Towards a global IoT: Resource Re-utilization in WSNs

Sharief M.A. Oteafy and Hossam S. Hassanein
School of Computing
Queen's University
Kingston, Ontario, Canada
{oteafy | hossam}@cs.queensu.ca

Abstract— **The Internet of Things (IoT) is envisioned as a paradigm shift, with a plethora of applications, on the premise of well-established enabling technologies; prominently Wireless Sensor Networks (WSNs) and RFIDs. The former has evolved to improve energy efficiency and resilient operation, yet true scalability has only been recently probed and quite sparsely advanced. Moreover, the traditional approach, whereby most WSN platforms are tailored for a single-application, imposes significant rigidity in re-utilizing platforms for new applications, and limitations on re-using previously deployed ones. In remedy, we present a novel paradigm in WSNs to efficiently utilize network resources, and extend it to a platform for multiple applications to cross-utilize resources over multiple WSNs. We present the approach in three phases; the first calibers resources in the network and their usability. Then applications are represented as finite sets of functional requirements. Finally, we present an optimization approach to find an optimal mapping between applications and resources. This paradigm presents a leap in scalability, not only in a WSN but across multiple ones, dynamically accommodating varying resources being introduced and removed; in addition to utilizing transient resources in their vicinity. To this end, we present an architecture to efficiently adopt WSNs in IoT with changing demands and scale. Our approach is further explained and demonstrated via a detailed use case depicting the premise of IoT applications.**

***Keywords-** Resource re-use; Internet of Things; Sensor networks; multiple applications; Transient resources*

I. INTRODUCTION

Visionaries have set forth a great environment for tomorrow; a world where every object (*thing*) is identifiable and interacting in seamless communication. Many enabling technologies potentiate great magnitudes of pervasiveness for services in the envisioned Internet of Things (IoT). They encompass Wireless Sensor Networks (WSNs) and RFIDs; the Internet and its multi-tiered services; semantic services and middleware, among others. However, a significant drag results from re-employing heritage technologies and paradigms that no longer scale to our IoT aspirations. This problem grows in magnitude as IoT attempts to integrate functionalities, hence complexities, of these technologies and paradigms. A true leap to the IoT requires a grounded, yet radical, shift in paradigms.

As a networking paradigm, IoT evolved on the premise of large scale deployments of two important technologies, namely RFIDs and WSNs [1]. The latter is often extended to include actuators in addition to sensing, thus adding a dimension of effect on the environment, instead of passive sensing. Although significant literature exists on the scalability of both technologies, we stand short of truly integrating architectures that meet IoT scalability demands. Though one of its main enablers, WSNs are yet far from "utilized" adoption in IoT. Its realization is affected by many obstacles, including the IP address space and allocations to *things*, availability of SNs on the Internet, adapting to large scale and control overhead [2].

As one of the recent directions in research, scalability in WSNs suffered from a trend long seen in its umbrella research; namely the "tailoring approach". That is, traditionally most WSN platforms are tailored for a single-application to meet a given efficiency metric. While this is quite justifiable in many scenarios, it presents a caveat in its re-adoption in IoT. By definition, the IoT is to encompass a significant number of integrating architectures, and generality in design, in addition to adherence to access standards, are important aspects of its realization. Thus far, very few exceptions (e.g. those adopting Zigbee) adopt standard access schemes in light of large scale integrations; they are further crippled by the closed (mostly proprietary) state machines governing their inter-operation.

We present a novel paradigm in utilizing WSNs, revamping their view as dedicated systems for sensing tasks, to generic platforms of dynamically assigned resources. By viewing nodes as resource providers, and assigning measurable attributes to these resources, we could better utilize and use them to leverage operational capacity across multiple WSN platforms. That is, multiple applications could run concurrently on different WSNs by optimizing their resource use according to availability and other cost metrics. Maintaining their topology will now shift from node availability to resource utility at nodes being introduced/removed, and utilizing ones that are ubiquitously available in their vicinities. Our paradigm is presented in three phases, namely: (1) resource abstraction and representation, (2) application representation as a finite set of functional requirements over these resources and (3) an optimal mapping to assign applications (their functionalities) to available resources across existing WSNs.

