IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received August 15, 2018, accepted October 8, 2018, date of publication October 24, 2018, date of current version November 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2877175

Internet of Too Many Things in Smart Transport: The Problem, The Side Effects and The Solution

LINA XU AND GAVIN MCARDLE
School of Computer Science, University College Dublin, Dublin, Ireland
Corresponding author: Lina Xu (lina.xu@ucd.ie)

ABSTRACT The Internet of Things (IoT) involves embedding electronics, software, sensors, and actuators into physical devices, such as vehicles, buildings, and a wide range of smart devices. Network connectivity allows IoT devices to collect and exchange data. The prevalence of IoT devices has increased rapidly in last five years, driven by cheaper electronics and a desire to monitor and control the physical world. We introduce the concept of IoT flood to describe the increased use of IoT devices. Just like the data deluge, the IoT flood has potential benefits and risks. This paper focuses on the hidden side effects of the increased usage of IoT, such as energy consumption, physical pollution, radiation, and health issues. We indicate that an evaluation system with carefully designed metrics reflecting the impact of IoT flood with input from academic, industry, and government is required. We propose some practical measures that can reduce the IoT flood, such as common platforms and data sharing to reduce the side effects. This paper demonstrates the IoT flood problem and potential solutions by examining the intelligent transport system domain where IoT is being deployed to solve problems related to time efficiency and energy consumption through smart mobility.

INDEX TERMS CO_2 emissions, energy efficient, Internet of Things, intelligent transportation system, IoT flood.

I. INTRODUCTION

In its most basic form, the Internet of Things (IoT) is built on a network of distributed micro-devices embedded with various sensing abilities, which are used to monitor the environment and send the information between devices and end users. This network is often referred to as a Wireless Sensor Network (WSN). WSN technologies were introduced more than 20 years ago and many projects have been proposed and undertaken that embrace this technology. WSNs have proved popular due to their simple design, implementation, deployment and usability. This has allowed IoT to evolve with a high diversity of uses which extend beyond sensing abilities to include actuators which can control aspects of the environment. IoT has been extremely popular and the corresponding systems are widely deployed to assistant people's everyday life.

IoT technologies have been and will be deployed in many scenarios to provide better services and support advanced management, scaling from smart home to smart cities. Applied IoT Technology can be seen in industrial predictive maintenance, connected health and translational medicine, smart transportation, asset tracking, smart cities and many other instances. For example, in the Intelligent Transport System (ITS) domain, IoT contributes to smart parking, autonomous vehicles, smart traffic control, smart routing, traffic light sequencing, smart road lighting, bike sharing and public transportation. It is likely, the uses of IoT in this domain will increase further as new application cases are proposed. The use of IoT in ITS demonstrates the quantity of IoT devices within a single domain. Although there are overlapping use cases, problems and solutions, typically new IoT devices and systems are deployed for each solution. There is no connected infrastructure or attempt to share of resources and data. Many other domains have also adopted IoT as a means to solve their problems. It has already been estimated that there will be over 50 Billion IoT devices operating within the next 3 years [1]. Therefore, we can see that the volume of IoT devices will be extremely large and this will lead to the IoT Flood problem in the near future.

As the proliferation of IoT within the single domain of ITS has demonstrated, it is now time for us to step back and carefully examine current IoT deployment and question the problems that the IoT flood introduces while we propose ways to prevent the flood advancing. This is particularly relevant given that Gartner has predicted that IoT is currently in the peak inflated expectation in the Hype Cycle for Emerging

Technologies 2017 [2]. The inflation will continue to increase and then dynamically drop due to realization on reality that IoT is not the panacea to solve all of the world's problems. However, the deployed physical IoT systems cannot be easily recycled after the drop. The question is: do we need so many systems and what are they actually going to bring to us?

Many of the IoT systems in smart transportation, aim to increase time and energy efficiency of existing systems while also reducing the environmental impact (e.g. CO_2 emissions) of the transportation sector. In Europe, Transport is the only major sector where CO_2 emissions are rising and so it is important to examine ways to do this. Even though IoT and smart technologies can improve this situation, we still need to be cognizant of the environmental impact of IoT itself.

Many studies have been conducted to reduce power consumption in individual IoT devices or at the system network level, such technologies include smart network selection [3], intelligent sleeping scheduling for sensors [4] and energy efficient routing for networks [5]. Few approaches are focusing on a broader scale crossing multi-systems. The percentage use of electricity by IoT systems in the whole picture remains unclear. With the explosion of connected devices, the associated energy cost is unpredictable [6], since it is not only depending on the quantity, but also the sensor types, operating frequency and other factors which can be highly dynamic in IoT.

In isolation, individual IoT devices are not generally big consumers of energy, however given that IoT devices will number 50 billion by 2020, collectively they are a large consumer of electricity. The problem is recognized by manufacturers of IoT hardware who have introduced protocols and technologies to support energy efficient communication. Techniques to reduce power consumption on those devices, even just 1% on, can make a huge impact considered globally. If we consider that the sources of the electricity can be from gas or coal, electricity efficiency can contribute to the reduction of CO_2 emissions even more. This is the motivation for many related studies in this direction.

The massive deployment of IoT devices will also cause electrical pollution. While we are more conscious and aware of water, air, light and land pollution, which are directly affecting our daily life, electrical pollution is also impacting our environment as obsolete devices are dumped. Wide scale deployments of IoT may cause heavy radiation in the air and potentially controversial health concerns.

