# A Self-Reconfigurable Sensor Network Management System for Internet of Things Paradigm

Rajan M.A, P. Balamuralidhar,Chethan.K.P , Swarnahpriyaah.M.
Innovation Labs, Tata Consultancy Services,
Plot # 96, EPIP Industrial Estate, Whitefield Road, Banagalore, India.
{Rajan.ma, balamurali.p, chethan.p, swarnahpriyaah.m}@tcs.com

***Abstract*—the Internet of Things (IoT) is the paradigm of inter connecting heterogeneous devices which are distributed globally and will be a part of the future Internet. Wireless Sensor Networks (WSN) are one of the integral classes of networks in the IoT. One of the major challenges to achieve IoT is to integrate and manage large heterogeneous networks. Autonomic network management system is the need of the hour to prop up successful implementation of IoT and it should be in sync with the existing Internet architecture and protocols for smooth and wider applications in IoT. Here we reviewed and proposed a novel heterogeneous and self optimizing sensor network management system which envisages energy saver, life time enhancer and flexible auto configuration of WSNs.**

***Keywords- Network Management System, Internet of Things, Wireless Sensor Networks.***

## I. INTRODUCTION

Internet of Things (IoT) is the paradigm of inter connecting heterogeneous devices around the world. The devices include things such as home appliances, vehicles, roads, smart materials needs to be addressable, manageable from the remote place through internet. The detailed study IoT[1] brings in the architecture framework, standardization. Since the number of devices networked around the globe is in millions, managing these devices are very difficult. Thus Network Management is very crucial for successful deployment and managing the IoT. The focus in the paper is on managing the special devices wireless sensor nodes which form the network themselves. In the future these wireless sensor networks will be part of IoT. Network Management System is an integrated system with hardware and software to manage the entities of the network. Specific to telecom, some of the entities are routers, switches, gateways and network elements. The aim of any NMS is to provide Fault tolerance, Configuration, Accounting, Performance and Security (*FCAPS*) to the user of the system. At an abstract level, NMS performs the automatic discovery, inventory and health monitoring of entities. Managing a sensor network is a daunting task when compared to the traditional telecom network management systems due to the limited bandwidth, transmission range and battery power of the sensors. A sensor network is an infrastructure less wireless self configurable network systems. Each sensor node is equipped with a transceiver capable of receiving and transmitting the data. The applications of sensor network are widespread. Earlier it was used only in the battle field. Now it is prevalent in almost all areas like medical field, nuclear filed, aerospace and home networking. Recently it finds application in farming, where the geo sensors are deployed in the farming field and the data collected from these sensors are sent to the agro experts. They do data analysis and based on it provides advice to the farmers related to farming and thus the farmer is benefited. Due to the cost effectiveness of sensors, sensor network is very much prevalent. Thus there exists a circumstance that thousands of sensors are deployed for some application. As a result of this some of the fundamental issues like configuring, controlling, managing widely spread sensors arises. It is not possible to manage individually manually. So there is a need for a sensor management system. Still today, we are not aware of any NMS standards of the SNMS. Thus this paper focuses on finding the fundamental issues, in the SNMS and provides a good architecture for the SNMS.

This paper is organized into several sections. Section II, the pros and cons of some of the existing network management protocols for SNMS are studied. Some of the issues in SNMS are analyzed in section III. The detailed SNMS architecture is proposed in section IV. In section V, novel self optimization SNMS architecture is proposed. Finally the conclusions are given in section VI.

## II. SENSOR NETWORK MANAGEMENT

### *A. SNMS protocols.*

There are many management protocols and architectures proposed for sensor networks in the literature from many different management perspectives: network-health monitoring, fault-detection, traffic management, congestion avoidance, power management, and resource management [13]. The systems are characterized by their power consumption, memory consumption, bandwidth consumption, fault tolerance, adaptability, and scalability. None of the reviewed systems in [13] provides a fully integrated view of all sensor network management design factors. Furthermore, most of these systems incorporate management functions within application protocols. The development of general purpose network management layer protocols is a challenging problem and remains a largely unexplored area for wireless sensor networks. Another significant open problem is the development of management policies and expressive languages or metadata for representing management policies and for representing the information exchanged between sensor nodes, managers, and end users.

