GE-International Journal of Engineering Research
ISSN(O): 2321-1717, ISSN(P): 2394-420X
Vol. 6, Issue 5, May 2018 Impact Factor- 5.613
Associated Asia Research Foundation (AARF) Publication
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

Wireless Sensor Networks within IoT Ecosystem

***Ms. Neelam Swami**

Assistant Professor, Department of Electronics and Communication Engineering,
Govt. College of Engineering and Technology, Bikaner, Rajasthan, India - 334004
e-mail:swami.neel87@gmail.com

Abstract— Within the context of Internet of Things there is an expectation that devices will always be connected and an assumption that data will always be available, however there is little concern for the physical devices producing these data streams. There is a need to balance the appetite for data with the constraints and capabilities of the supporting physical infrastructure. This paper presents a management framework for wireless sensor networks within IoT ecosystems. This framework through cooperation and negotiation can lead to the creation of multiple virtual networks deployed over the same physical infrastructure to share resources, context, insight etc., in order to meet dynamic service requirements. This necessitates a shift from traditional management approaches focused on centralized management for bespoke solutions to the development of novel approaches for autonomous management via distributed intelligent gateways that proactively monitor and manage IoT WSN infrastructures to support multiple application verticals.

***Index Terms*—Reference Architecture, Virtual Sensor Networks, Virtual Entity, IoT Management Framework**

I. INTRODUCTION

Wireless sensor and actuator networks (WSNs) are viewed as a key enabling technology to bridge the gap between the physical and virtual world to realise IoT where IoT offers the ability to interconnect real world objects (RWO) and allow them to interact and cooperate with each other and/or users to form new applications. There are many proprietary and non- proprietary solutions available for WSN which has resulted in the development of a static one-to-one relationship between the WSN devices and the application case. This scenario driven approach has resulted in WSN becoming information silos with limited connectivity to the external world prohibiting their impact and stifling the large scale deployment of these networks. Providing a generic infrastructure that can support an extensive ecosystem of smart applications with varying demands and requirements is a pre-requisite for IoT.

Currently much of the focus in IoT has been at the service layer and above; there is a lack of consideration on the impact IoT services have on the management of the underlying physical infrastructure (sensors, actuators, networking, communications, data quality, security and privacy). Many of the solutions that are available are generally capable of abstracting from the underlying hardware and focus on data modelling, distribution, service creation and discovery. The general consensus\expectation is that the IoT will result in billions of embedded devices being seamlessly interwoven into the fabric of our everyday lives and to leverage these the community must move away from bespoke solutions for application verticals and deliver more generic approaches to architecting, deploying and managing IoT systems.

The view put forward in this paper is that to achieve this in a scalable way, you cannot decouple the management of the underlying supporting WSN infrastructure and the services they provide for. Being able to integrate devices to the internet via IP protocols (6LoWPAN), gateways (Internet Bridge, AMQP brokers, MQTT) and APIs (RESTful) is essential to enable the dynamic creation of IoT services, however solutions must consider functionality for the management of heterogeneous distributed networks, which interconnect the physical nodes of the cyber physical systems (CPS). These solutions must address problems such as resource optimization (resource constrained devices), conflict resolution, mobility and large scale geographically dispersed heterogeneous networks of devices. This is a non-trivial task and should not take a clean slate approach but rather build on existing solutions and technologies (distributed middleware, virtualization, software defined networking, federated networks, orchestration and provisioning etc.) to enable the creation of an infrastructure management approach for IoT applications. This paper introduces a reference framework for managing WSNs in the context of IoT. This includes a review of how WSN currently map to IoT (Section 2), the specification of a management framework for WSN infrastructures within IoT ecosystems (Section 3) and the application of this framework to a WSN health monitoring service (Section 4).

II. RELATED WORK

The integration of WSNs into IoT platforms typically focus on providing a data-centric mechanism for IoT services. This sees the publishing of data remotely either directly or through the use of a bridge, with data being stored in a server or published to third party cloud platform. This enables the design of content rich applications; however the effect these applications have on the physical infrastructure resources is somewhat loosely coupled at most. With the continued proliferation of the numbers of connected devices, there is a need to provide a set of autonomous management functions

that integrate configuration, operation, security, administration and maintenance of all elements of the IoT network. IoT applications will necessitate the dynamic grouping and autonomous management of smart objects; however, traditional network management is not directly transferable in cases where manual configuration and tuning is often required by network administrators.