Many IoT deployments are made to support sustainable development by monitoring environmental conditions. However there is a danger that IoT deployments are contributing to pollution and delivering unintended consequences. There is therefore a need to balance the number of IoT devices without undermining the Quality of Service (QoS) and Quality of user Experience (QoE) of an IoT deployment. This article reviews existing work in this area and describes the current stage of IoT platforms, followed by problem statement in the current state of art work. A novel solution is proposed to reduce the quantity of IoT devices while still maintaining the QoS through a connected IoT infrastructure. The solution is comprised of a technological framework that supports the sharing and reuse of IoT devices and the data they collect in a more complete scale. In addition, we propose methodologies, policies, standards and guidelines to curb the IoT flood by encouraging reuse and sharing of IoT infrastructure and data. ITS is used as a case study.

II. EMERGING PROBLEMS WITH IoT DEVELOPMENT

The technology evolution from WSN to IoT has enabled IoT systems and applications to flourish. IoT has greatly changed the traditional ways of managing and monitoring, which has become an attractive potential solution for many problems. However, heavily developing IoT systems without control can be harmful and cause unanticipated and controversial issues.

A. THE EVOLUTION FROM WSNs TO IoT

A WSN is a network composed of autonomous wireless micro-devices, which can monitor the surrounding environment, record the data and transmit the information back to a central server or to the cloud [7], [8]. WSNs were originally proposed for military surveillance purposes [9]. Due to its early success, this technology was re-purposed for tasks such as habitat monitoring [10], weather monitoring [11], agriculture monitoring [12] and wildlife monitoring [13]. WSN technologies were introduced more than two decades ago and many projects have been proposed and undertaken since then. However, due to the complexities associated with establishing and maintaining WSN, only limited usages and applications were available to the public.

Reference [14] has suggested that a similar and successful paradigm to compare WSN against is the case of the Internet. The original Internet was invented in the late 1960s. However, it did not become universally popular until 1995 when the Internet access was more free and convenient. The number of Internet users has increased impressively for the last decade owing to numerous simple to use Over-the-Top (OTT) applications developed over it, such as World Wide Web, electronic mail and social networking.[1] The Internet has brought great convenience to society and its importance is self-evident.

In a similar way, as the number of applications of WSNs or more specifically IoT increases, the popularity of the technology will improve, which will encourage more IoT devices and services. There are several differences between WSNs and IoT and the most fundamental one is that the dynamics and diversities in IoT are much higher than that in WSNs. For example, traditional WSN applications are mainly focusing on monitoring the environment and collecting the field information. However, IoT applications can range from smart kitchen to smart city monitoring. The scale of IoT systems is normally much larger and involves multiple aspects simultaneously. A smart city system may be

[1] http://www.internetworldstats.com/stats.htm

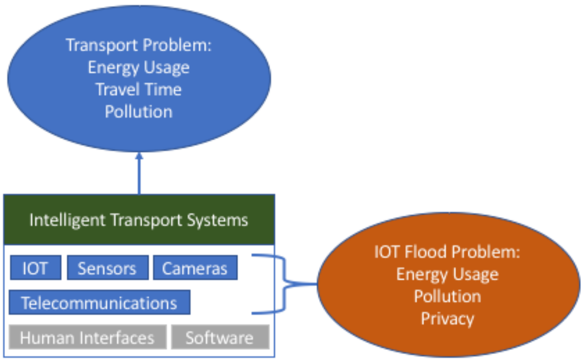

FIGURE 1. **IoT flood: A case analysis for ITS.**

composed of millions of IoT devices to monitor buildings, roads, people, environment, and traffic. To account for the proliferation of sensors and devices, the concepts of Internet of Things (IoT) [15] and Internet of Everything (IoE) [1] were proposed and currently they are widespread and popular in many fields (e.g. connected health, intelligent transport and travel, environmental monitoring) leading to a proliferation of devices.

B. IoT FLOOD

We propose the term ''IoT flood'' to describe the current situation of IoT. The IoT devices and the infrastructures are like water, permeating our living environment even without our awareness. The IoT flood is a result of a perfect storm. The increase in IoT devices has been supported by decreases in manufacturing costs, improvements to the reliability and accuracy of sensors and communication technology as well as cheaper data storage and communication costs. Simultaneously an ability to process *Big Data* efficiently has emerged. This has led IoT systems to be deployed for many uses by industry, individuals and governments. Rivers, farmland, forests, oceans and urban environments are at risk of the IoT flood as new IoT systems are deployed to monitor and act in diverse situations.

While the predictions for the number of IoT devices differ, all sources agree the number of devices will be large. For example, Gartner Research [16] has an expectation to see 20 billion IoT devices by 2020. Statista[2] shows that by 2020, the installed base of the IoT devices is forecast to grow to almost 31 billion worldwide and reach 75 billion by the end of 2025. Cisco [1] has also predicted that there would be 50 billion IoT devices by 2020. All different sources have strong confidence that the number of IoT devices will be extremely large and the total number is expected to keep increasing.