When considering WSN for integrating to IoT, the management architecture and protocol should be seamlessly

978-1-4244-9190-2/11/$26.00 ©2011 IEEE

supporting IP. From this point of view SNMP is an important protocol to consider.

Simple Network Management Protocol (SNMP) [9], [10] developed in the late 1980's by ISO, is a widely used standard management protocol for traditional TCP/IP networks. However, there are several aspects of WSNs that make standard SNMP inefficient for WSNs. Firstly, the communication overhead associated with SNMP is too high for low bandwidth and low power wireless links for WSN. SNMP is based on a centralized approach where managed sensor nodes are polled frequently. Secondly, a Management Information Base (MIB) is required to be stored at each sensor node which is often limited in storage as well. Finally, sensor-specific failures, which are common in WSNs, are not handled effectively by SNMP.

The Ad Hoc Network Management Protocol (ANMP)[7] is for managing mobile adhoc wireless networks and it uses the hierarchical clustering of nodes in order to reduce the number of messages exchanged between the manager and the agents. ANMP is an extended SNMP which includes MIB extensions, dynamic configuration of agents, dynamic extension of the agents, and an application-specific security module. Guerilla [12] is another adaptive management architecture for ad hoc networks, which provides management flexibility and continuity by making its nomadic managers adapt to dynamic network conditions

The Management Architecture for Wireless Sensor Networks (MANNA) [11] provides a general framework for policy-based management of sensor networks. It gathers dynamic management information from the MIB and maps them into a WSN model. The WSN model is executed though management functions and services. However, one of these functions, MIB update a centralized operation, is extremely expensive in terms of communication overhead.

The Sensor Network Management Protocol, sNMP [8] is a management, which defines sensor models that represent the current state of the network and defines various network management functions. sNMP provides algorithms and tools for retrieving network state information through the execution of the network management functions. It is also an MIB-based framework like MANNA and have similar drawbacks of MIB based systems.

The Sensor Network Management System (SNMS) [13], is an interactive system for monitoring the health of sensor networks. SNMS provides two main management functions: query-based network health data collection and event logging. The querying system allows users to collect and monitor physical parameters of the nodes environment. The event-driven logging system allows the user to set event parameters which allow nodes to report their data only if they have met the specified event thresholds set by the user.

L-SNMS [14] is an improved scheme over SNMS [13] by incorporating an RPC (Remote Procedure Call) mechanism. The RPC mechanism additionally provides the user with the necessary support needed in order to access the functions and variables of applications running on the sensor nodes during runtime.

From the discussions so for from IoT perspective, to manage wireless sensors or devices across the globe through Internet, a heterogeneous sensor network management is the requirement.

### *B. Architectural considerations for WSN*

To manage a wide range of IoT based heterogeneous networks the usage scenarios are to be considered which requires that the node architecture must be flexible and adaptive these cluster of nodes are managed by the gateway. Each network will demand a slightly different combination of lifetime, sample rate, response time and in-network processing. Wireless sensor network architecture must be flexible enough to accommodate a wide range of application behaviors. Additionally, for cost reasons chosen of each device will be depended on the hardware and software need for a given application. The architecture should be easy to integrate the right set of software and hardware components. Thus, these devices require an unusual degree of hardware and software modularity while simultaneously maintaining efficiency. In order to support the lifetime requirements demanded, each node must be constructed with a robust architecture as possible. Wireless sensor network node has limited circuit area and computing power by its nature, hence a special architectural consideration is needed to design. Any typical IoT monitoring application can divide in to set of regular tasks such as, sensing, processing and generating the sensed data in to messages, sending radio messages and radio listening and sending if the node working as router , The below are the few features for a each sensor device in a network to support IoT based networks

- A Event-Driven System based node in which master components are involved With event handling to eliminate the event –processing over head
- A node should support standard mechanisms like Hardware Acceleration etc to improve the performance and power
- A sensor node is optimized for specific application
- Data processing / filtering should be done at the gateway to increase the life time of the node.
- A node has to be named with low-level naming to decrease the communication overhead.
- Since power is the main requirement for the sensor node and energy efficiency depends on the software running on it, there should be a power aware protocol to understand the power requirement by the system and runs application.
- And there are other futures like response time and accuracy wherein this helps to improve the system performance. Thus a sensor node designed by considering the above features certainly brings down the complexity of sensor network management with some processing overhead. Once sensor node has been designed the next challenge is to design a efficient, and intelligent gateway to process the data from different sensor nodes.

