International Journal of Multidisciplinary Research and Modern Education (IJMRME)
ISSN (Online): 2454 - 6119
(www.rdmodernresearch.org) Volume I, Issue II, 2015

IOT ECOSYSTEMS WITH WIRELESS SENSOR NETWORKS

Vijayamala S Yakri
Krupanidhi Group of Institutions,
Bangalore, Karnataka

Abstract:

In the Internet of Things, there is an expectation that computers will always be connected and data will always be available, but the actual devices generating those data streams are not very concerned. The demand for data must be matched with the limits and resources of the physical facilities funded. This paper provides a management system for IoT sensor networks. This architecture will help build several virtual networks that use the same physical infrastructure to exchange services, contexts, insight etc to fulfill complex service needs. This is the framework by collaboration and agreement.This involves moving from conventional management approaches based on centralized management for tailor-made solutions to modern approaches for autonomous management across hierarchical intelligent gateways, which proactively track and control IoT WSN infrastructures to serve many vertical applications.

Key Words: Reference Architecture, Virtual Sensor Networks, Virtual Entity, IoT Management Framework

Introduction:

Wireless sensor and actuator networks (WSNs) are seen as a crucial technology to bridge the gap between physical and virtual environments in IoT where IoT will interconnect real-world objects (RWOs) and enable connectivity and communication to shape new applications. WSN has several proprietary and non-proprietary solutions which have contributed to a static one-on-on-one partnership between the WSN devices and the case of operation. This strategy driven by the script has led to the WSN being knowledge silos that inhibit their influence and stifle the broader implementation of these networks, with minimal access to the external world. A robust ecosystem of intelligent software with different demands and specifications is a precondition for IoT's provision of a generic infrastructure.

At present the focus of IoT was greatly on the service layer and beyond the effect on the management of the underlying physical infrastructure by IoT services is not taken into account (sensors, actuators, networking, communications, data quality, security and privacy). Many of the available technologies are typically able to a sequent data modeling, delivery, service development and exploration using the underlying hardware. The general consensus is that the IoT will contribute to the seamless interwoven of thousands of embedded devices into our daily lives, and to make the most of this, the group must step away from tailor-made vertical technology implementations and include more broad approaches to IoT systems development, implementation and management.

The opinion in this article is that the management of the supporting WSN systems and facilities it supports cannot be decoupled to do this in an increasingly flexible manner. These technologies can fix concerns like resource optimization, dispute resolution, accessibility and wide scale, distributed geographically heterogeneous application networks. This is not a trivial job, but can also draw on current solutions and technology (distributed middleware, virtualization, networking tools, federated networking, orchestration and provisioning etc to help create an infrastructure management strategy for IoT applications. The IoT framework is a non-trivial approach.

Literature Review:

WSNs are usually embedded in IoT platforms to provide a data-centered mechanism for IoT operation. This allows content-rich apps to be developed; however these applications are not at least very closely connected to physical infrastructure services. A sequence of autonomous management tasks that combine the setup, operation, protection, administration and maintenance of all elements on the IoT network must be supported by continued multitude of connected device numbers. The hierarchical aggregation and autonomous control of artificial objects is important for IoT implementations. However, conventional network management cannot be converted directly if the Current administrators often need manual setup and tuning.

The physical unit may be abstracted as a simulated object and reused outside its original context. There are several various platforms and strategies suggested as mediators between sensors and data users, some of which include data wrapping and semantin interoperability [1, 2], middleware [2, 3, 4], virtual object repositories [5], [6]. The need to re-provide the technology to satisfy application, protection and data ownership requirements is one of the main challenges posed by a difference review of the representative samples of the IoT systems currently available.Middleware systems can also support lower latency (e.g. by edge analytics) and increased IoT system energy performance. In order to ensure smooth, cross-platform integration, the supply of SDKs and implementation assistance is also essential. With IP-enabled applications, however the need to provide a more stable/encapsulation system is always sufficiently strong for incorporating sensors into the Internet [7].

The ultimate aim, however, is not yet realistic to provide a completely IP-based network, owing to the restricted existence of the devices' resource and the fundamental gaps in connectivity with the wireless sensor network. The creation of Middleware Platforms [8] or Internet Bridges [9], [10] has therefore been strongly emphasized in order to allow connectivity to the network from the application layer.REST or RESTful methods like [11, 12] are becoming ever more common. Recorded State Transition (REST) for example, the IETF [13] Restricted Embedded Application Protocol (CoAP) facilitates the full use of the current, well-defined http specification to optimize and mitigate the inclusion of new application-specific functionality. Many embedded devices have no memory, computing speed, or lifespan, so this capability is usually abstract and deployed on the internet.Turning end devices into RESTful tools allows create physical mash-ups [14] in relation to heterogeneous end devices, yet little consideration has been paid to how to push all these devices into the IoT environment, supposing that data are still accessible and that the net-smart artifacts will deliver stable data without becoming concerned.