If IoT systems are well managed, they can contribute to our environment and improve our daily lives. However, if there is a free-for-all in terms of deployment anywhere, the number of IoT deceives can quickly grow out of control and they will in many cases not fulfill their designed goals. For example, many IoT systems aim to reduce power consumption of other systems, however, the energy use of the IoT deceives is variable and is dependent on the type of the sensors, the frequency of sampling and the communication chip. This hidden power consumption for constructing and running an IoT system is still not clear. For example, industry proponents suggest that emerging connected home technologies could help households reduce their energy bills by 10-25%. However, social research from Australia and the UK is revealing the possibilities that IoT systems might also increase energy demand.[3] Limited IoT systems have addressed this issue in their research since a complete evaluation metric system and platform is still missing. Many approaches have been proposed to support energy efficient communication, only focusing on wireless transmission layer. With the IoT flood coming, the power consumption to support the system will be hugely increased in the next decade unless action is taken. For example, according to Sandhi Bhide, Intel's director of innovative IoT solutions, in 2012 there were approximately 75 million vehicles shipped with an average of 80 sensors in each vehicle, equaling 6 billion sensors total. If the average wattage of power per sensor is 1 watt, this means that 6000 megawatt-hours are consumed by these sensors. In 2020, it is expected that 110 million vehicles will be delivered with 200 sensors per vehicle, which equates to 22 billion sensors in auto mobiles alone consuming an estimated 22,000 megawatt-hours.[4] 22,000 megawatt-hours is equivalent to 17.8 million energy customers (the population of Shanghai) – just to power sensors in auto mobiles. Currently, electricity has become a key commodity for modern societies. At the same time, it had a destructive impact on the environment because of increasing energy generation from the fossil fuels rather on improving its efficiency and the related CO_2 increases contributing to global warming [17]. If left unchecked, IoT devices without proper management can further sabotage our environment through electrical pollution.[5] Electrical pollution is the pervasiveness of obsolete electrical items which are not recycled. It is estimated that a computing device becomes obsolete after 3 - 4 years due to advances in technology which means the device needs to be replaced. Without proper management this could be a serious problem for the billions of IoT devices which will be in operation in 2020. The next section explores these unintended consequences associated with IoT deployment in the Transportation sector.

III. INTELLIGENT TRANSPORTATION SYSTEMS (ITS)

Intelligent Transportation Systems (ITS) involve the use of technology to support more efficient, reliable and sustainable transport. While the term can be applied to any mode of transport, ITS is most commonly used in relation to road

[2]https://www.statista.com/

[3]https://theconversation.com/the-hidden-energy-cost-of-smart-homes-60306

[4]https://newsroom.intel.com

[5]http://www.ecopolitan.com/

transport (freight, public transport, private cars, bikes, etc.). At its core, an ITS consists of sensors which collect data about current conditions and software and algorithms which process the data to make decisions or in many cases to inform a human in the loop to enact decisions.

IoT deployment within ITS is common, so this section highlights the IoT flood and associated consequences within this single domain. Firstly, the background and current state of IoT-based ITS and smart mobility is presented. Then the reasons behind the IoT flood in ITS is revealed. The problems are only now emerging and so the solutions are still missing.

A. ITS AND SMART MOBILITY

In addition to the direct costs of road transport (fuel, insurance and infrastructure), indirect costs are prevalent and increasing. Reference [18] has indicated that inefficiencies in transportation can cause significant losses of time, decrease in the level of safety for both vehicles and pedestrians, create high pollution, lower quality of life, and waste non-renewable fossil energy. The time lost to road users due to congestion runs into the billions. For example, in New York City, congestion cost $33 billion in 2017.[6] Activity in road transport has an environmental cost too. Road transport contributes about one-fifth of the EU's total CO_2 emissions – the main greenhouse gas. Transport is the only major sector in the EU where greenhouse gas emissions are still rising.[7]

ITS and smarter travel have been proposed to address poor time and energy efficiency problems in traditional transportation and mobility. In particular, an IoT deployment that can sense current traffic conditions and provide adaptations is of interest to researchers and city planners. The IoT devices can range from a simple induction loop to count vehicles to video and bluetooth detectors for activities. In-vehicle sensors can also determine the vehicle speed and the surrounding environmental conditions.

When such sensors are part of a common communication platform, the data can be used within traditional transportation control and management and enable traffic information exchanging and analysis. Due to the attractive features that ITS can provide, many applications and systems have been developed. For example, Schneider Electric Solutions[8] aim to provide integrated solutions for smart mobility. With the help of highly developed machine learning and deep learning technologies and the increased availability of data, based on traditional ITS, smart mobility has been proposed and become the trend [19], [20]. Smart mobility is mostly based on data driven designs and focuses on behavior analysis and future prediction [21]–[23]. It will further advance ITS by gaining predictive analysis and smart coordination features. Depending on the system scale, the prediction and coordination can be optimized for a local neighborhood, a city or even at a country level. In Europe, the European Commission has been pushing the ITS implementations and developments. It also features smart transport as a major theme in its calls for research proposals.[9] As a result, a plethora of ITS projects led by both academics and industry partners has emerged. A search of the EU Community Research and Development Information Service (CORDIS) shows over 120 distinct projects with the keyword Intelligent Transport which have received funding from the European Commission (https://cordis.europa.eu/). Within the Irish context, many ITS projects have been proposed to encourage and enable greener transportation in Ireland such as [24]–[26], aiming to provide comprehensive information for users and also to assist smart transportation and decision making. Smarter Travel [27] is the transport policy for Ireland that sets out how the vision of a sustainable travel and transport system can be achieved. Transportation Infrastructure Ireland (TII) [28] supports several projects to improve the efficiency of the public transportation and national roads. All the projects are fully or partially funded and supported by the Irish government.