Innovation in gateways and the sensor nodes for data gathering and data processing and data storing in sensor networks is grabbing more attention in the recent days. A common requirement among all these data gathering and data processing networks is the need for one or more gateways to connect the WSNs with their remote sensors. Gateways which are in the monitoring application have few common tasks such as, Process the Raw data collected from the WSN, Managing a efficient and light weight data base for the WSN, transfer WSN measurements to remote users, help the user to command the WSN nodes, fault detection and alerting to the user. This functional commonality suggests the possibility of designing a common gateway platform. Equally important is the ability of the gateway to consume little energy, a feature which will benefit all deployments. We have carried out a small experiment to find out the energy consumption of a sensor node .the experimental setup involves two IEEE 802.15.4 compatible radio modules based on CC2430 from Texas Instruments. Both the antennas are quarter-wave monopole on small (finite) ground plane that is typical of modern mixed signal boards. One module is programmed for periodic data transmission. The data packet size is 20 bytes with a transmission interval of 100msec. The second module is put in receive mode and connected to a host PC, where it stores the RSSI values corresponding to the messages received from transmitting module. With the above setup we measured the following parameters as shown in the table I.

From the above measurements we could see that the energy consumption of a node is more while transmitting, receiving and a considerable loss while data processing .When there are more devices to be monitored and controlled it necessary to give more attention to managing these senor nodes intelligently in order to increase the overall life time of N/W. The fig-1 describes the software architecture with software components that should be presents in the gateway in order have a very efficient, less energy consumption, fast processing and robust gateway.

TABLE I. CURRENT CONSUMPTION OF THE COMMUNICATIONS NODES

| Equipment Current Draw | Mode | Table Column Head |
|---|---|---|
| ***Transmitter*** | ***Active(Tx is on)*** | ***40mA*** |
| | ***Processing*** | ***4mA*** |
| | ***Sleep*** | ***10 µA*** |
| Receiver | ***Active(Rx is on)*** | ***32mA*** |
| | ***Idle*** | ***3mA*** |
| | ***Sleep*** | ***8 µA*** |

## III. FEASIBILITY STUDY OF NMS FOR SENSOR NMS

It is evident form the previous section that, a good SNMS brings down the energy consumption in the sensor networks considerably with less overhead. In this section, a detailed analysis is done to choose or adopt from the existing NMSs to design a best possible SNMS. Current Network Management cannot be directly deployed as SNMS. In this section a rigorous study of the existing NMS are studied in order to design a good SNMS. A typical NMS architecture is a 3 layer system : The NMS, Element Management system (EMS) and network elements are distributed. This necessitates an interface protocol between them to communicate with its immediate lower/upper layers .Several interface options are available for the communication between the NMS and EMS. Some of them are 1. SNMP 2. CORBA. 3. Socket .4 Serial interfaces, 5. etc.. Though there are some rules or protocols to exchange the information or message exchange between these layers for SNMS are available, but needs to be streamlined. Prominent among them is sensorML (designed by NASA): an XML based standard developed to discover, process and locate the sensors. This type of interface can be used between EMS and sensor nodes. The standard Internet based interface available between two wireless devices is 6LOWPAN in which the sensor nodes are capable of IPV6 addressing.. Here the 802.15.4 data format is encapsulated and compressed to form an IPV6 format and vice versa. The design of SNMS depends on the type of protocol or interface used by the wireless networks. Some of the prevailing technologies or protocols in WSN are ZigBee, WHART, MiWi. etc all. There is a need of managing the heterogeneous WSNs under one roof. Thus a Heterogeneous Sensor Network Management System is the need of hour to manage IoT.

