Cloud-centric Sensor Networks – Deflating the hype

Are we ready to push service-oriented nodes on the Cloud?

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

Abstract— **Much has been deliberated lately on the adaptability of Wireless Sensor Networks (WSNs) to transition into a Cloud-based paradigm. This divergence has been mainly attributed to enabling a dynamic design, larger spread and a more distributed control scheme for WSNs that are inherently static and data-centric. Thus, transitioning into a service-centric paradigm, with the "Cloud" as an enabler, seems appealing. In this paper we argue against the seemingly straight forward transition, and emphasize the pitfalls in transitioning WSNs to an inherently distributed architecture. We articulate on four grounds, temporal and spatial limitations, resilience measures, energy efficiency and functional decomposition. Sheer connectivity, as an intrinsic property that presents hindrances in all these factors, is addressed in light of each. Finally, we present insights into future progressions of WSNs that boosts their dynamic presence without impacting intrinsic design dimensions. This paper serves both as an analytic overview of current directions and hindrances, and an overview to where we can go next in remedy to current and projected bottlenecks in Cloud-based sensing systems.**

Index Terms*—Cloud-centric; Sensor Networks; dynamic paradigms; service-oriented; energy efficiciency

I. INTRODUCTION

The rise of Cloud Computing (CC) and progression of Wireless Sensor Networks (WSNs) have instigated many integration claims. The former being a well-connected and self-healing infrastructure, along with the latter as an interconnected and low-cost sensing technology, provided the basis of many arguments for the integration. The overarching theme of the Internet of Things (IoT) has long dominated the literature hype around such integration efforts [1] [2].

The idea of integration, in its simplest terms, calls for exploiting WSNs on an infrastructure level to provide data for powerful cloud-based storage and analytics. Thus, depending on a reliable backbone to interconnect many WSNs to better sense objects and people on the planet. While an appealing notion, there is much merit attributed to both systems in isolation, yet significant challenges when integration comes into play.

As a reliable technology, cloud-based services have gained significant attention in the past few years due to three core properties: (1) Reliable connectivity and operation with significant emphasis on data replication and accessibility (2) standardized protocols that promote interoperability between different systems, and (3) an ever evolving virtualization of hardware that sporadically resides over different locations in the globe with geo-based service provisioning [3].

On the other hand, WSNs have emerged over many years of research into a self-healing untethered technology that enables sensing in regions deemed ever unreachable. More importantly, the ever growing plethora of applications where WSNs have already been utilized generate significant momentum for both research and market uptake/adoption. WSNs are already considered a core facilitator for the IoT [2] and have expanded to support middleware [4] and light-weight operating systems (OS). Contiki, a strong OS contender for WSNs, enables IPv6 connectivity [3] and has been the building block of many protocols, such as the light-weight uIPv6 protocol stack [5].

Cloud computing hailed many features, mostly dependent on reliable connectivity over the Internet [3]. The notion of elastic processing and storage capabilities, which expand per user/application need, offered an important infrastructure for dynamic systems that require connectivity. Also, this infrastructure enabled the proliferation of Software as a Service (SaaS) over the elastic infrastructure [3]. This paradigm enticed researchers to investigate the potential of integrating WSNs with Cloud-based services.

The seemingly intuitive merger of both paradigms is anything but. On the one hand, Cloud-based hardware and services evolved to potentiate dynamic services that require a varying hardware profile, have a variable consumer base, and need to adapt to global-scale services; under the umbrella of the Internet. On the other hand, WSNs are static in terms of design goals, user profile, usability and access profiles. That is, interest in operation and data collected are confined to the WSN owner.

This work presents an investigative effort in assessing the validity of merging claims, the assumption base of many integration models, and the hindrances presented by the natively contrasting paradigms of Cloud-based services and WSNs. We underline the importance of investigating mainstream tracks of introducing dynamic operation in WSN design, and the importance of considering Cloud services in

that challenge. We highlight the benefits of employing a paradigm with dynamic mediators (entities) that build upon Cloud-based services to improve WSN dynamicity, in contrast to the hindrances of integration presented in this work.