Abstracting the physical device as a virtual entity allows it to be reused outside the context for which it was originally deployed. A number of research works have focused on virtualization of real devices to link data generated to software systems (data processing, fusion services) or IoT applications. There are a plethora of platforms and techniques proposed that act as mediators between sensors and data consumers, some include the use of data wrappers

and semantic interoperability [1, 2], middleware [2, 3, 4], virtual object repositories [5] and data mash-ups [6]. [7] Provides a gap analysis of a representative sample of IoT platforms currently available, one of the major challenges that needs to be addressed from the view point of middleware solutions is the ability to re-provision the infrastructure to meet application, privacy and data ownership demands. Middleware platforms must also promote reduced latency (e.g. via edge analytics) and improved energy efficiency of IoT devices. In addition the provision of SDKs and support for developers is critical to allow seamless and cross-platform integration. Having IP enabled devices is often considered enough to integrate sensors in the internet however there is a need to have a more robust/encapsulating framework to be truly IoT ready [8]. Although the ultimate target, having a full IP-based network is not yet feasible due to the resource constrained nature of devices and the fundamental differences between traditional internet communications and how wireless sensor networks communication has been developed. Therefore significant emphasis has been placed on developing middleware platforms [9] or Internet bridges [10] [11] to allow access from the application layer to the network. Representational State Transfer (REST) or RESTful approaches such as [12, 13] are becoming more common place. For example the Constrained Application Protocol (CoAP) as defined by the Internet Engineering Task Force (IETF) [14] allows constrained embedded devices to maximize the use of the existing, well-defined HTTP interface, and minimize the addition of new application-specific features on top of it. Many embedded devices do not have the memory, processing power or lifetime to run complex applications therefore this functionality is generally abstracted and deployed within the Internet. Turning end devices into RESTful resources helps in developing physical mashups [15] with regard to heterogeneous end devices yet there has been little focus on how pushing all of these devices into the IoT will impact on the underlying infrastructure, the assumption is that the data will always be available and little concern with regard how smart objects networks can sustain reliable data delivery, connectivity and life-time. A major advantage of IoT systems is that by default they are multi-service; serving more than one distinct application or service. This implies not only disparate traffic types within the network, but also the ability of a single network to support many applications without compromising on performance [16]. Abstracting the entire underlying infrastructure in virtual entities makes it possible to create different network applications which accomplish the needs and requirements of different IoT applications, using the same infrastructure. Different IoT marketplaces have been appeared over recent years, which use virtualization of the network and the virtualization of the smart objects to provide end-to-end services without considering the characteristics or state of the network and their components. From the end-user view, the underlying infrastructure should be considered as an autonomous system which works as expected and is managed by itself. The translation of applications requirements to the underlying infrastructure should be achieved by the generation of policies, which will provide a set of rules aims to accomplish the application specifications. Another aspect to consider is the management of the network, iCore [17] provides a base framework for the representation, registration, composition and discovery of virtual entities to support multiple IoT applications over the same infrastructure. Similarly OpenIoT

[18] provides mechanisms for context-aware ranking of smart objects to establish relevance to application needs; it is acknowledged that many middleware platforms provide basic search capabilities (proximity and data type) focus and as such they will be leveraged by the project. A typical IoT application involves data being collaboratively published remotely (either directly or via an Internet bridge), stored in a data warehouse and published to third party