The remainder of this paper elaborates on our paradigm, in light of the research directions currently adopted in IoT literature, and the emerging challenges yet to be probed. Section II presents a background on enabling technologies for IoT and its drives. Our paradigm of viewing WSNs as resources and functionalities is presented in Section III, and the representation of applications and their requirements are detailed in Section IV. An optimal model for overlay of applications in WSNs and ubiquitous resources in IoT is presented in Section V. Finally Section VI concludes with research directions stemming from related domains, and the challenges currently facing state of the art research in IoT.

II. ENABLING TECHNOLOGIES AND IOT DRIVES

The drive for a truly interconnected IoT paradigm with seamless identification, communication and sensing spawned from advances in WSNs, RFIDs and a pool of services. However, these enabling technologies had application specific goals driving their development. Hence, integrating their capabilities in developing the IoT is a two-fold challenge: improving the platforms to scale and utilizing them efficiently in the varying domains of IoT. This section outlines recent advances in WSNs, its support for multiple applications, and recent approaches to scalability and integration with larger systems.

A. Evolution of sensing platforms

Aided by major leaps in MEMS, sensing and wireless communication protocols, WSNs have evolved and gained prominence in today's applications. In earlier phases, much of the research done focused on reducing energy consumption per operation/application, resulting in energy-efficient routing, MAC and duty cycling protocols. Towards these protocols, a general saturation has been achieved. Most tracks still striving on those elementary protocols are merely incremental.

However, a shift of interest lately focused on resilience in harsh environments, where WSNs penetration was projected. Intrinsically, such architectures lost generality and scope as they catered for very specific coupling of applications and environments. Resilient architectures have already advanced in fault tolerance, security and longevity, yet a greater scope for scalability arose [3]. This is magnified by the granularity of these approaches as they cater for specific harsh factors.

Applications now not only require a multitude of nodes, at varying locations, with different tasks; but also demand the versatility to scale and adapt to nodal changes and network expansions, both in functionality and number. As an enabling technology for IoT, new WSN research directions arise for uniquely identifiable nodes, dynamicity in changing applications, and catering for multiple ones as the need arises.

B. Supporting multiple applications

Traditionally, most WSN platforms are tailored for a single-application to meet a given efficiency metric. A few advancements in interchangeable node operation [4], as pre-set schemes, have been proposed to break this design bottleneck. Nevertheless, they stand far from meeting today's demand for scalability, cost effectiveness and resilience to varying nodal and network failures; in addition to changing environments and requirements from pre-deployed WSNs.

Two main streams of research cater for altering applications on a WSN. The first handles remote/dynamic re-programming, whereby newer versions of the software governing nodal operation is disseminated in the network, and broadcasted (usually multi-hop) through it. Significant overhead in communication is often incurred; draining energy and mounting time latency. The other approach is adopting generic middleware for nodes [3], such that the application layer catering for nodal services is interfaced efficiently and dynamically to the underlying operating system functionalities.

Both directions however lack on the dynamicity required for IoT realization. The former exhausts the network in revamping nodes' software. As an approach, it is yet in the phase of infrequent nodal modifications when the need arises. The latter does not cater for nodes that could, at given times, associate themselves with resources in their vicinity, thus changing their resource pool over time. Such as when utilizing the camera of a nearby smartphone.

C. Large scale integrations

A core premise of IoT is the ability to stretch to the global scale [5]. Such ultra large scale (ULS) deployments of WSN are yet a goal. One of the largest actual deployments to date has been GreenOrbs [6], although over a 1000 nodes, it is still confined to a limited forest and uses a homogenous structure.

For the IoT, expanding to ULS is inevitable. IoT's true potential for services will not be realized via networks existing in isolation, let alone not able to inter-communicate. Issues with reliable long range communication, that does not incur significant time latency nor exhausts nodal resources remains a major domain of development. Moreover, expanding on techniques for assisting location detection, aside from traditional GPS or approximate RSS trilateration should be investigated to enable a true ULS deployment that could be easily probed for services via the IoT infrastructure.