B. PROBLEMS FOR ITS SYSTEMS

The pressure to solve transport problems is being promoted by local and national governments as well as the European Commission and is contributing to the IoT flood and associated problems described in Section 2.2. The situation is likely to deteriorate without proper effective control and interventions. Many studies, efforts and resources have been dedicated to the development for ITS and smart mobility. Even though many existing systems are supported and funded by the EU and national governments, there is limited interaction between projects. While there is a common vision to achieve more efficient and sustainable road transport, there is no common IoT infrastructure in place or proposed. Therefore, each project must deploy new IoT devices to address their particular part of the wider transportation and travel problem. Below we highlight how this push for smarter travel has led to IoT flood in ITS.

1) LIMITED INNER AND INTER SYSTEM INTERACTION

We have investigated several ITS developed in the international and Irish market ([24]–[28]). A common drawback in existing work is that they rarely have designed an interface to interact with other ITS. This drawback makes platform and real-time data sharing impossible. For example, if a smart bus system wants to get information for road traffic from existing smart road system, without pre-designed interfaces, it will create extra work as each ITS needs to deploy their own set of IoT devices to collect the data. When the system scales up, it can be expected that more devices will be required to meet users needs.

In addition to limited inner (among ITS) interactions, there are limited considerations on inter system interactions with

[6] https://www.economist.com/graphic-detail/2018/02/28/the-hidden-cost-of-congestion

[7] https://ec.europa.eu/clima/policies/transport/vehicles_en

[8] https://www.schneider-electric.ie/en/work/solutions/

[9] https://ec.europa.eu/transport/themes/its_en

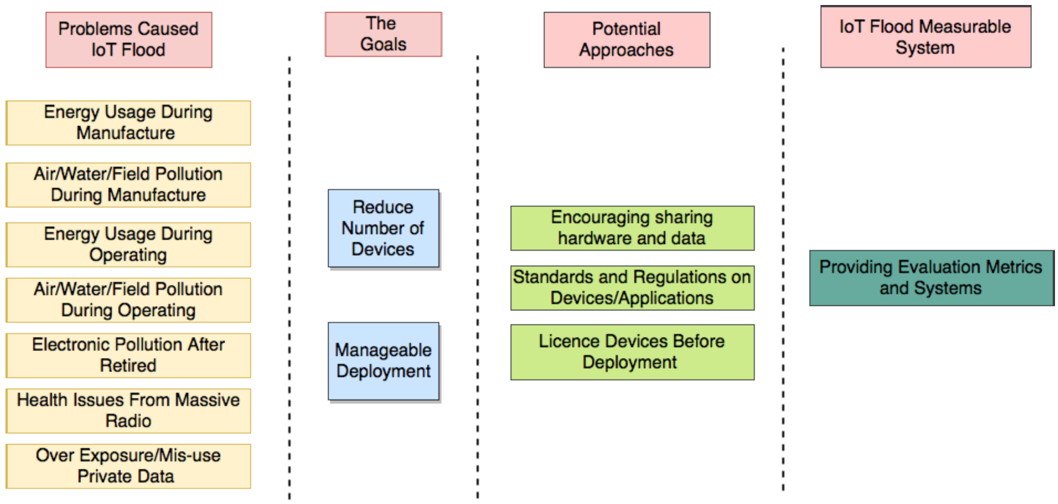

FIGURE 2. The problem caused by IoT flood and possible approaches to achieve the solutions.

other IoT domains. For example, little interest has been shown for the intention to share hardware, software or data with other smart systems, for example, between ITS and smart health. When proposing novel systems, few researchers have considered a mechanism to integrate with other smart systems which could reduce redundancy, lead to fewer IoT devices and provide more data. For many cases, those integration and collaborations between different ITS or other smart systems can greatly improve the overall QoE. For instance, an ambulance in a smart health system should be able to integrate with an ITS in order to determine the most efficient route to travel.

2) LIMITED RE-USABILITY

The limited interaction between systems can also limit hardware and data reuse and contribute to the global IoT Flood. Within ITS, if any information is unknown for a given system, a new IoT deployment is most likely required in order to collect it. Limited research has utilized existing hardware platforms for the purpose of reuse within new or existing domains. Hardware re-usability in current ITS is low. This results in new deployment whenever there is a new system proposed and a waste of a large number of devices when a system is retired.

C. NO ANTICIPATION FOR IoT FLOOD

The fundamental reason for the problems in ITS is that when designing and evaluating a system, IoT flood and the associated unintended consequences are not considered.

If we can

1) Solve the limited inner and inter system interaction problem, we can improve the utilization rate of each IoT system.
2) Solve the limited re-usability concern problem, we can improve lifetime of IoT system and delay device retirement.

Each of these solutions can significantly contribute to the prevention of the negative impact of IoT flood. In the next section techniques to achieve these solutions in the wider IoT domain are proposed.

IV. SIDE EFFECTS OF IoT FLOOD AND SOLUTIONS

We have introduced the concept of "IoT flood" in Section II-B to describe the dramatic increasing quantity of the IoT devices in the near future and the problems that we will be facing as the number of devices increases to a level where control is difficult or impossible. Figure 2 summarizes the problems and potential solutions.