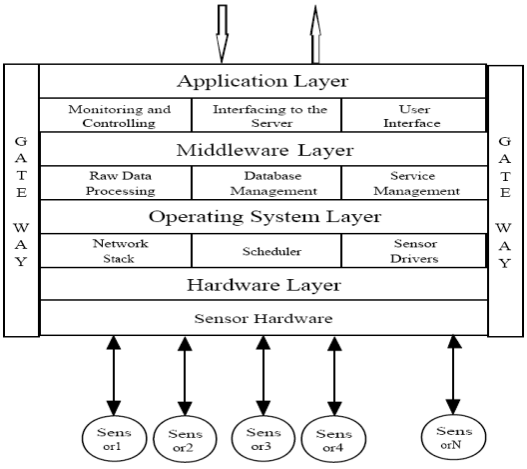


Figure 1. Sensor Gateway Architecture.

## IV. HETEROGENEOUS SENSOR NMS ARCHITECTURE.

### A. *Integrated SNMS Architecture*

Based on the previous section, a novel heterogeneous sensor network management is proposed with 5 layer abstracts. 1. Sensor User Interface Management (SUIM) 2. Sensor Security Management. (SSM). 3. Sensor Network Configuration Management.(SNCM) 4. Sensor Node Management (SNM) and 5. Gateway Management (GM). This architecture supports management of heterogeneous WSNs under one roof, where the heterogeneous is with respect to the type of management or interface protocols of the WSNS. This is very optimum with respect to IoT ,because the locally networked things are capable of interfacing with outside world through their own interfaces. The functionality of the each management layer is as shown in the figure 2. The SUIM is capable of managing user aspects of the system such as sensor display, user authentication and context sensitive query processing. The SSM provides the security management features such as 1.

Physical security of the sensors: Alert the user about the sensor displacement or theft. 2: Data tamper proof. 3: Sensor Authentication: Any sensor which is introduced to the network has to be first authenticated through authentication management and then starts participating in sensor network activities. The SNCM handles network configuration, topology management, and data collection scheduling and sensor power management. The SNM performs activities such as new sensor discovery, sensor configuration, failure discovery, sensor database synchronization and sensor data processing. The heterogeneous GW takes care of gateway configuration or federation, gateway poling and an interface between the SNMS and the gateways. Besides this, it performs command generation to manage the sensors and event notification processing. It is capable of handling heterogeneous interfaces like SNMP,CORBA, etc….at the same time. So for from the discussion, different kinds of management are supported by this architecture. This necessitates the need of different message structures to handle these management operations. In the next subsection, various interfaces, message formats for some of the management operations are discussed.

### *B. Interfaces, Messages and Flow for SNMS*

The proposed 5 layer in SNMS management is grouped into user, SNSM and Gateway cores. The user core has user Interface Management operations. The SNMS core comprises SSM, SNCM and SNM and the gateway core has gateway management components.

#### *1) Interfaces.*

Except gateway core, other cores have an interface with Database Management System. The interface between the gateway core and the gateways can be through the standard interfaces like SNMP, CORBA, COM/DCOM and etc... For the simplicity, the interfaces assumed to be SNMP. The interface between the cores is through Inter process communication like message queues, semaphores and shared memory. The cores can be distributed or reside on single server.

### *C. Message Structures.*

The following four basic message types are designed for the smooth functioning of SNMS: 1. the command message frame, 2.Name-Value Frame, 3. Sensor Synchronization message Frame and 4. Sensor Event Reporting Message Frame. The command message frame (in fig 3a) has 5 fields 1. Tx#: Transaction Id is a unique id for each transaction (management operation).2.Gateway # denotes the identification number of the gateway. 3. Sensor # is the unique id or name of the sensor that is generated from the gateways and inventoried at the SNMS. If the sensor id is Broadcast id (unique number like 0xFFFFF), then the command is a broadcast command applicable to all the sensors of the gateway. If the sensor id is Multicast Id (0x00000), then the command is a multicast command for the group of nodes. 4: Command is the actual command that should be issues the sensor or group of sensors and 5. Input Parameter: is the additional data or sensor related parameters (transmission power sleep duration) required to configure the sensor.