III. WSNS AS ENABLING RESOURCES FOR IOT

Traditionally, WSNs are viewed as a group of nodes, pre-designed to perform a given task; which is mostly pre-determined and static. The nodes form a network to communicate their reports to the sink(s). Accordingly, different modalities of control dictate how data is sensed, aggregated/analyzed if any, routed back to the sink and all the network maintenance operations that support these operations (MAC, duty cycling, etc).

Realizing the rigidity of this model in adapting to IoT, especially in terms of node-level unique accessibility from a bigger "web", and the integration of heterogeneous sensors and components, create a cumbersome problem; one that is further magnified by the varying application requirements over time. Simply put, the IoT realization cannot be seen via single-tasked static nodes that are deployed with a static pool of resources. Figure 1 lists some of the prominent hindrances in adopting current WSN architectures in the IoT.

We introduce an abstraction of all components in a WSN, including ones with confined temporal properties (i.e. resources "*passing by*"), and extend the definition to encompass IoT components that add to its resource pool (e.g. cell phones, municipal antennas, objects with different access networks, etc). Then, applications of WSNs when represented as functional requirements based on a set of resources, will be covered in Section IV. To this end, it is important to note the significant advancements in connectivity across different access networks, and the recent advancement in vertical handoffs that leverage resource management when enforced [7]. As such, we assume that inter-connectivity between different wirelessly-enabled devices will not be an issue, as we converge to an era of broadband connectivity across networks.

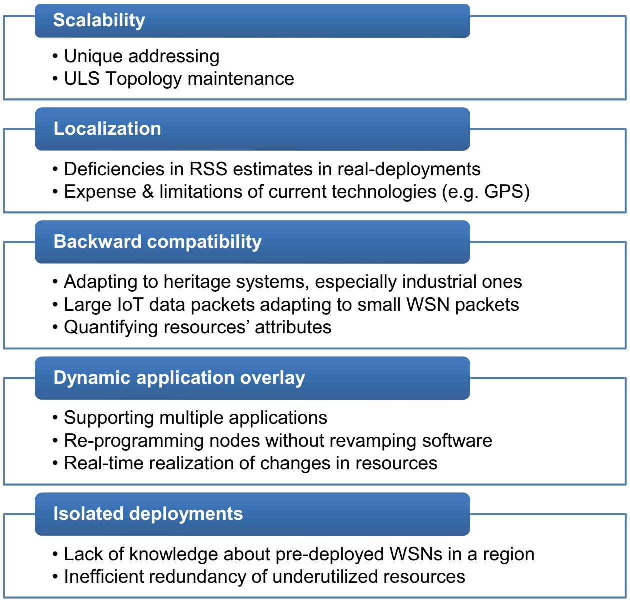

Figure 1. Hindrances in adopting WSNs for IoT

A. Sensing nodes as resources

In a typical setting, sensing nodes are equipped with a processor, memory, transceiver and a sensing platform. Other units in sensing nodes, such as location systems (e.g. GPS) or energy harvesting (e.g. photovoltaic cells) comprise auxiliary components that are mostly application dependent.

Instead of considering such nodes as black boxes that perform a pre-set operation, we hereby view them as a group of components forming a pre-specified set of resources. As such, a typical sensing node would offer the four aforementioned primary resources, in addition to the ones it has been equipped with, or added to it post-deployment. This is an important feature introduced here to cater for nodes that are augmented with more components after deployment. This triggers a significant dimension of research on components added on the fly, elaborated upon in Section VI.

Wired sensors are encompassed under this representation. Simply put, ignoring such sensors that have been invested in and deployed is a waste of resources. In fact, they have the advantage of resilience and power sustenance; metrics which current SNs strive to maintain. In current deployments, they are mostly enterprise-owned systems running proprietary software, yet their integration with established systems facilitates access; a benefit which should not be overlooked. Moreover, there is a significant pull from current infrastructures to maintain their old systems, as long as they are functional, hindering much of the penetration planned for IoT. As such, isolating them from the IoT will incur significant voids in its implementation.