cloud platforms. This provides a scalable solution and supports the development of content rich applications; however the underlying infrastructure is still maintained and managed locally outside the context of the IoT therefore the management approach is only loosely coupled with the internet. IoT enabling technologies such as wireless sensor actuator networks (WSN) need to provide a set of management functions that integrate configuration, operation, administration, security, and maintenance of all elements of the network to ensure expected Quality of Service (QoS) is achieved [19]. Traditional management solutions for sensor networks typically take a centralized view of network management and are located externally from the network itself in management stations. The management stations host applications to interact almost on a per-device basis using protocols such as SNMP, TMN and OSI-SM, to extract performance metrics (e.g. packet counter, latency) or inject commands to support configuration, fault, performance, and security management and have been shown to be successful for relatively static, small scale networks [20]. However in contrast to IoT systems these networks evolve slowly with minimal configuration change or intervention required. A major advantage of IoT systems is that by default they are multi- service; serving more than one distinct application or service. This implies not only disparate traffic types within the network, but also the ability of a single network to support many applications without compromising on performance [16]. In this case a centralized approach to network management rapidly becomes unwieldy. Existing approaches to wireless sensor network management have addressed various aspect of management at different levels, these can be classified under the following categories, a sensor network management framework (BOSS, MANNA), Sensor Network Management Protocols (RRP, SNMS, sNMP), QoS Aware Routing (SAR, Energy Aware Routing, SPEED, Mobicast, RPL), Management by Delegation (Agilla, Agent-Based), Debugging and Visualization Tools (e.g. Sympathy, MOTE-VIEW), Power and Traffic Management (e.g. SenOS, Siphon) [19]. These approaches and protocols play an important role in ensuring reliability and the type of protocol used needs to be considered during the design of the wireless sensor networks in the IoT to ensure the infrastructure can be managed effectively. While significant progress has been made in recent years in the areas of hardware design, system architectures, protocol design and power management to make wireless sensor networks easier to deploy and maintain, the differentiation of the proposed approach is that it aims to extend and refine existing management concepts and embed them directly into an IoT architecture. A WSN IoT management framework enables a decentralization view of management functionality, proactive management of the infrastructure, scalable and reusable management services and autonomy of management entities. The management functionality of WSN will no longer be developed as an add-on to the service provided rather as an intrinsic part of the system that is delivered within the IoT. Future IoT will demand that WSN will be viewed as platform independent, large-scale infrastructures that encapsulate data management, processing, actuation, analytics. They must also become more context-aware and contribute to the delivery of the QoS of the overall IoT system.

III. IOT MANAGEMENT FRAMEWORK FOR WSNS

No one architecture will match all the application areas envisioned for the IoT and the diverse requirements those areas bring. However, a modular scalable architecture that supports broad use case applicability, abstracts common functionality and features is needed to drive IoT technology and application development. The Industrial Internet Consortium (IIC) [21] and

IOT-A are leading lights in terms of promoting a reference architecture approach for the IoT, with these having common objectives i.e. the development of reference model to support a common understanding of the IoT (IoT-A) and a reference architecture to provide a common foundation for the development of interoperable IoT system architectures (IIC, IoT-A). The most prevalent implementation patterns identified by the IIC are the three tier pattern and the gateway-mediated edge connectivity and management architecture pattern. The three tier architecture consists of the enterprise, platform and edge tiers. The enterprise tier manages domain-specific applications, end-user interfaces and receives data from the platform and edge tiers and actuates control commands to the lower tiers. The platform tier is responsible for the management of edge devices and manages data flows from the edge tier. The edge tier is responsible for data collection from edge devices. The gateway-mediated edge connectivity and management architecture pattern is described as a local connectivity solution for edge devices where a gateway is used to bridge to a wide area network (WAN).

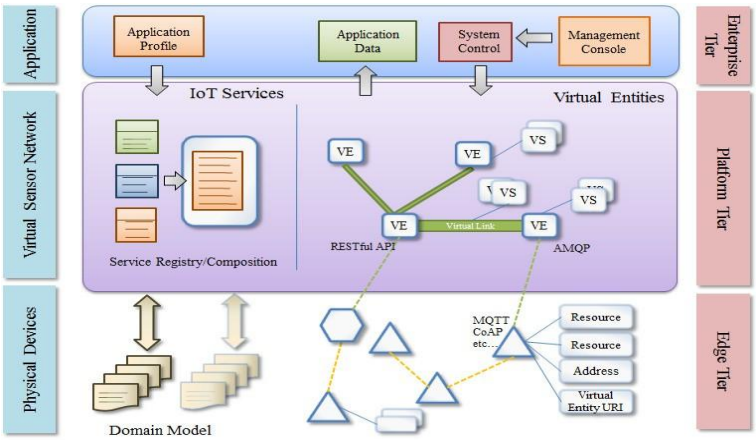

Fig. 1. WSN Management Framework

This readily maps to WSN topologies where the gateway acts as an endpoint for the WAN and manages the edge devices in the WSN. We view this implementation pattern as being akin to the edge tier in the three tier architecture pattern with the gateway being responsible for managing local connectivity, data processing and remote device management. To address the need for seamless integration and management of WSN in IoT ecosystems we have developed a framework that maps across the three tier implementation pattern for IoT systems. Fig. 1. presents an overview of the proposed management framework, on the left defines the typical layers of WSN, and on the right of the figure shows the relationship between these and the three tier implementation pattern for IoT systems.