A significant feature of IoT systems is that it is multi-service, which supports several different programs or utilities by nature. This includes the ability of a single network to manage a variety of applications without sacrificing on performance [15], as opposed to different forms of traffic in the network. A full separation of the underlying networks of virtual entities allows various network technologies to be built to satisfy different IoT applications needs and specifications utilizing the same infrastructure.In recent years there have been various IoT marketplaces that use network virtualization and smart object virtualization to offer end-to-end services without taking into account network capabilities or status and their elements. From the end-user point of view, the infrastructure at the bottom can be perceived as a stand-alone and self-management system.

By generating policies, which include a sequence of rules to meet applications specifications, the conversion of application requirements to the underlying infrastructure can be carried out. Another factor to be addressed is network management; iCore [16] provides the basis for representing, capturing, writing and exploring virtual entities to support many IoT-based applications within the same networks. Likewise Open IoT [17] offers context-aware arrangements for the classification of intelligentsia in order to determine their relevance to application needs; it is recognized that many middleware frameworks provide simple search functionality (proximity and sort of data) and are used to support the project.

A standard IoT app includes joint publication of data from a distance (either directly or over an internet bridge), data processed in a data warehouse and transmitted to cloud services of third parties. This offers a modular approach and facilitates the creation of content-rich applications; however, beyond the framework of IoT, the underlying architecture also remains in place and is handled locally.In order to maintain an expected level of service (QoS), IoT technology such as the Wireless Sensor Action Network (WSN) must have a variety of control functions combining the setup, operation management, safeguard and maintenance of all network elements [18].

Traditional sensor network control systems usually have a central network management view and are centrally situated in management stations from the network itself. Control stations are hosting applications to communicate nearly per system across protocols like SNMP, TMN, and OSI-SM to extract performance measurements (e.g. packet counter, latency), or to insert commands to help setup, malfunction, performance, and protection management. However these networks are slowly emerging with minor improvements in interfaces or processes as compared to IoT services. One significant benefit of IoT systems is that they are multi-service by default; serving a variety of common demands or programs. This includes the ability of a single network to manage a variety of applications without sacrificing on performance [15], as opposed to different forms of traffic in the network. In this situation it easily becomes impervious to a centralized approach to network management.

A number of management issues have been discussed at the different levels by current wireless network sensor management techniques, which can include sensor network management mechanisms (BOSS, MANNA), sensor network management protocols (RRP, SNMS, sNMP), QoS Aware Routing (SAR, Energy Aware Routing, Pace, Mobicast, RPL), delegate management (Agilla, Agent-Base). These methods and protocols play a major role in ensuring reliability, and in developing the wireless IoT sensor networks the type of protocol used needs to be taken into consideration to allow the infrastructure to be efficiently handled.

While considerable progress has been accomplished in recent years in the areas of hardware design, device architecture, Protocol Design and power management to enable the implementation and maintenance of wireless sensor networks, the distinction being that it seeks to expand, improve and integrate current management principles directly into an IoT architecture. WSN can no longer improve its management functionality as an additive to the service offered rather than an integral part of the framework delivered in IoT. Future IoT allows WSN to be regarded as an autonomous network for large-scale infrastructure encompassing data management, processing, performance and analysis. They can also become more context conscious and lead to the QoS delivery of the whole IoT system.

IOT Management Framework for WSNs:

No architecture suits all of the IoT applications areas and the different specifications of these areas. However for driving IoT technology and application creation a modular scalable architecture which supports widespread case application and abstracts common functionalities and features is required. IOT-A and IOT-A lead in the promotion of an architectural approach to IoT, sharing similar goals: development of a baseline model that promotes a shared definition of IoT (IoT-A) and a baseline architecture that offers a common framework for designing interoperable IoT device architectures (IIC, IoT-A). The three-tier patterns and the gateway-mediated edge networking and design pattern are the most typical implementation patterns found by the IIC. The three levels are the business, platform and edge levels. The corporate level handles domain-specific software, end-user interfaces, gathers platform and edge levels data and operates controls on the lower levels. The platform level controls the edge system control and manages data stream from the edge level. The edge level gathers data from boundary sensors. The connectivity gateway and management design pattern for managing the connectivity of end devices is characterized as a regional connectivity approach for gateways to link to a broad area network (WAN).