B. IoT objects as resources

Pervasive technologies and services, including cell phones, municipal cameras and data collectors, form a significant resource pool that awaits true utilization by IoT. Although WSNs form a prominent enabling technology, exploiting its capabilities in isolation of other resources in their vicinities would not deliver the IoT paradigm. That is, our challenge is not tailoring WSNs to work for IoT, rather interweave it in the greater paradigm of IoT. That includes resource sharing and cross-utilization between WSNs and nearby architectures to better utilize their resources.

Consider a cell phone passing by a deployed WSN. As a device, it is present in that vicinity for a given duration **T**. It includes a processor, storage, and strong transceiver. All of these resources are significantly more capable than their compliments in a typical SN. What if for a duration **T**, a subset of underutilized resources in such a cell phone could be exploited for long-range relaying of WSN messages or leveraging inter-network data processing.

The remainder of this section will present an abstraction that encompasses these attributes of all resources to be utilized by WSNs. Those include ones deployed in the WSN, others attached/introduced post-deployment, and ones available in the vicinity of WSNs. This representation was also adopted in earlier work [8].

C. Resource attributes

Full utilization across WSNs and other ubiquitous resources cannot be achieved without a clear and rigorous representation. As a core component of our paradigm, we manifest resources via a group of attributes; according to which functional requirement of applications would be drawn. Here we present six core attributes, spanning resources, their availability and usability. The attributes are detailed as follows:

1) Functional capability

A single resource/component could usually perform multiple tasks. For example, if the resource is an RF unit, it has the capacity to Tx, Rx or sense the channel (idle listening). As such, this attributes represents the functions this resource could offer. A camera could possibly take pictures, videos at varying FPS ratings, and so on. Infrared sensors could be used for estimating distance or detecting intrusion. The cases are many.

2) Levels of operation

Often operation granularity is seen in many resources. For example in a transceiver, it could Tx at different levels (usually a step function) to reach further. The resource could also be shut off, to conserve energy, and that is also catered for in this attribute. This is distinguishable from functional capacity since for each function there could be multiple levels of operation. Accordingly, this attribute dictates the ability of a certain resource to meet a functional requirement. E.g. a transceiver would transmit packets as per its operational capacity, but might not be able to Tx at the required dB level for a given application. Hence, even though the resource is available, its operational level deems it unusable. This attribute also be viewed as states of operation.

3) Power consumption

In light of the functional capabilities and the operational (state) level of each attribute, a proper representation of the power dissipation is used. Accordingly, resource utilization would cater for increments in operational levels to meet functional requirements, in light of the power trade-offs. This attribute would most prominently be represented in mW for each resource's operational level.

4) Location

In a static deployment, understanding where a resource exists is imperative to its utilization. This is of more importance as we note the prominent dynamicity of IoT environments. Simply assuming long. and lat. readings for a global positioning might not always be needed, or even feasible. In fact, different applications vary in interpreting location. Often it the relative distance to an anchor point; sometimes the approx. region within which sensing or communication are possible. This remains a challenge in seeking unanimity of definition, yet global positioning paradigm is currently the *de facto* when referring to location.

5) Duty cycling

A major technique for power saving in SNs is duty cycling; where nodes spend only a given percent of their lifetime "on". Generally, it reflects the temporal property of the resource, marking its availability. We introduce the notion of *transient resources*: those having temporal limits on their availability in a given region. Combining the values for location and duty cycling attributes, such resources are catered for in this model.

6) Region of fidelity

We present this attribute as a more relaxed definition of coverage. It encompasses a broader definition of accurately reporting an event in the resource's vicinity. In sensor networks, this reflects typical coverage; for a camera it is the focal length and depth of field within which pictures (and video) are useful; for an ultrasound thickness sensor it's the medium it could detect thickness within. No assumptions are made on the region shape; hence it is application dependent.

