 2016.

[6] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, “Service composition approaches in iot: A systematic review,” *Journal of Network and Computer Applications*, vol. 120, pp. 61–77, 2018.

[7] P. Ferreira, R. Martinho, and D. Domingos, “Iot-aware business processes for logistics: limitations of current approaches,” in *INForum:*, 2010, pp. 611–622.

[8] A. R. Rao and D. Clarke, “Perspectives on emerging directions in using iot devices in blockchain applications,” *Internet of Things*, p. 100079, 2019.

[9] T. Omitola and G. Wills, “Towards mapping the security challenges of the internet of things (iot) supply chain,” *Procedia Computer Science*, vol. 126, pp. 441–450, 2018.

[10] I. García-Magariño, S. Sendra, R. Lacuesta, and J. Lloret, “Security in vehicles with iot by prioritization rules, vehicle certificates and trust management,” *IEEE Internet of Things Journal*, vol. https://doi.org/10.1109/JIOT.2018.2871255, 2018.

[11] I. García-Magariño, R. Lacuesta, and J. Lloret, “Agent-based simulation of smart beds with internet-of-things for exploring big data analytics,” *IEEE Access*, vol. 6, pp. 366–379, 2018.

[12] H. Wang, X. Chen, Q. Wu, Q. Yu, X. Hu, Z. Zheng, and A. Bouguettaya, “Integrating reinforcement learning with multi-agent techniques for adaptive service composition,” *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 12, no. 2, p. 8, 2017.

[13] N. Nascimento, “A self-configurable iot agent system based on environmental variability,” in *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 2018, pp. 1761–1763.

[14] A. Perez-Diaz, E. Gerding, and F. McGroarty, “Coordination of electric vehicle aggregators: A coalitional approach,” in *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 2018, pp. 676–684.

[15] P. Pace, R. Gravina, G. Aloi, G. Fortino, G. Ibanez-Sanchez, V. Traver, C. Palau, D. Yacchirema *et al.*, “Iot platforms interoperability for active and assisted living healthcare services support,” in *Global Internet of Things Summit (GIoTS), 2017*. IEEE, 2017, pp. 1–6.

[16] A. Abtoy, A. Touhafi, A. Tahiri *et al.*, “Ambient assisted living system’s models and architectures: A survey of the state of the art,” *Journal of King Saud University-Computer and Information Sciences*, vol. https://doi.org/10.1016/j.jksuci.2018.04.009, 2018.

[17] S. Laghari and M. A. Niazi, “Modeling the internet of things, self-organizing and other complex adaptive communication networks: a cognitive agent-based computing approach,” *PloS one*, vol. 11, no. 1, p. e0146760, 2016.

[18] A. Rivas, P. Chamoso, and S. Rodríguez, “An agent-based internet of things platform for distributed real time machine control,” in *Ubiquitous Wireless Broadband (ICUWB), 2017 IEEE 17th International Conference on*. IEEE, 2017, pp. 1–5.

[19] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, “Urban planning and building smart cities based on the internet of things using big data analytics,” *Computer Networks*, vol. 101, pp. 63–80, 2016.

[20] M. Naor and M. Yung, “Universal one-way hash functions and their cryptographic applications,” in *Proceedings of the twenty-first annual ACM symposium on Theory of computing*. ACM, 1989, pp. 33–43.

[21] S. E. Marzen, “Novelty detection improves performance of reinforcement learners in fluctuating, partially observable environments,” *Journal of theoretical biology*, vol. 477, pp. 44–50, 2019.

[22] I. García-Magariño, G. Palacios-Navarro, R. Lacuesta, and J. Lloret, “Abscev: An agent-based simulation framework about smart transportation for reducing waiting times in charging electric vehicles,” *Computer Networks*, vol. 138, pp. 119–135, 2018.