In the remainder of this paper we elaborate on the development of Cloud Computing and elastic services, over variants of the Cloud, in Section II. This background also overviews recent efforts in enabling IPv6 connectivity in WSNs and efforts under 6LowPAN initiatives. Section III presents the core arguments for this work, elaborating on the factors of hindrance that challenge the integration of WSNs with Cloud-based services. We conclude in Section IV with future work and directions that could carry forward the merger of both paradigms under an umbrella of facilitation and mediated operation, rather than offloading and sheer connectivity.

II. BACKGROUND

WSNs evolved with static post-deployment designs. That is, goals, operational mandates and task-allocation for sensing nodes (SNs) are set prior to deployment. Practitioners and researchers alike saw the need to transition WSN design to cater for more dynamic post-deployment operational mandates, in addition to malleable application goals [6] [4]. An overview of the current components of a cloud-centric vision of WSNs is depicted in Fig.1.

A. *The Cloud variants*

The Cloud evolved as a virtual resource pool that exists on the Internet, manifesting hardware that resides over different geographical locations. The spatial distribution of these locations, and the rules of shared resources, along with the access rights given to different users, dictated a differentiation in the types of Clouds [3].

We elaborate on three distinct types of Clouds. The first is the Private Cloud which serves a given company/deployment. It offers a dedicated virtualization of resources to terminals belonging to a company, for example, and eases maintenance and software upgrades that are to impact cloud-connected terminals [7].

The public Cloud, much like Amazon EC2, offers a resource pool (mainly storage and processing) for public users at a given set of rates (depending on demand) [8]. A more restrictive type of Cloud that was devised to cater for companies/deployments of similar requirements was presented as Community Clouds. In this case the resources are shared, with pre-determined access rights, between terminals in the closed community of these companies. This again mitigates