D. Resource Pool (ReP)

A core challenge of the IoT is devising the underlying platform that will "encompass it all". Simply relying on Internet protocols to seamlessly integrate the IoT is quite farfetched. Without loss of generality, we introduce a general architecture to span components and their resource representations, which need not be the Internet. Referring to it as the Resource Pool (ReP), its physical locality need not be confine to a centralized location; in fact true scalability will almost dictate decentralized operation. The design of this entity remains an open problem, and a challenge that many disciplines probe [3]. Security issues and scalability, being affected by Internet link capacities and charges, disconnection in service and control practiced by different agencies, are but a few challenges for ensuring a connected and scalable IoT.

IV. DYNAMIC MULTI-APPLICATIONS IN THE IOT

Capturing the essence of applications, we adopt the view of an application as a finite set of functional requirements, needed over a given duration. In fact, coupling this with the detailed view of resource attributes discussed in Section III, it is straightforward to note the mapping. That is, knowing the available resources, and the functional requirements as dictated by the application, we could reach one of two states: (1) the application could be met, hence optimal assignment of tasks to resources need to take place, or (2) the current resources cannot meet the application's demands, hence new resources need to be introduced or requirements relaxed. Thus, we define it as

Definition 1: *An application is comprised of a set of functional requirement* **F** *mapped to a set of resources* **R** *across connected resources.*

Traditionally, mapping applications to the underlying WSN was one-to-one. When expanded over more than a single network, an application is limited by compatibility issues and usage of resources across heterogeneous platforms. However, this paradigm remedies a new challenge in efficiently performing this mapping, over resources from multiple networks, while maintaining its large-scale feasibility.

Formally, for a set of applications **A** where $|A| \geq 1$, we represent the functional requirements of each application $\boldsymbol{a_i} \in \boldsymbol{A}$ as a non-empty set $\boldsymbol{f_i}$. Thus, aggregating over all applications, we derive the set $\boldsymbol{F} = \bigcup_i \boldsymbol{f_i}$ to encompass the set of functional requirements needed. This changes over time, and hence rounds of operation are carried, and denoted by **T**. At each round $\boldsymbol{t_k} \in \boldsymbol{T}$ the sets **F** and **R** are recalculated. Hence, using ReP the aggregation of applications will dictate the mapping denoted as $\boldsymbol{F} \rightarrow \boldsymbol{R}$ at each round $\boldsymbol{t_k}$. Thus, we formally note overall ***network utility*** in meeting **F** as:

Definition 2: *Network utility is an aggregated indicator of the degree by which multiple applications are served, such that resource utilization is maximized across platforms while global network constraints are maintained. Thus network utility is the aggregation of the satisfiability of all applications it serves.*

Thus, we hereby identify network utility as an optimization problem with two sets of constraints, namely: (1) network level constraints such as lifetime, privileged operations and threshold of permitted loads on certain (mostly pivotal) nodes/resources (2) application driven constraints. Since our model runs in rounds, this mapping tolerates changes as resources change. A proposed optimal mapping scheme is presented in the following section. Fig. 2 depicts the varying resources adopted in our paradigm, and the representation of R and F as optimal mapping is performed.

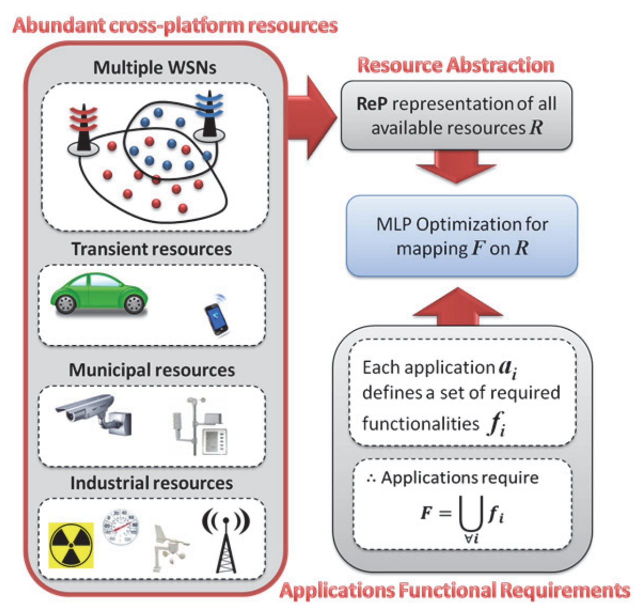

Figure 2. Optimal mapping of multiple applications over IoT resources across different platforms