In this section, firstly we further discuss the side effects of the IoT flood beyond just the quantity. Then we propose possible approaches to solve the IoT flood problem, including encouraging platform and data sharing, providing standards and regulations, supervising the development of IoT systems and giving licenses to the permitted devices in the market. In order to lead the market to the expected direction, a system with comprehensive evaluation metrics should be provided. Such a system should be able to provide insights and awareness for IoT system designers and developers to observe whether their system would cause an IoT flood problem and also help them to understand the impact of the side effects.

A. SIDE EFFECTS OF IoT FLOOD

Figure 3 has presented an overview of the causation for IoT flood and the side effects it may generate. We are living in a world where IoT devices are massively deployed for many purposes and a clear trend has shown that the number will continue grow in the next decade. This situation, as we already described, is considered as the IoT flood. The side effects along with it are discussed herein.

1) ENVIRONMENTAL PROBLEMS

Many IoT systems, especially in the ITS domain have been proposed to improve environmental sustainability by

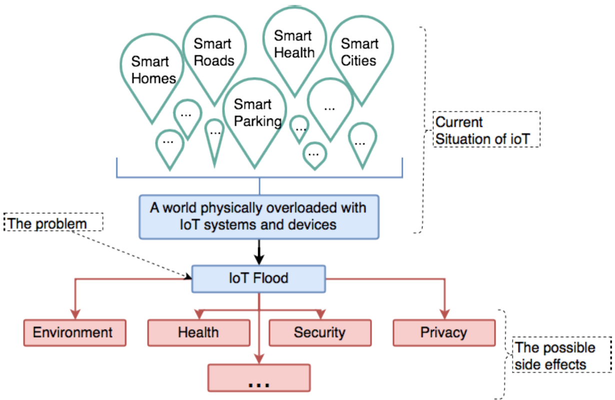

FIGURE 3. The causation of IoT flood and possible side effects.

monitoring CO_2 emissions to highlight and address urgent environmental problems. The time and fuel saved by an IoT based ITS in transportation is the primary criterion used to evaluate the system's success. However, the environmental cost of IoT deployment is not typically considered. For example, energy usage and air/water field pollution during manufacturing, energy usage/water field pollution during operation and electronic pollution caused after retirement should all be discussed and measured as part of the impact of IoT deployment. In reality, the hidden side effects that the IoT flood brings can be easily neglected.

The environmental problems caused by the IoT flood are currently critical and urgently requiring a solution. According to the Eurostat,[10] household, manufacturing and transportation are the largest contributors to CO_2 emission in Europe. IoT devices are prevalent in all of these domains and manufacturing those devices to cater for an increasing demand can result in more CO_2 emissions.

2) HEALTH CONCERNS

In order to support full wireless coverage of IoT networks, a large amount of a network access points such as WiFi, 4G and 5G will be deployed. The large deployment of wireless IoT devices and the network infrastructures to support them will create heavy radio signals in the air. There are many discussions and opinions regarding to the health risk posed by exposure to such a dense radio signal environment [29]. The industry has developed standards and rules to regulate the market from a health and safety perspective [30], [31]. The World Health Organisation (WHO)[11] has organized workshops to understand and discuss the risks of base station and wireless network exposure.[12] While some others, for example GSMA has indicated that the evidence that mobile phones or wireless networks could pose a health risk to humans or the environment has become increasingly weaker.[13] The related health concerns frequently draw people's attention and fade out but should be considered within IoT deployment.

3) SECURITY CONCERNS

IoT poses a risk to security and privacy to users and IoT flood will exacerbate this. Typical IoT devices are in charge of sensing the environment and collecting the data. There is a risk that the devices can be hacked or the data can be intercepted if secure communication channels are not utilized. Those IoT devices can create serious damage if controlled by attackers and unauthorized users. Such behavior may not even draw the system operators' and authorized users' attention. The problem is compounded if many IoT devices are abandoned by the systems but they still can operate due to long battery life and continue to collect and transmit data.

4) DATA PRIVACY CONCERNS

As the European General Data Protection Regulation (GDPR)[14] came into effect on the 25^{th} May 2018, protecting user data and securing user privacy are urgent issues to be solved in many IoT applications. Users' data cannot be detected nor captured without their awareness. Privacy has the highest priority for all existing and future application development, including IoT systems. The IoT flood makes it extremely difficult to determine how the data will be collected and how they will be used. According to GDPR, users' personal identities must not be identifiable nor traceable. Under the new legislation, data processing must have a lawful and legitimate purpose. Arbitrary IoT device deployment should be forbidden. The data collection needs to be minimized and efforts are required to limit the storage and discourage unnecessary data redundancy and replication. Over collecting data through densely deployed IoT systems should be prohibited. In addition, the data needs to be accountable and liable. Massive deployment of IoT systems with unaccountable devices will be regarded as a violation.

B. SOLVING IoT FLOOD PROBLEM

An effective way to avoid a flood is to control the water from the sources. Control can be achieved by stopping the water at source or channeling the water through proper management to reduce its negative impact. The same approach can be applied to the IoT flood by reducing the number of IoT devices and carefully managing the future deployments. There are several approaches that can be utilized to achieve these goals.