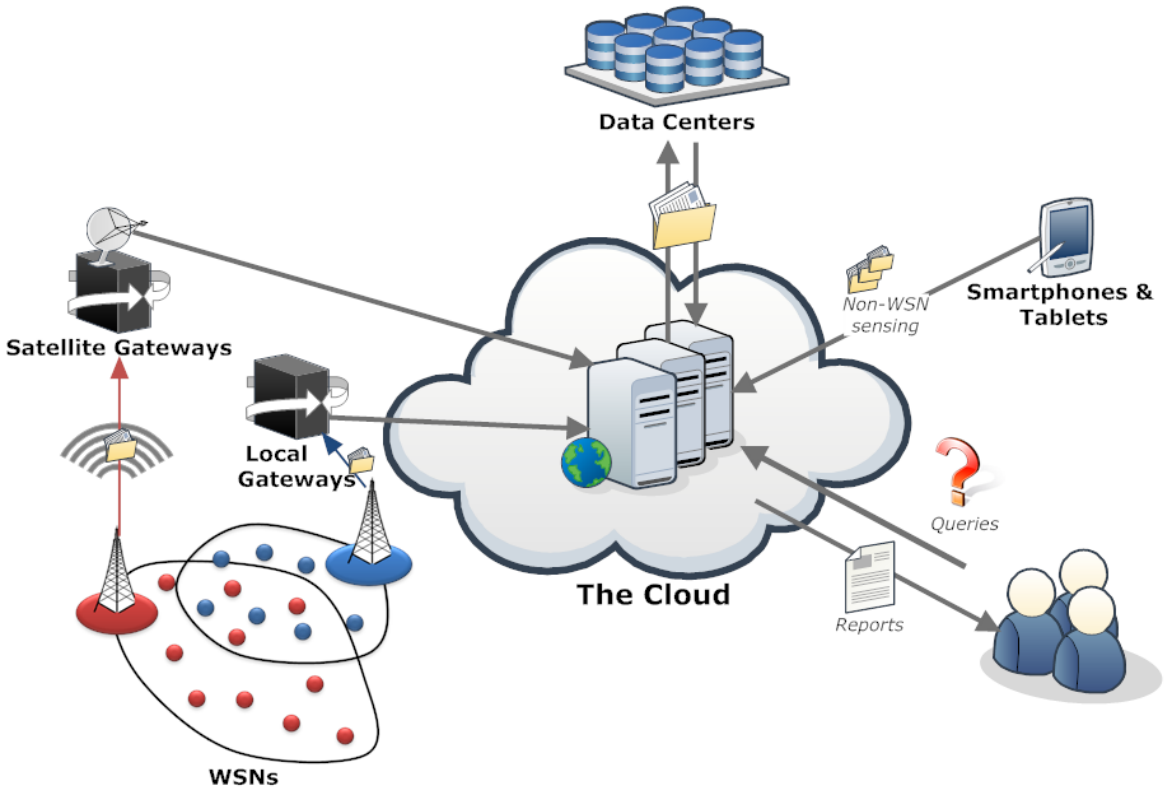

Figure 1. Overview of interacting components in Cloud-centric Wireless Sensor Networks (WSNs)

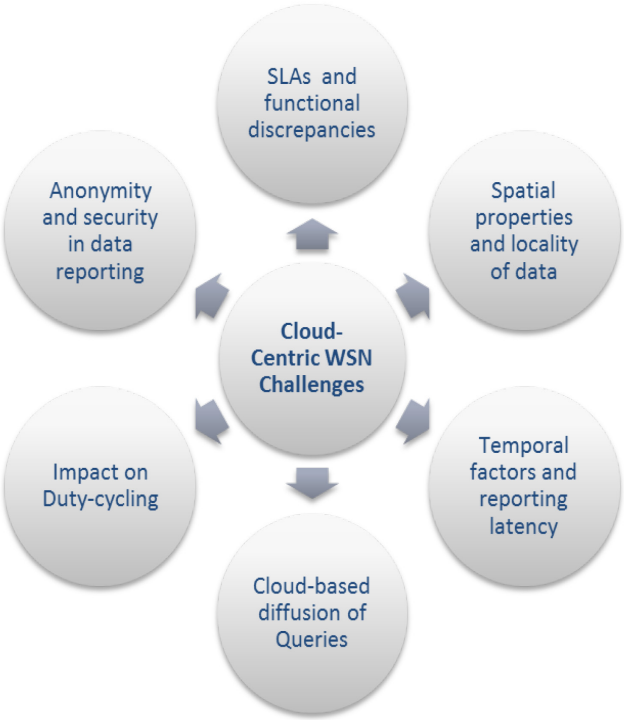

Figure 2. Mainstream challenges in realizing Cloud-centric WSNs

maintenance issues and restricts public access [7], yet enables a more economic maintenance plan for users.

B. 6LowPAN and stub nets

The rise of IPv6 with its enormous address space (2^{128}), and the potential for assigning unique addresses for everything, set forth many arguments on WSN connectivity. On one hand, being able to access each sensing node and probing it for data, via unique addressing, seems great. On the other hand, issues of duty cycling, constrained operation and security, to name a few, raise many questions and challenges.

Recent efforts by the Internet Engineering Task Force (IETF) under the 6LowPAN working group released an informational RFC on the mandates for routing in IPv6 networks [9]. This document elaborated on the formation of mesh topologies and the resulting multi-hop routing in a 6LowPAN setting. The idea is that supporting IPv6 addressing is becoming an increasingly appealing solution for connectivity in Machine-2-Machine communication and devices (mainly SNs) that possess limited power [9].

C. SOA and SODA

Considering WSNs as service providers has been debated in the literature for some time. The idea simply spurred from establishing an interface to the hardware of a SN. Accordingly, the application-level development of software to govern SN operation would be programmed in the language of choice for the programmer, without the need for understanding the underlying hardware profiles, MAC and routing protocols, and so on [10]. An initial model, named TinySOA was presented to address these issues [10], which soon converged in the literature on WSN middleware.