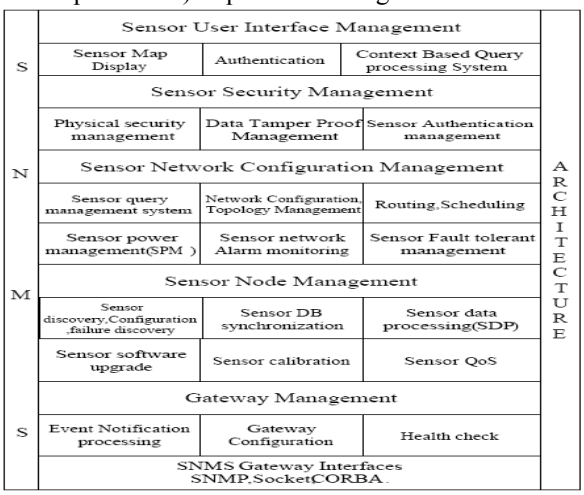


Figure 2. Heterogeneous SNMS Architecture.

The input structure typically in the form of name value pair is as shown in figure 3b. Using single command, one can configure multiple parameters of the sensor or sensors by specifying the details in the input field. The Name-value pair data frame (N-V-F) as shown in figure 3b has 3 fields 1. Length: is the number of name-value pairs 2. name1: denotes the name of the parameter. For instance name can be transmission range. 3. Value: is the actual value of the corresponding name parameter. So the N-V-F has list of N-pairs along with the length.

The Sensor synch message frame (fig-3c) is required to synchronize the information about the sensors between SNMS and the gateway. The entire data about the sensors under a gateway will be huge for large number of sensors, so the entire data Cannot be transferred to the NSM in a single stretch, instead the data is transmitted iteratively in bunches of frames. To facilitate this protocol, the frame has 6 fields: 1.Tx#: Transaction Number. 2: Gateway Id. 3. Length: Number of sensors' data in the frame. 4. Is End: This indicates whether the data transmission is complete or not if its' value is 1 or 0 respectively. 4: sid. Denotes the sensor id or name of the sensor.4: s-data: is the N-V-F which holds the information about the sensor such as neighbor information, transmission range, battery power and etc. The Sensor Event Reporting (fig-3d) message frame is designed for handling events reporting from the sensors to SNMS through gateway. This frame is a generic design which accommodates any type of events. It has 6 fields: 1.Et#: is the event number generated by the gateway. 2. Gateway id. 3. Sensor id. 4. Event Type: indicates the type of event like alarming or configuration change or neighbor change etc… 5. Event data: is the data related to the event and 6. Time: is the time of the event generated These messages can be implemented as XML frames and these XML frames can be converted into specific protocol requirement. For instance, these frames can be converted into MIBs and through MIBs the sensor

management is done through gateway, where it is enabled with SNMP protocol. Similarly equivalent IDLs are generated

| TX # | Gateway ID | Sensor ID | Command | Input Parameter |
|---|---|---|---|---|

Fig. 3a : Command Message Frame

| Length | Name 1 | Value 1 | Name 2 | Value 2 | ..... | Value n | Namen |
|---|---|---|---|---|---|---|---|

Fig. 3b : Name-Value data Frame

| TX # | Gateway ID | Length | S1 id | S1 Data | ..... | Sn id | Sn Data | Is End..? |
|---|---|---|---|---|---|---|---|---|

Fig- 3c : Sensor Synchronization Message Frame

| Et # | Gateway ID | Sensor ID | Event Type | Event Data | Time. |
|---|---|---|---|---|---|

Fig- 3d : Sensor Event Reporting Message Frame

Figure 3. Message formats for SNMS

The ever growing complexity of systems will be unmanageable with the traditional manual approach. It will hamper the creation of new services and applications, unless the systems will show *self-** properties, such as *self-management, self-healing* and *self-configuration*. Towards higher reliability and resilience intelligent systems are being adopted for autonomic management. Distributed intelligence and cooperative approaches are an observed trend in this direction. The advantage of autonomic systems for managing complex wireless networks have been widely appreciated and extensive research is in progress towards cognitive networks. Architecturally there are various approaches explored such as centralized agent, hierarchical agents, peer-to-peer agents and control mechanisms such as policy-based and bio-inspired adaptation towards forming the autonomic control loop between network devices and control agents.