The gateway is an easy terminal for WSN and handles edge devices in the WSN, hence maps WSN topologies. We consider this paradigm as being close to the edge level in the three-tier architectures and the gateway handles local linking, data processing and remote system administration. To learn on a methodology has been developed to chart the three level deployment trends of IoT frameworks for the smooth integration and management of WSN in IoT ecosystems.

The edge tier consists of physical instruments (sensors and actuators) that can isolate data from the environment they are used to communicate with. It is required that each system has IP-addressed access and an internet connection in order to fulfill the specifications of IoT applications. This can be directly (using middleware such as CoAP) or via a gateway communication controlled edge (or internet bridge). A variety of communication mechanisms, including AMQP or RESTable APIs, allow the device layer to communicate with platform level.It aims to include a modular, distributed and extensible computer-based architecture that allows heterogeneous embedded systems to be interoperable, resources can be coordinated, the management of events is dynamic, and to allow the knowledge processed available for IoT applications and corporate services.

Therefore, from an enterprise standpoint, the framework provides a dividing point between sensor / actuator subsystems and the application and the platform provides managed access and contact with the sensors from the viewpoint of hardware vendors (or system integrals), background knowledge that expands its operation spectrum to a multi-controlled solution beyond a single WSN one. Furthermore the integration of cloud vendors with the platform will deliver as part of their solution scalability, distributed computing capabilities and management functions.The framework modules may be delivered across the network or implemented in the cloud. The foundation of the network is a secure framework for connectivity through clear messaging services (AMQP). The modules that are used on the framework (database server, message broker, webserver) are built on shelf components that are capable of run on a cluster, and can thus be quickly replaced as required without external platform modifications.

The Virtual Agent is a core component of the platform (VE). For IoT, a VE mostly targets the abstraction of technical heterogeneity and can be viewed as a simulated

image of the physical unit.But we go beyond easy, virtual representation of the real world object in the sense of the proposed architecture and provide cognitive abilities to efficiently build a smart mediator and handle the physical WSN in relation to service specifications and device functionality. A common Agent encapsulates communication interfaces with other organizations and networks based on message broker (e.g. MQTT, RabbitMQ) and external entities via internet standard (e.g. REST), network resources (i.e.) and system resources (physical device mapping). They will extend/reduce resources they are made of, according to the agent's specifications and skills. The model of the organization within the real environment and all other metadata to facilitate intelligent management are other essential components (e.g. access control, security policies). The plan is to allow the creation of a more trusted, reusable and open infrastructure that meets the diversified service quality (QoS) standards by local engagement between these virtual entities. The organization level allows users, using platform management tools, to define application criteria, including web-based tools to help applicants pick data sources, handle access monitoring policies, access VE APIs and deploy processing services. The owner of the physical infrastructure also has a maintenance tool for tracking computer status, network and system setup and errors.

Initial Implementation:

The first implementation of the frame and its extension to the development of a health monitoring framework for WSN are discussed in this section. With regard to monitoring of WSN-Health, a variety of stakeholders, including a wireless network engineer, system integrator or facility manager, are involved in visualizing system output. Therefore it is necessary to build an easy-to-use tool to demonstrate the current state, continuous efficiency and health of the network installed even for those with minimal wireless device experience. It involves improving the standard management features for the use of IoT resources and the integration of an internet-based management interface (i.e. health/QoS monitoring; delivery of data, merge, and storage and default identification). The following discusses how the tool has used the three level architecture for handling a real world implementation.

A. Edge Tier:

The edge stage consists of a variety of sensor systems, including temperature, level of light and humidity, which track environmental parameters. Cross Bow's TelosB multi-sensors were used for instrument testing. They run on ultra-low power with a compact battery pack that permits long-term deployment. They use TinyOS with a 6LoWPAN stack that provides network statistics and topology-related data with its custom sensing program. Each sensor is attached to an embedded PC base station, which serves as a mediated platform gateway and physical deployment. The building consists of two floors with a surface area of around 1,632m2. There are a number of classrooms, offices and big open office and research areas in the building. There were two floors of the building with the wireless sensors network. This lead to 56 sensors and 2 gateway systems being deployed. Every five minutes the sensors and network data are programmed to be sensed and registered.