However, further developments in service-oriented architectures, not only encompassing WSNs, had grown to realize a grander scheme. More specifically, the notion of Service-oriented device architecture (SODA) was presented to tackle the notion of an arbitrarily dense and resourceful infrastructure, including SNs [11]. Thus, instead of approaching WSNs via specific middleware, the view expanded to resource abstraction. This facilitated a more definitive and self-sustaining definition of functional requirements.

More importantly, the main idea lies in severing service development on the enterprise level from the pool of devices that grow in number and heterogeneity [11]. This is achieved by providing a high-level abstraction of the hardware and resources in these devices.

Augmenting SODA onto a Cloud architecture facilitates a dynamic and independent visibility of resources, which would be updated on local Clouds. Thus, Cloud-based services would exist on abstract layers that only perceive WSNs as a component in the device base.

III. HINDARNCES IN ADOPTING CLOUD-CENTRIC WSNS

The case for adopting a resilient and dynamic architecture for WSNs is indeed valid and important. However, attempting to piggy-back such design parameters on the Cloud is yet farfetched. This section presents an elaborate discussion on the hindrances and challenges in realizing a Cloud-centric paradigm that is a merger of the status quo in both technologies/systems.

We argue on 8 major points, elaborating the discrepancy in design and implementation between both technologies, and the potential issues in merging their operation. It is important to note that our arguments are posed in regards to WSN efficiency, rather than Cloud adaptability. That is, our concern is the evolution and progression of WSN design, operation and maintenance, rather than expanding the applicability of Cloud-based services. Literature expansions on the latter topic are self-sufficient and beyond the interest of this work. We present in Figure 2 an overview of the mainstream challenges facing this integration.

A. Spatial limitations

WSNs collect data that are geographically-sensitive, thus the importance and criticality of collected data are often localized. The idea of enabling remote access to WSN data is often warranted, but far from the mainstream. If we are to advocate Cloud-based connectivity, to enable distributed access to geographically-sensitive data, the question lies in the frequency of requests that would outweigh the accessibility to data and overhead of maintaining a synchronized and “online” presence of such WSNs.

Advocating that the Cloud infrastructure and WSNs share a distributed infrastructure does not warrant coupling them. In

most scenarios, a single interface to the WSN via a dedicated link would suffice to the primary user of the WSN.

It is also important to note that the value of information varies by location. Thus adopting distributed access to WSN collected data (e.g., temperature readings, in the most benign case) dictates dynamic valuation of information. That is not an intrinsic property of WSNs, and remains an issue seldom questioned in application-specific deployments.

B. Temporal limitations

System responsiveness is an important metric in distributed systems such as the Cloud; whereby a cap is mandated for the waiting time expected for a request (e.g., query) to be met. In WSNs, the duty cycling of sensing nodes, the control overhead, MAC contention and back-off timers, in addition to sensing latency, all prolong WSN responsiveness. Thus, integrating a system that is mostly assumed to be event-triggered or low-duty-cycled with a system that is responsive by design, will create significant discrepancies.

Designing and designating service level agreements (SLAs) between WSNs and Cloud-based services will dictate significant overhead in design that is not appreciated in an already energy-stringent technology. The notion of addressing round-trip latency in Cloud-based services and WSNs is a significant integration challenge.

Moreover, is it important to note that in many (especially non-critical) applications, SNs keep track of time to order events, rather than ensure accurate time keeping. That is, since the problem of maintain synchronized clocks in WSNs carries significant overhead, there is little assurance of accurate clocks.

The impact of time discrepancies, consistency checks and synchronization on data validity and timeliness are of significant hindrance in synergizing WSNs with Cloud-based services.

C. Data represntation SLAs

The various range of representations for sensed data, and the encoding/aggregation of it, presents a significant challenge in addressing SNs from the Cloud. More specifically, WSNs adopt compression and aggregation schemes to reduce the amount of data traversing the network, optimizing on power consumption, and in many scenarios this aggregation is lossy [10]. That is, the packets received at the sink could not be decoupled into the original data values. Thus, mandating a SN-based representation for data, and stringent SLAs on the quality of data reported, pose a significant challenge when integrated with the Cloud.