V. Optimizing Application overlay of WSNs in IoT

Optimal mapping of applications' functional requirements to available resources ensures that the network operates under pre-set fair constraints. Moreover applications are offloaded efficiently over multiple networks without resource starvation or exhaustion. We adopt a linear programming (LP) formulation to solve the mapping problem, noting that other heuristics could be adopted. The problem is relaxed and maintained as an LP to aid computational tractability.

A. Assumptions

We assume that WSNs and their SNs, municipal, industrial, institutional and all personal wirelessly accessible devices form a pool of resources for the cross-platform utilization of our paradigm. As previously mentioned, there are no assumptions on the access network types, as research on vertical handoffs already established leverage to that end. We also assume multiple applications, for varying domains, requesting functionalities from this pool of resources. As such, a single resource could be probed for its functionalities by different applications. Although most structured networks (WSNs, RFIDs, cellular devices, etc) have backbones of their own, we will assume WLOG that our scheme will optimize over ReP, disregarding its physical locality. We assume such resources are already deployed and reachable.

Active nodes holding resources are assumed to have a measurable reservoir of energy, in J, usable by the attached resources. To facilitate dynamic handling of transient resources, the mapping of **F** to **R** is done in rounds, with a duration $\boldsymbol{\tau}$ dependent on the dynamicity of resources in play.

B. Optimal mapping

As with any optimal formulation, the choice of the objective function is of utmost importance. In our paradigm, we aim to maximize Network Utility (NU), as in definition 2, across the required functionalities; aggregated from the multiple applications. Formally:

$$NU = \sum_{i=1}^{|A|} satisfiability_{\ i} * a_i$$

Then, it is imperative to define satisfiability in light of different applications. The notion of satisfiability is coined here with the ratio of functional requirements of a given application that are met. For example, if an application requires images taken at 10 locations, and only 8 of them are possible, then its satisfiability is capped at 80%. As conflicting applications vary in their number of functional requirements $|f_i|$ satisfiability will degrade more significantly for those with smaller $|f_i|$.

Moreover, we note that since some resources could be utilized by multiple applications in concurrency, and each node/thing could hold more than a resource, then resource utilization across applications would actually represent a 3-dimensional matrix, defined as:

$$R_{n,r,i} = \begin{cases} 1 & \text{if resource } r \text{ of node } n \text{ is used for application } i \\ 0 & \text{otherwise} \end{cases}$$

Also, constraints on global performance dictate careful calibration of power consumption – by all applications – across platforms. This is carried out at the beginning of each round $\boldsymbol{T_k}$ formally represented by:

$$\forall\, \boldsymbol{a_i} \in \boldsymbol{A} \left(\sum_{\substack{resources \\ of\ node\ i}} Energy\ consumed\ by\ \ a_i \right) \leq node_i\ energy$$

To demonstrate the versatility of this approach, a use case is depicted in Fig. 3. In light of the recent nuclear tragedy of Fukushima (Japan), many Geiger counters (measuring ionizing radiation) have been deployed in excessive redundancy. Whether by governments, industries or different organizations and individuals, a huge amount of data generated from these readings struck researchers as one of the prominent drives of having a platform such as the IoT. Not only would it serve in aggregating the readings and better aiding their analysis, but also reducing the unnecessary redundancy and underutilization of such expensive equipment.