1) ENCOURAGING SHARING

Sharing hardware and data can largely reduce the amount of new IoT devices required. When new information is required, only devices that are necessary and critical to QoS will be deployed. Sharing in this way will reduce the IoT flood problem and encourage inter and inner system interaction between

[10] http://ec.europa.eu/eurostat
[11] http://www.who.int
[12] Base Stations and Wireless Networks: Exposures and Health Consequence's Geneva Switzerland, 2005
[13] https://www.gsma.com/
[14] https://www.eugdpr.org/

IoT systems. Smart IoT systems should not narrow down in a single direction as demonstrated with ITS. Smart transportation is not only about smart travel route to avoid traffic and achieve fuel and time efficiency, it can also improve service by involving smart car parks, safety and personalized, context awareness. IoT deployment needs to collaborate with smart governance, smart grid, smart healthcare and should not operate in isolation. This will achieve maximum reusability and gain. Putting a system in a larger context can produce more optimized solutions. Raw data and meaningful information mined from the data can be shared between smart systems without the need for new IoT deployments. Exchange and sharing that information could benefit all the sectors and systems.

2) STANDARDS AND REGULATIONS

In order to achieve the ITS goals, it is necessary to promote 1) energy efficient sensors and 2) reduce the number of sensors deployed through a set of regulations and standards. The standards can be part of the International Organization for Standardization (ISO). The following should be considered:

1) energy efficient sensors and applications: Energy efficient communication and processing from hardware, Medium Access Control (MAC) layer, networking layer and application layer.
2) sensors should have the capability to support platform/data sharing and promote re-usability. Specific interfaces and components should be provided for such a purpose. IoT platforms should follow the similar pattern of cloud service and data centers, encouraging centralized management and hardware sharing for the purpose of reducing the number of sensors. IoT applications should allow data sharing in a larger scale for the propose of better QoS and QoE.

Applying standards and in particular regulations to control and manage the market will be beneficial. A set of unified standards can also assist and bring convenience when sharing and reusing. Each system should be able to provide well defined interfaces for interaction from hardware and software levels with others. Regulations should be carried out for centralized organizations to refer to when authorizing licenses for IoT devices. If an IoT device can only be deployed with a license, the number of sensors will be well managed and the data collected will be well controlled. IoT is flourishing now, it is urgent to regulate and control the market from a centralized management manner for deployment, data collection, storage and usage.

C. A COMPREHENSIVE EVALUATION SYSTEM

In order to achieve those standards, it is necessary to develop guidelines and a comprehensive evaluation system to enable the implementation of the standards. As shown in Figure 4, IoT systems can exist in a healthy IoT world and function with limited side effects, or cause IoT flood and many side effects, or somewhere in the middle of the scale. Deployment without proper management and control will push the systems towards to IoT flood side of the scale. On the other hand, if adhering to good practice and standards, the IoT flood problem will be solved. The design and development of an IoT system determines where it exists on the scale. A comprehensive evaluation system can reveal the scale to IoT developers and make the index of their system on the scale visible.

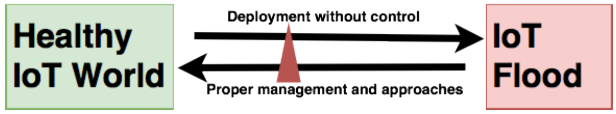

FIGURE 4. The evaluation system can indicate where an IoT system located on the scale.

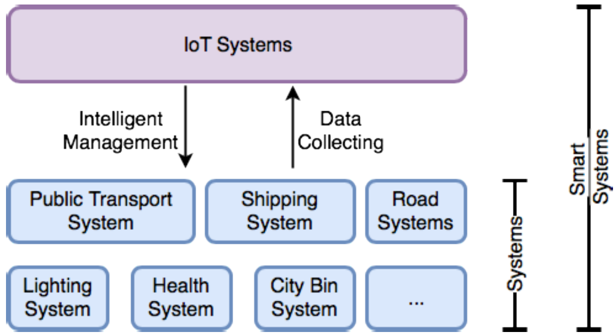

FIGURE 5. The smart IoT systems to manage existing systems to improve efficiency.

Such an evaluation system must reflect the environmental issues that has drawn limited attentions in the current IoT. IoT systems can be seen as intelligent systems to improve the efficiency of existing systems – smart systems of systems, as shown in Figure 5. Normally people evaluate the performance of an IoT system by the improvement in efficiency of the under-laying systems, such as the time saved from taking the public transport. However, the majority of deployments have failed to address the impact of the IoT systems themselves leading to the side effects as shown in Figure 3.

We indicate that an evaluation system is required to measure the performance of the whole part of the smart systems. It should be able to show how energy efficient smart IoT systems are. To answer that, we need to evaluate the IoT systems outside the box and assess the performance in a complete metric space. For example, the evaluation should consider the following facts which are normally overlooked:

- How many devices will be required? What is the environmental cost (air, water, field pollution) to manufacture those chips and deploy/maintain them?
- How much energy/electricity will be used a day?
- What are the energy/electricity sources? Are they clean?
- Once retired, is it possible to recycle the devices/system?
- How well the system can carry out the platform and data sharing plan?