D. Impact on Resilience

WSNs are designed to withstand varying levels/types of faults based on the designated applications. Accordingly, pre-set schemes ensure that redundant/overlapping deployments ensure a certain coverage level (per unit area). These resilience schemes are designed to withstand operational mandates of the WSN, as dictated by the sink.

Overhead from cloud-based services and frequent probing of SNs affect the operational mandate of SNs. This is especially true for cases where SNs respond to non-WSN requests (e.g., via IPv6 connections). The overhead and probed-operation disrupt duty cycling schemes that are designed to prolong WSN lifetime and ensure a viable set of nodes to sustain resilience.

E. Energy efficiency at steak

Establishing a joint operation between energy-constrained WSNs and power-driven Cloud architectures result in a significant impact on energy consumption in the former. The contrasting operational mandates mean that WSN shall suffer from the frequent probing of the Cloud, and power drainage due to unstable and uncoordinated duty cycling.

Communicating to individual nodes via IPv6 and demanding "live" connections and accessibility are in hindrance to their longevity [14]. This is an intrinsic property of WSNs that has long carried its success in remote sensing applications. Yes, there is merit in probing real time data from SNs deployed in remote regions. However, enabling such "accessibility" is to the network's detriment.

F. Functional decomposition discrepancies/re-design

Would functional decomposition pertaining to SNs be spatial, temporal or load balancing? These are important challenges to consider in the efforts to merge both technologies. At the Cloud level, little information is available about the inner workings of WSNs, hence dictating a given decomposition of functionalities requires of SNs is complex.

At which level would coordination be handled within low-end SNs? Given their limited resources, which entities would dictate a governing scheme that will alter their operation? Would dictating a synergy between the Cloud and WSNs dictate re-designing the operational mandate of sinks to handle functional decompositions and mitigate their impact on WSN operation? These questions remain open challenges that impact discrepancies in service descriptors across heterogeneous sensing platforms.

G. Breaching anonymity

A strict coupling exists between the collector of data and the data itself. In this case, sensing nodes act as collectors. One of the core arguments for cloud-based sensing is utilizing a core for all the information that is to be collected over the masses. However, the argument only holds if the contributors of data are either willing to sacrifice their anonymity or are assumed to be indifferent.

H. Traffic bottlenecks and Query diffusion

An important factor to consider is query handling in a merged architecture. If we were to assume that the Cloud would alleviate querying efforts, and leverage WSN performance by handling the processing of queries, then where are they executed? The offloading process, and distribution of query handling are important tasks with significant overhead in distribution, processing, and potentially aggregation.

IV. Conclusions and Future Directions

Practically, depending on an Internet backbone for WSNs is important if not inevitable. The argument lies not in whether or not it is important to piggy-back WSN operation and accessibility on Cloud services, yet in the design and mediation leading to beneficial synergy between both technologies.

This work highlighted a number of mainstream research issues and challenges facing the cooperative integration of WSNs and Cloud-based services. On the one hand, many variations of the integration model have been proposed in the literature motivated by IPv6 connectivity and Cloud pervasiveness. Yet, on the other hand, WSNs are inherently application oriented and lack the flexibility in design and operation to tolerate access and disruptions from beyond the sink/base station.

We argued over a set of mainstream research topics that require further analysis and investigation to quantify their impact on integration efforts. Most importantly, establishing solid arguments on the benefit of integration and synergy at each component, to outweigh the undue overhead on resource-limited energy-constrained WSNs.

There are a number of directions to pursue in developing WSNs that are capable to cope with Cloud-centric paradigms. At the core of any synergy attempt, there must be room for dynamic operation by SNs. Specific scenarios for both homogeneous and heterogeneous WSNs require investigation to determine query-diffusion and service provisioning on energy-constrained SNs. An interesting development in dynamic over the air reprogramming of SNs [15] enables post-deployment maintenance of WSNs. More valuably, enabling a tunable operational mandate for WSNs when integrated with Cloud services.