B. Platform Tier:

The framework includes many network monitoring services that are used to provide the customer with constructive analyses and network performance. When data created from the network is released in the Health Tracking System, it is transmitted through a set of analyzing mechanisms. For instance, the computer agent acts as an autonomous monitoring service that produces a graphical representation of the physical node. The organization can conduct such data processing e.g. measurement of

the receiving rate of packets and hold it for ongoing study. For the maintenance of network communications, a similar approach is taken.In addition to the current scenario, an analytical service like propagation model tuner and topology modeler will take real-time data and use it for decision making in the design, extension and simulation of future systems.

Other resources such as error detection and diagnosis can be quickly added. This part helps the design by presenting effective recommendations on the topology and layout of the network. The tool delivers real-time warning and incident tracking with priority alarm notifications and automatic notification enabling infrastructure management.

For e.g., if no packet was received within a given time span, each warning will automatically check the battery level at the last lecture, the nearby operation nodes will be verified, and a suggested cause of failure, as well as remedial action that the system manager requires. The administrator shall document all modifications in the user's deployment setup including devices inclusion, elimination or repositioning, and commit to the domain model until it is done. The web-based interface may be used. This ensures the monitoring and the risk estimation of the adjustment by ensuring that the system model is retained according to behavior done by the customer. All other tools and resources maintain clear vision of system configuration.

C. Enterprise Tier:

The organizational level consists of a machine interface for remote access and display of sensor and statistical data derived from the networks. This provides a summary of device state, the data on a map of floor plans, data analyses and time series measurement graphs. This includes a data dashboard. The front end of the tool was designed using an HTML5 interface template. The two-way contact with the platform level is rendered using a Web Sockets Gui. This approach allows the display method to be used on multiple end-user computers, such as a PC, a tablet or a Smartphone. Output measurements are displayed in graphical format to provide the wireless network sensor status with an instant view; metrics such as packet reception rate, path stability, network existence and traffic distribution are used.This helps the user to pick a particular building and floor plan and load from the domain model the latest implementation setup. The configuration of the device is then overlaid on an area map that displays each device's exact location. The current state of the system is shown when the deployment is loaded. This shows the current state and overall health of your system as you position the cursor over the device. For example, the name of the next overview is given which demonstrates the device's cyclic counter, the current receipt rate of the packet and the last message's delta time.

Conclusion:

This paper offered a foundation for a management strategy that fits smoothly with potential IoT implementations of a wide scale. The Architecture supports an interconnected approach to WSN technology management, through the management of a service network, which mediates between IoT applications' specifications and the physical infrastructure. This system has been initially developed and used for a WSN health surveillance toolkit, which overlays three layers of IoT architectures. In potential ventures, additional resources are expected to improve the distribution of smart objects in order to promote an efficient and collaborative management approach, which assures the robustness and efficiency of IoT infrastructures.

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. F. Kawsar, K. Fujinami, T. Nakajima, "Prottoy Middleware Platform for Smart Object Systems", International Journal of Smart home Vol 2, No 3, July 2008.
6. J. Mineraud, O. Mazhelis, X. Su, S. Tarkoma, "A gap analysis of Internet-of-Things platforms", ar Xiv preprint ar Xiv: 1502.01181,2015.
7. 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.
8. J. Dominguis, A. Damaso, R. Nascimento and N. Rosa, "An Energy-Aware Middle ware for Integrating Wireless SensorNetworks and the Internet", International Journal of DistributedSensor Networks, Volume 2011.
9. M. Kosanvc., M. Stojcev., "Connecting Wireless Sensor Networks to Internet", Facta Universitatis, Mechanical Engineering Series, Vol. 9, pp 169-182, 2011.
10. 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 onEmbedded and Ubiquitous Computing, 2010.
11. 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 SensorSystems, 2011.
12. M. Kosanvc, M. Stojcev, "Connecting Wireless Sensor Networks to Internet", Facta Universitatis, Mechanical Engineering Series, Vol. 9, pp 169-182, 2011.
13. 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.
14. 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, Tele communications and Computer Networks (Soft COM), 2011.
15. J. Gubbia, R. Buyyab, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, andfuture directions", Elsevier Journal on Future GenerationComputer Systems, 2013.
16. R. Giaffreda, "iCore: A Cognitive Management Framework forthe Internet of Things", Springer Berlin Heidelberg, 2013.
17. J. Kim, and L. Jang-Won, "Open IoT: An open service frame work for the Internet of Things." Internet of Things (WFIoT), 2014 IEEE World Forum on. IEEE, 2014.

18. W. L. Lee, A. Datta, and R. Cardell-Oliver, "Network management in wireless sensor networks." Handbook of MobileAd Hoc and Pervasive Communications: American ScientificPublishers (2006).