Whether a system designed to reduce CO_2 emission can achieve its target depends on many factors. The hidden effects should also be considered. Systems should be evaluated out of the traditional metric box. It is urgent to utilize a complete metric space and system for evaluation to reflect environmental and other impacts. Based on the above understanding, we have proposed several metrics that should be included:

1) CO_2 emission: To evaluate the total CO_2 emission, it is essential to consider outside the box in order to obtain an accurate real world estimation. To reduce to energy cost, there are several approaches, such as fostering energy efficient communication and processing protocols and algorithms, reducing the number of sensor deployments, using clean energy sources, applying energy harvesting technologies, etc. The Handbook Emission Factors for Road Transport (HBEFA) [32] was introduced to provide emission factors for all current vehicle categories (PC, LDV, HGV, urban buses, coaches and motor cycles), each divided into different categories, for a wide variety of traffic situations. Emission factors for all regulated and the most important non-regulated pollutants as well as fuel consumption and CO_2 are included. This can be a successful paradigm for IoT analysis.
2) Re-usability: Reusing other existing systems, supporting further development and simplifying future updating are all good guidelines to follow.
3) Sharing: Hardware and data sharing will significantly reduce new deployment and contribute to making smart strategies at a larger scale, city level or even country level with a global platform and data set.
4) Advanced/novel ICT technologies: In order to enable less IoT devices in a system without undermining the QoS, more effort on data analysis technologies for missing data prediction, novel architecture designs for hardware and data sharing should be encouraged and motivated. Since GDPR has been applied, many services and existing applications are facing over-exposing private information problem. Technologies which allow high QoS systems through collecting privacy preserving data should be prioritized. Besides, energy harvesting technologies to allow devices to be self-powering are also in urgent demand – even 1 milliwatt saved across 50 billion devices translates into a huge attractive reduction.

D. THE MOTIVATION FOR EXECUTION

There are many approaches to address the IoT flood problem and they are all aiming to achieve two general goals: 1) reduction in the number of IoT devices and 2) manageable deployment. However, motivating institutions and companies to make an effort remains a challenge. Taking ITS as an example, the goals of ITS are to improve 1) time efficiency and 2) energy efficiency. In order to achieve time efficiency, a platform or mechanism to allow hardware and data sharing is necessary to obtain the global optimizing solution. The management is required from a centralized force. To achieve real energy efficiency, the CO_2 emission needs to be evaluated in the proposed evaluation system described in Section IV-C. To solve existing problems in ITS and smart mobility, a centralized management and governance structure is required [33]. Industries need to follow the standards and systems need to be qualified before entering the IoT market.

V. CONCLUSION

There is no doubt that the number of IoT devices is increasing. We have introduced the term IoT flood to describe and capture the challenges associated with this massive increase in device deployment. The magnitude of the increases has the potential to produce unintended consequences and side effects in relation to energy usage, the environment and health. It is imperative that researchers understand the risks and begin to seek ways to address them. We have highlighted how the IoT flood can occur in the ITS domain due to a lack of sharing of devices and data and the narrow focus of projects. The article takes an initial step at solving the IoT flood by proposing the reuse of data and devices. In order to have support for this, regulations and standards are required. Finally, the article argues that in order to measure the impact of IoT success, evaluation metrics of the unintended consequences should be measured.

In the future work, firstly we will aim to provide a set of comprehensive evaluation metrics to 1) rate the potential risk of IoT flood for IoT systems and 2) measure the impact of the IoT systems, especially focusing on the environmental side effects. Other issues such as health, security and privacy will then be considered.

REFERENCES

[1] D. Evans, "The Internet of everything: How more relevant and valuable connections will change the world," in *Proc. Cisco IBSG*, 2012, pp. 1–9.
[2] Gartner Inc. (Jul. 2017). *The Hype Cycle for Emerging Technologies Report*. [Online]. Available: https://www.gartner.com
[3] L. Xu, J. Xie, X. Xu, and S. Wang, "Enterprise LTE and WiFi interworking system and a proposed network selection solution," in *Proc. Symp. Archit. Netw. Commun. Syst.*, New York, NY, USA, Mar. 2016, pp. 137–138.
[4] J.-M. Liang, J.-J. Chen, H.-H. Cheng, and Y.-C. Tseng, "An energy-efficient sleep scheduling with QoS consideration in 3GPP LTE-advanced networks for Internet of Things," *IEEE J. Emerging Sel. Topics Circuits Syst.*, vol. 3, no. 1, pp. 13–22, Mar. 2013.
[5] L. Xu, G. M. P. O'Hare, and R. Collier, "A balanced energy-efficient multihop clustering scheme for wireless sensor networks," in *Proc. 7th IFIP Wireless Mobile Netw. Conf. (WMNC)*, May 2014, pp. 1–8.
[6] C. Gray, R. Ayre, K. Hinton, and R. S. Tucker, "Power consumption of IoT access network technologies," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 2818–2823.
[7] C.-Y. Chong and S. P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," *Proc. IEEE*, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.
[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.
[9] K. Romer and F. Mattern, "The design space of wireless sensor networks," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 54–61, Dec. 2004.
[10] J. Polastre, R. Szewczyk, A. Mainwaring, D. Culler, and J. Anderson, "Analysis of wireless sensor networks for habitat monitoring," in *Wireless Sensor Networks*, C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Eds. Norwell, MA, USA: Kluwer, 2004, pp. 399–423. [Online]. Available: http://dl.acm.org/citation.cfm?id=1013825.1013844