With two typical WSNs deployed in many regions, we assume one (in red) that measures temperature data and another (in blue) that collects humidity readings. They partially overlap in deployment region and are homogenous. With the 3 Geiger counters deployed in isolation, little could be done to merge their readings; especially that two of them are beyond the communication range of the WSNs. However, using our paradigm the transient resources could be utilized for their communication abilities, to relay readings to WSN sinks. As such, at each round of optimal assignment, when messages are passed on to the nearby (red) sink, temperature readings from its WSN would be offloaded to the other (blue) sink.

Most importantly, the same platform of resources, could serve multiple applications. For example radiation information from the three counters could be used for measuring current nuclear pollution levels; but the same readings could also be used for decision making on the exposure of certain regions to prolonged radiation deeming its harvest inedible. In the domain of IoT, we envision the re-use of not only resources, but also the same information from a resource over multiple applications.

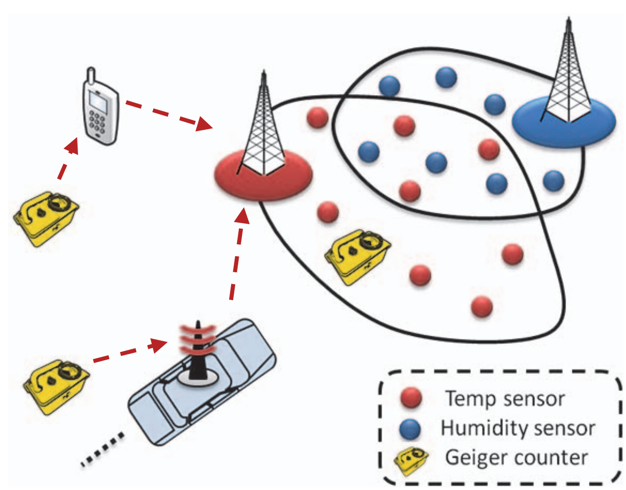

Figure 3. Use case for resource utilization in IoT involving a WSN for temp monitoring (in red), Humidity monitoring (in blue), Geiger counters present in a large region, and two common transient resources (vehicle and smartphone)

VI. Research Directions and Current Challenges

In all fairness, little consensus has been seen in the domain of IoT. Mainly due to the varying domains interplaying their effect on how IoT potentials would truly be realized, it is quite cumbersome to frame the future of key technologies that would dominate IoT architecture and operations [1]. Nevertheless, many aspects still pose challenges to such realization.

Realizing IPv6 communication

With an enormous address space (2^{128}) and the ability to encompass almost all objects uniquely, much deliberation is taking place about the future of IPv6 in the IoT [2]. However, as appealing as it is to simply assign IP addresses to *things* for enabling web services, many challenges deem it a distant goal. Most notably, SNs duty cycle to prolong their lifetime as neighboring nodes take over their tasks, hence often being in *sleep* mode is not consistent with the web paradigm. This also applies to passive *things* that form a significant portion of IoT. Also, data packet sizes of IPv6 present a heavy load on constrained SNs, yet recent efforts in devising operating systems able to handle IP packets have been pursued [13].

A challenge worth deliberating is the resulting traffic on the Internet if all nodes are accessible, with arising security issues. It is imperative to consider Internet connectivity to backhauls and sinks in WSNs, but unrealistic for all SNs. Thus, we note the penetration level of IP in WSNs a challenge, one that should be energy-efficient and light-weight secure operation.

Readers everywhere

A major enabler of real-time identification is RFID, yet many challenges hinder its large scale adoption. Costly deployments of readers, their limited pervasiveness, and the efficient scheme of tagging all things pose major hindrances. Most notably, the readers limited communication range and capacity in interrogating multiple tags, are all areas of development to realizing an efficient and truly ubiquitous IoT paradigm. Ali *et al* investigated reduction of redundant readers which hinder performance due to inter-reader collisions [10].

Security and Privacy to draw upon the ethics of IoT

A major reason for the pervasiveness of IoT is the projected invasiveness of interactive objects that support machine-to-machine communication, and possibly violate many privacy issues. These are most notably seen in ubiquitous social spaces that target real-time identification and reflect personal profiles on user's environment [12].