The edge tier consists of the physical devices (sensors and actuators) which can extract data from and interact with the environment in which they are deployed. To fit with the requirements of IoT applications, it is expected that each device is IP addressable and has a connection to the internet. This may be directly (via application middleware such as CoAP) or is via gateway mediated edge connectivity (or internet bridge). The device layer can interact with the platform tier via a number of communications mechanisms including but not limited to AMQP or RESTful APIs. In order to effectively manage the physical infrastructure the platform requires knowledge of the domain specific deployment, including a semantic

representation of the device, application and network specification (sensors, actuators, duty cycle, sensing period, frequency, channel, transmit power, communications protocol, etc). The platform tier is composed of a service layer which acts a mediator between IoT applications and the physical infrastructure and a set of virtual entities that abstract from the underlying edge tier. The service layer was developed based on an event driven architecture combined with dynamic service composition and invocation principles. The objective of this layer is to provide a scalable, distributed and extensible computational platform that enables the interoperability of heterogeneous embedded systems, orchestration of resources, complex event processing and to make this processed information accessible to IoT applications and services that sit within the enterprise tier.

From an enterprise perspective the platform therefore serves the purpose of providing an abstraction layer between the sensor/actuators subsystems and the application and from the hardware provider (or system integrators) perspective the platform provides controlled access and interaction to the devices, context information extending their service offering beyond a bespoke WSN solution to a multi-tenant application paradigm. In addition by integrating with the platform infrastructure providers can offer scalability, distributed processing capabilities and management functionality as part of their solution. The components of the platform tier can be distributed over the network (gateway device) or deployed within the cloud. The backbone of the platform is a reliable communications infrastructure provided by transparent message services (AMQP). The components used within the platform (database server, message broker, webserver) are all based on off the shelf components with the ability to run on a cluster, therefore these technologies can be easily interchanged where required without further modifications to the platform. A key component of the platform is the Virtual Entity (VE). In the context of IoT a VE is primarily targeted at abstracting the heterogeneity of the technology and can be considered a virtual representation of the physical device. However within the context of the proposed framework we move beyond a simple virtual representation of the real world object and include cognitive capabilities to effectively compose an intelligent agent to mediate and manage the physical WSN within the context of service demands and system capabilities. Fig. 2. shows the functional composition of a VE that represents a wireless sensor. A standard the agent encapsulates interfaces for communication between other entities and services based on message broker (e.g. MQTT, RabbitMQ) and external entities via internet standard (e.g. REST), resources can be composed of network resources (i.e. other IoT services) and device resources (physical device mapping). Depending on the requirements and capabilities of the agent they can extend/reduce the services they are composed of. Other important components include the model of the entity it represents within the physical world and any additional metadata to support intelligent management (e.g. access control, security policies). It is envisaged that by local interaction between these virtual entities will enable the emergence of more reliable, re-usable and accessible infrastructure that meets disparate quality of service (QoS) expectations. The enterprise tier enables developers to specify application requirements through the use of platform support tools, these include web based tools that allows application providers to select of data sources, manage access control policies, access API's of VE and deploy processing services. In addition a management tool is provided to the owner of the physical infrastructure to monitor the status of the devices, network and mange system configuration and failures.