A reliable and progressive vision for this synergetic effort is introducing arbitrators/mediators that are able to represent energy constrained devices to the Cloud. As such, SNs would not have to engage in long range communication, change their duty cycling nor adapt to heterogeneous components beyond their WSN. The design of such arbitrators remains an open problem that requires significant investigations on 6LowPAN stub net formations and buffering capacities to deal with the challenges highlighted in this work.

Acknowledgment

This research is funded by a grant from the Ontario Ministry of Economic Development and Innovation under the Ontario Research Fund-Research Excellence (ORF-RE) program.

References

[1] R. Buyya, C. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", Future Generation computer systems, Vol. 25, no. 6, pp. 599-616, 2009.

[2] S. Li, L. Xu, X. Wang, and J. Wang, "Integration of hybrid wireless networks in cloud services oriented enterprise information systems" Journal of Enterprise Information Systems, Vol. 6, no. 2, pp. 165-187, 2012.

[3] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, et al., "A view of cloud computing", ACM Communications, Vol 53, Iss. 4 pp. 50-58, 2010.

[4] L. Mottola and G. Picco, "Programming wireless sensor networks: Fundamental concepts and state of the art" ACM Computing Surveys (CSUR) Vol. 43, no. 3, 2011.

[5] M. Durvy, J. Abeillé, P. Wetterwald, C. O'Flynn, B. Leverett, E. Gnoske, M. Vidales et al. "Making sensor networks IPv6 ready." In Proceedings of the 6th ACM conference on Embedded network sensor systems, pp. 421-422, 2008.

[6] S. Oteafy and H. Hassanein, "Utilizing transient resources in dynamic wireless sensor networks," Wireless Communications and Networking Conference (WCNC), 2012 IEEE , pp.2124-2128, 2012.

[7] H. Jin, S. Ibrahim, T. Bell, W. Gao, D. Huang, and S. Wu, "Cloud types and services", Handbook of Cloud Computing, Springer US, pp. 335-355, 2010.

[8] S. Ostermann, A. Iosup, N. Yigitbasi, R. Prodan, T. Fahringer and D. Epema, "A performance analysis of EC2 cloud computing services for scientific computing" Lecture Notes of the Institute for Computer Sciences, Cloud Computing, Vol. 34, Springer Berlin Heidelberg, pp. 115-131, 2010.

[9] E. Kim, D. Kaspar, C. Gomez, and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing", Internet Engineering Task Force (IETF), RFC 6606, 2012.

[10] E. Avilés-López, and J. García-Macías, "TinySOA: a service-oriented architecture for wireless sensor networks", Journal of Service Oriented Computing and Applications, Vol. 3, no. 2, pp.99-108, 2009.

[11] S. de Deugd, R. Carroll, K. Kelly, B. Millett, and J. Ricker, "SODA: Service oriented device architecture", IEEE Pervasive Computing, Vol. 5, no. 3, pp.94-96, 2006.

[12] R. Kyusakov, J. Eliasson, J. Delsing, J. Deventer, and J. Gustafsson, "Integration of Wireless Sensor and Actuator Nodeswith IT Infrastructure Using Service-Oriented Architecture", IEEE Transactions on Industrial Informatics, vol.9, No.1, pp.43-51, 2013.

[13] S. Chong, M. Gaber, S. Krishnaswamy, and S. Loke, "Energy-aware data processing techniques for wireless sensor networks: a review", In Transactions on large-scale data-and knowledge-centered systems III, Springer Berlin Heidelberg, pp. 117-137, 2011.

[14] J. Ko, J. Eriksson, N. Tsiftes, S. Dawson-Haggerty, J. Vasseur, et al., "Industry: beyond interoperability: pushing the performance of sensor network IP stacks", In Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems (SenSys), pp. 1-11, 2011.

[15] N. Bin Shafi, K. Ali, H. Hassanein, "No-reboot and zero-flash over-the-air programming for Wireless Sensor Networks," 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp.371,379, 2012.