## V. AUTONOMIC SENSOR NETWORK MANAGEMENT SYSTEM (A-SNMS)

By integrating the concepts discussed so far a simplified architecture for an autonomic SNMS (A-SNMS) could be conceived as an intelligent control loop feeding on the environmental parameters, network state and application context measurements and synthesizing an optimal control strategy with respect to set goals at network level. This includes an optimization core accessing network state information through a suitable SNMS protocol along with various context parameters. Then the optimization engine computes the control parameters such that the set goals are met in an optimal sense subject to the constraints set as policies. Goals will include QoS targets, network lifetime etc. Policies will specify constraints such as network size, membership control, security settings etc. The simplified design is as shown in the figure 4.

## VI. CONCLUSION

The sensor network management is very essential for smooth management of the network and also it extends the life of the sensor nodes. The standardization of the management functionalities, message formats and interfaces are need of the hour. To achieve this goal a good heterogeneous and self optimized SNMS architecture and framework is proposed. Extensive study is under progress to design and implement the optimized framework that enables self-reconfigurable wireless sensor networks.

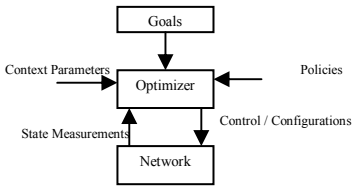


Figure 4. Simplified view of the system architecture

## REFERENCES


[1] Balamuralidhar P, Santosh Bothe, Prateep Misra, "Internet of Things", Chapter for the Book on "Future Trends in Wireless Communications", GISFI, *River Publications*, Feb 2010.

[2] The Internet Engineering Task Force (IETF), http://www.ietf.org

[3] R. Barr, J. C. Bicket, D. S. Dantas, B. Du, T. W. D. Kim,B. Zhou, and E. G. Sirer." On the Need for System-Level Support for Ad Hoc and Sensor Networks". *Operating System Review*, 36(2): vol. **36**, no. 2, pp. 1–5, 2002.

[4] Chih-Chieh Han, Ram Kumar Rengaswamy, Roy Shea, Eddie Kohler and Mani Srivastava. "SOS: A dynamic operating system for sensor networks", Proceedings of the *Third International Conference on Mobile Systems, Applications*, And Services (Mobisys), pp 1-2 . 32 oct 2005.

[5] The Internet Engineering Task Force (IETF) ,Simple Network Management Protocol RFC , www.ietf.org/rfc/rfc1157.txt

[6] Adam Dunkels, "IP for Smart Objects", *Whitepaper no 1 Cisco Systems*, Sep 2008.

[7] W. Chen, N. Jain, and S. Singh. "ANMP: Ad hoc network network management protocol", *IEEE Journal Sel. Areas Comm,* vol. 17, policy, pp.23-34.

[8] B. Deb and B.Nath. "Wireless sensor networks management" http://www.research.rutgers.edu/_bdeb/sensor networks.html, 2005.

[9] Holger Karl and AndreasWillig. "Protocols and Architectures for Wireless Sensor Networks". John Wiley & Sons, Ltd, 2005.

[10] James F. Kurose and Keith Ross. "Computer Networking: A Top-Down Approach Featuring the Internet". *Addison-Wesley Longman Publishing Co., Inc.*, Boston, MA, USA, 2002.

[11] Linnyer B. Ruiz, Jose M. Nogueira, and Antonio A. F. Loureiro. "Manna:A management architecture for wireless sensor networks". *IEEE Communications Magazine*, 41(2):116–125, February 2003.

[12] Chien-Chung Shen, Chavalit Srisathapornphat, and Chaiporn Jaikaeo. "An adaptive management architecture for ad hoc networks". *IEEE Communications Magazine*, 41(2):108–115, February 2003.

[13] Gilman Tolle and David Culler. "Design of an application-cooperative management system for wireless sensor networks". *2nd European Workshop on Wireless Sensor Networks,pp 121 – 132,* January 2005.

[14] Fenghua Yuan, Wen-Zhan Song, Nina Peterson, Yang Peng, Lei Wang, Behrooz Shirazi, Richard LaHuse, "A Lightweight Sensor Network Management System Design", *Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, p.288-293, March 17-21, 2008.