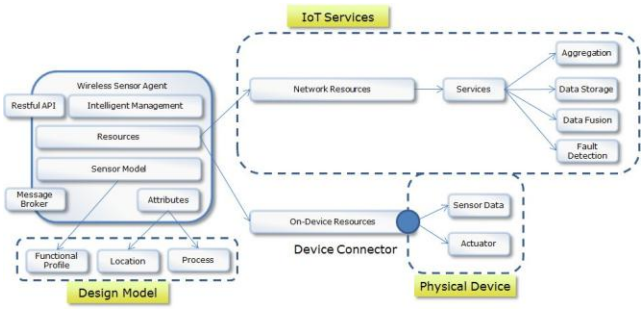

Fig. 2. WSN Virtual Entity

IV. INITIAL IMPLEMENTATION

This section presents the initial realization of the proposed framework and its application to the development of a WSN Health Monitoring system. In the case of WSN-Health monitoring, there are a number of stakeholders that are interested in visualizing system performance, including the wireless sensor network engineer, systems integrator or facility manager. Therefore it is important to create an easy to use tool to present the current status, on-going performance and health of the deployed network usable even for those with little experience in wireless systems. This includes the development of common management functionalities (e.g. Health/QoS Monitoring, Data Distribution, Fusion, Storage and Fault Detection) that were deployed as IoT services and incorporated into a web-based management interface. The following describes how the tool has been used to manage a real world deployment covering the three tier architecture.

A. Edge Tier

The edge tier consists of a number of sensor devices that monitor environmental parameters including as temperature, light levels and humidity. The TelosB multi-sensors from CrossBow were used for testing the tool. They operate with ultra-low-power with a small battery pack enabling long term deployment and utilize TinyOS running a 6LoWPAN stack with a customized sensing application that includes network statistics and topology related data. Each sensor is connected to a base station linked to an embedded PC which acts as a mediated gateway for the platform and the physical deployment.

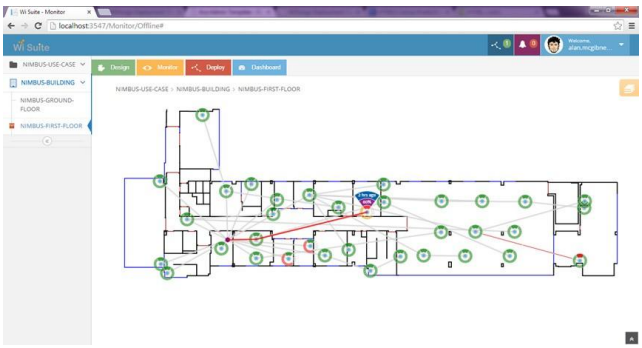

Fig. 3. Sensor Network Deployment at Commissioning Phase

The deployment building consists of two floors with a footprint of approximately 1,632m^2. The building hosts a number of labs, offices and large open office and laboratory spaces. The wireless sensor network was deployed across both floors of the building. This resulted in the deployment of 56 sensors plus 2 gateway devices. Sensors are configured to sense and report data every five minutes and network statistics every thirty minutes. Fig. 3. shows the positioning of the devices within the first floor of the building and demonstrates how the management services can be used at deployment time to commission the network and ensure all devices are connected.

B. Platform Tier

The platform consists of a number of network management services used to proactively analysis and present the network performance to the user. As data generated from the network is published into the WSN health monitoring framework, it is distributed to a number of analysis processes, for example a device agent acts as an independent monitoring service creating a virtual representation of the physical node, a client (visualization or analysis service) can then subscribe for this information over the platform communications mechanism (RabbitMQ) which in turn is published on each update. The agent may perform some data processing e.g. calculation of packet reception rate, and maintain this for continuous analysis. A similar approach is taken for managing the network links. In addition to the current status, an analysis service such as propagation model tuner and topology modeler which can take real time data and use it as decision support for future system design, extensions and simulation.

The tool is easily extensible to include other services such as fault detection and diagnosis. This component offers design support by providing actionable recommendations on the network topology and architecture. The tool offers real time alarm and event monitoring with prioritized alert reporting and automated notification supporting the maintenance of the infrastructure. Fig. 4. provides an example of a fault that has been detected and reported to the user, the user can login to the system dashboard and view the status and activity history of the device (e.g. Packet reception rate, battery status, last message received etc).