With a paradigm that is yet feared for its social implications on accessible objects – which are actually personal properties – the research community is yet to establish both the security measures and ethical standards to ensure controlled exposure to IoT services and platforms.

Ambient tracking of passive objects

With pervasive identification schemes, we could assume the ability to identify objects when passing by readers [10]. However, lack of reliable positioning schemes that hold no assumptions on active objects, pose a significant challenge in tracking. That is, passive objects that are not equipped with GPS are hard to track; they cannot send strong signals to utilize RSS, and often suffer negligence in dense environments.

Transient resource utilization

Many of the abundant resources in the *things* to integrate with the IoT, have been designed to serve their respective device purpose. E.g. vehicles that pass by a given region with many resources (memory, transceivers, GPS, etc). An interesting approach to utilizing vehicular networks for sensing and data dissemination is presented in [11]. Being able to detect their underutilization and communicating effective win-win scenarios to cross-utilize these components by WSNs is a great challenge. How would WSNs economically utilize resources passing by their fields while maintaining their efficiency metrics (longevity, security, operational cost, etc)?

Resource on the fly

While resources are typically statically deployed in WSNs as per their pre-set design, there is a new domain of interplay between deployed WSNs and resources that could be introduced post-deployment. For example, a WSN deployed for fire monitoring with only thermometers could be aided with cameras post-deployment for more granularity in detection, and ensuring that rises in temperature are in fact due to fires. How would the WSN platform adapt to such resources, and incorporate them in efficient load balancing and task allocation across the required spatial domain? How would the network dynamically re-configure and adapt its control operations?

References

[1] A. P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby and M. Zorzi, "Architecture and protocols for the internet of things: A case study," IEEE PERCOM, 2010, pp. 678 – 683

[2] D. Guinard, V. Trifa, F. Mattern and E. Wilde, "From the internet of things to the web of things: Resource-oriented architecture and best practices," Architecting the Internet of Things, Eds. Springer Berlin Heidelberg, 2011, pp. 97-129.

[3] M. Wang, J. Cao, J. Li and S. Dasi, "Middleware for Wireless Sensor Networks: A Survey," J. of Computer Science and Technology, vol. 23, 2008, pp. 305-326.

[4] M. Krasniewski, R. Panta, S. Bagchi, C. Yang, and W. Chappell. "Energy-efficient on-demand reprogramming of large-scale sensor networks", ACM Transactions on Sensor Networks, Vol. 4, No. 1, Article 2, 2008, pp. 1-38.

[5] L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey", Computer Networks, Vol. 54, No. 15, 2010, pp 2787-2805.

[6] Y. He, L. Mo, and Y. Liu, "Why are long-term large-scale wireless sensor networks difficult: early experience with GreenOrbs". SIGMOBILE Mob. Comput. Commun. Rev., vol. 14, Iss. 2, 2010

[7] AE M. Taha, H. Hassanein, H.. Mouftah, "Vertical handoffs as a radio resource management tool", Computer Communications, Vol 31, Iss 5, Mobility Management and Wireless Access, 2008, pp 950-961

[8] S. Oteafy and H. Hassanein, "Re-usable Resources in Wireless Sensor Networks", IEEE Global communications (Globecom), 2011.

[9] M. Durvy et al. "Making sensor networks IPv6 ready", ACM conference on Embedded network sensor systems (SenSys), 2008 , pp. 421-422.

[10] K. Ali, W. Alsalih and H. Hassanein, "Using Neighbor and Tag Estimations for Redundant Reader Eliminations in RFID Networks", IEEE Wireless Comm. and Networking Conference (WCNC), 2011.

[11] U. Lee, E. Magistretti, M. Gerla, P. Bellavista, A. Corradi, "Dissemination and Harvesting of Urban Data Using Vehicular Sensing Platforms," IEEE Trans. on Veh. Tech., vol.58, no.2, 2009, pp.882-901

[12] A. Hasswa and H. Hassanein, "Using heterogeneous and social contexts to create a smart space architecture," IEEE Symposium on Computers and Communications, 2010, pp. 1138-1142.

[13] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," 1998.