[11] G. Booch, R. A. Maksimchuk, M. W. Engle, B. J. Young, J. Conallen, and K. A. Houston, *Object-Oriented Analysis and Design With Applications*, 3rd ed. Reading, MA, USA: Addison-Wesley, 2007.
[12] L. Ruiz-Garcia, L. Lunadei, P. Barreiro, and I. Robla, "A review of wireless sensor technologies and applications in agriculture and food industry: State of the art and current trends," *Sensors*, vol. 9, no. 6, pp. 4728–4750, 2009.
[13] K. H. Pollock, J. D. Nichols, T. R. Simons, G. L. Farnsworth, L. L. Bailey, and J. R. Sauer, "Large scale wildlife monitoring studies: Statistical methods for design and analysis," *Environmetrics*, vol. 13, no. 2, pp. 105–119, 2002.
[14] L. Xu, R. Collier, and G. M. P. O'Hare, "A survey of clustering techniques in WSNs and consideration of the challenges of applying such to 5G IoT scenarios," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1229–1249, Oct. 2017.
[15] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.
[16] D. Evans, "Leading the IoT, gartner insights on how to lead in a connected world," Gartner Res., Stamford, CT, USA, Tech. Rep., 2017, pp. 1–28.
[17] M. Hoel and S. Kverndokk, "Depletion of fossil fuels and the impacts of global warming," *Resource Energy Econ.*, vol. 18, no. 2, pp. 115–136, 1996. [Online]. Available: http://www.sciencedirect.com/science/article/pii/092876559600005X
[18] G. Dimitrakopoulos and P. Demestichas, "Intelligent transportation systems," *IEEE Veh. Technol. Mag.*, vol. 5, no. 1, pp. 77–84, Mar. 2010.
[19] F.-Y. Wang, "Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 3, pp. 630–638, Sep. 2010.
[20] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, and C. Chen, "Data-driven intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1624–1639, Dec. 2011.
[21] Z. Ning, F. Xia, N. Ullah, X. J. Kong, and X. P. Hu, "Vehicular social networks: Enabling smart mobility," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 16–55, May 2017.
[22] C. Garau, F. Masala, and F. Pinna, "Cagliari and smart urban mobility: Analysis and comparison," *Cities*, vol. 56, pp. 35–46, Jul. 2016. [Online]. Available: http://www.sciencedirect.comscience//article/pii/S026427511630021X
[23] C. Benevolo, R. P. Dameri, and B. D'Auria, "Smart Mobility in Smart City," in *Empowering Organizations*, T. Torre, A. M. Braccini, and R. Spinelli, Eds. Cham, Switzerland: Springer, 2016, pp. 13–28.
[24] ITS Ireland. *Intelligent Transport Systems (ITS) Ireland*. Accessed: Jul. 17, 2018. [Online]. Available: https://www.itsireland.ie
[25] Ireland Advance Systems Access Control. (2016). *Advanced System: Intelligent Transportation Systems (ITS)*. Accessed: Jul. 17, 2018. https://advanceaccess.ie/its/
[26] Enterprise Ireland, "Intelligent transport system—A directory of irish resources," in *Proc. 9th Eur. Intell. Transport Syst. Congr.*, Dublin, Ireland, Jun. 2013, pp. 1–44.
[27] Tourism Department of Transport and Ireland Sport. (2009). *Smarter Travel Ireland*. Accessed: Jul. 17, 2018. [Online]. Available: http://www.smartertravel.ie
[28] The National Roads Authority and Ireland the Railway Procurement Agency. (2015). *Transport Infrrastructure Ireland*. Accessed: Jul. 17, 2018. [Online]. Available: http://www.tii.ie
[29] A. Zamanian and C. Hardiman, "Electromagnetic radiation and human health: A review of sources and effects," *High Freq. Electron.*, no. 4, no. 3, pp. 16–26, 2005.
[30] *EEE Standard for Safety Levels With Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz*, IEEE Standard C95.1-2005 (Revision IEEE Std C95.1-1991), Apr. 2006, pp. 1–238.
[31] *IEEE Recommended Practice for Radio Frequency Safety Programs, 3 kHz to 300 GHz*, IEEE Standard C95.7-2014 (Revision IEEE Std C95.7-2005), Aug. 2014, pp. 1–58.
[32] Switzerland Environmental Protection Agencies of Germany and Austria. (2004). *The Handbook of Emission Factors for Road Transport (HBEFA)*. Accessed: Jul. 17, 2018. [Online]. Available: http://www.hbefa.net
[33] I. Docherty, G. Marsden, and J. Anable, "The governance of smart mobility," *Transp. Res. A, Policy Pract.*, vol. 115, pp. 114-125, Sep. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S096585641731090X

LINA XU received the B.E. degree from the Software Engineering School, Fudan University, China, the B.Sc. degree in computer science from University College Dublin (UCD) through a joint program, and the Ph.D. degree in computer science from UCD in 2014. She was a Research Scientist with HP Labs from 2014 to 2016. She has been an Assistant Professor with the School of Computer Science, UCD, since 2016. She is working on a smart living project aiming to apply IoT technologies to smart living. Her research interests include Internet of Things (IoT), 5G network, smart networking, and machine learning.

GAVIN MCARDLE was a Science Foundation Ireland funded Research Fellow at IBM Research. He is currently an Assistant Professor with the School of Computer Science, University College Dublin, and a Collaborator with CeADAR–Centre for Applied Data Analytics. He has an extensive publication record, including edited books, book chapters, articles, and research papers. He has received several grants from the National and European funding agencies to support collaboration with researchers in academia and industry. His research focus includes location-based services, user profiling, geovisual analysis, smart transport, smart city technology, and urban dynamics. He has been a keynote speaker at several international conferences and institutes.