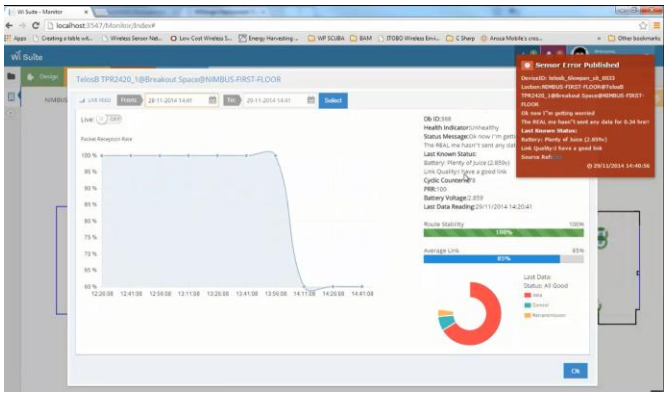

Fig. 4. Alert manager and device history dialog

Each alert provides a recommended course of action, for example if no packet has been received for a defined period the system will automatically verify the battery level at the last reading, check neighboring nodes for activity provide a suggested cause of failure and remedial steps that are required by the system manager. Any changes in deployment configuration made by the user including the addition, removal or re-positioning of devices is captured through the web-based interface and committed to the domain model once completed. As a result all other tools and services maintain a consistent view of the system configuration, this assures change control and risk assessment by ensuring the system model is maintained based on actions taken by the user.

C. *Enterprise Tier*

The enterprise tier consists of a software interface to remotely access sensor and statistic data extracted from the network and visualize it within the context required. This includes a data dashboard to provide a quick overview of the system status, data overlaid on a floor plan map, data graphs and time series analysis graphs. The tool front end was designed using a responsive design template using HTML5. Bi- directional communication with the platform tier is realized through the use of a *WebSockets* interface. This implementation approach enables the visualization tool to be used on a number of end-user devices be it a PC, tablet or smart phone. The dashboard view as shown in Fig. 5. presents the user with an overview of the complete deployment of a selected project and building (by default a period of 24 hours is selected). Performance metrics are presented in graph format to create an instant view of the status of the wireless sensor network; metrics such as packet reception rate, route stability, network lifetime and traffic distribution are included. The dashboard also presents a breakdown summary of the number of active devices with inline charts identifying problem devices by building floor giving the user an efficient mechanism to assess the current status of the overall network. To drill down further into the performance of the network the user can use the monitor view (Fig. 6.). From this view the user can select a specific building and floor plan and load the current deployment configuration from the domain model. The device configuration is then overlaid on to the map of the environment showing the exact position of each device.

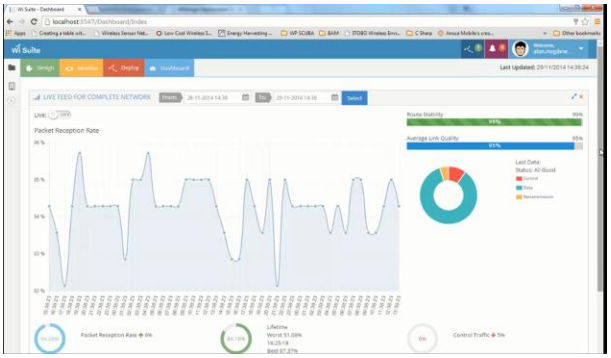

Fig. 5. Dashboard View

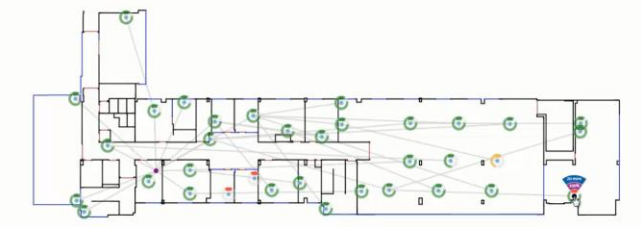

Fig. 6. Monitor View

When the deployment is loaded the current status of the device is shown. This highlights the current battery status and overall health of the device, if the user places their mouse over the device more information is provided such as name of the further summary is provided which indicates the cyclic counter of the device, current packet reception rate and the delta time of last message received.

V. CONCLUSION

This paper presented a reference framework for realizing a management approach which will seamlessly integrate with future large-scale IoT deployments. The framework promotes an encompassing approach to WSN infrastructure management that mediates between the requirements derived from IoT applications and the physical infrastructure via a management as a service platform. An initial realization of this framework has been developed and applied to a WSN health monitoring toolset which overlays the three tiers of IoT reference architectures. In future work it is planned to enhance this implementation with additional services to facilitate a distributed and collaborative management approach to enable self-management of smart objects to ensure robustness and reliability in IoT infrastructures.

ACKNOWLEDGMENT

The authors wish to acknowledge the support of the EU Commission under the FP7 GENiC project (Grant Agreement No 608826) in part funding the work reported in this paper.

REFERENCES

[1] J.F Gómez-Pimpollo, R. Otaolea, "Smart Objects for Intelligent Applications - ADK", IEEE Symposium on Visual Languages and Human-Centric Computing, 2010, pp. 267-268.

[2] K. Aberer, M. Hauswirth, A. Salehi, "Infrastructure for data processing in large-scale interconnected sensor networks", Proceedings of Mobile Data Management (MDM), Germany, 2007.

[3] D. Le Phuoc, H. Mau Quoc, J. X. Parreira, M. Hauswirth, "The Linked Sensor Middleware - Connecting the real world and the Semantic Web", Semantic Web Challenge 2011, ISWC 2011.

[4] M. Eisenhauer, P. Rosengren, P. Antolin, "A Development Platform for Integrating Wireless Devices and Sensors into Ambient Intelligence System", Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2009.

[5] V. Foteinos, D. Kelaidonis, G. Poulios, P. Vlacheas, V. Stavroulaki, P. Demestichas, "Cognitive Management for the Internet of Things" IEEE Vehicular Technology Magazine, December 2013.

[6] F. Kawsar, K. Fujinami, T. Nakajima, "Prottoy Middleware Platform for Smart Object Systems", International Journal of Smart home Vol 2, No 3., July 2008.

[7] J. Mineraud, O. Mazhelis, X. Su, S. Tarkoma, "A gap analysis of Internet-of-Things platforms", arXiv preprint arXiv:1502.01181,2015.

[8] D. Christin, A. Reinhardt, P. Mogre and R. Steinmetz, "Wireless Sensor Networks and the Internet of Things: Selected Challenges", Proceedings of the 8th GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze", Hamburg, Germany, 2009.

[9] J. Dominguis, A. Damaso, R. Nascimento. and N. Rosa, "An Energy-Aware Middleware for Integrating Wireless Sensor Networks and the Internet", International Journal of Distributed Sensor Networks, Volume 2011.

[10] M. Kosanvc., M. Stojcev., "Connecting Wireless Sensor Networks to Internet", Facta Universitatis, Mechanical Engineering Series, Vol. 9, pp 169-182, 2011.

[11] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin,"IOT Gateway: Bridging Wireless Sensor Networks into the Internet of Things", Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010.

[12] W. Colitti, K. Steenhaut., N. De Caro, B. Buta, V. Dobrota, "REST Enabled Wireless Sensor Networks for Seamless Integration with Web Applications", Proceedings of the eight IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, 2011.

[13] M. Kosanvc, M. Stojcev, "Connecting Wireless Sensor Networks to Internet", Facta Universitatis, Mechanical Engineering Series, Vol. 9, pp 169-182, 2011.

[14] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP)", CoRE Working Group, Internet- Draft, draft-ietf-core-coap-18, Expires December 2013.

[15] L. Mainetti, L. Patrono and A. Vilei, "Evolution of Wireless Sensor Networks towards the Internet of Things: a Survey", Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2011.

[16] J. Gubbia, R. Buyyab, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Elsevier Journal on Future Generation Computer Systems, 2013.

[17] R. Giaffreda, "iCore: A Cognitive Management Framework for the Internet of Things", Springer Berlin Heidelberg, 2013.

[18] J. Kim, and L. Jang-Won, "OpenIoT: An open service framework for the Internet of Things." Internet of Things (WF- IoT), 2014 IEEE World Forum on. IEEE, 2014.

[19] W. L. Lee, A. Datta, and R. Cardell-Oliver, "Network management in wireless sensor networks." Handbook of Mobile Ad Hoc and Pervasive Communications: American Scientific Publishers (2006).

[20] D. Dudkowski et al. , "Architectural Principles and Elements of In-Network Management ", Proceedings of the 11th IFIP/IEEE International Symposium on Integrated Network Management, 2009.

[21] Industrial Internet Consortium, "Industrial Internet Reference Architecture", http://www.iiconsortium.org/IIRA-1-6.pdf, last accessed 07/08/2015.

[22] Internet of Things-Architecture (IoT-A), http://www.iot-a.eu/, last accessed

07/08/2015.