Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Current Methodology of Sensor Virtualization in Smart Home

Monali Sonule
Research Scholar
Dept of Computer Engineering
D.Y. Patil Inst. Of Engg& Tech
Pune University (India)

Mrs. Swati Nikam
Assistant Professor
Dept of Information Technology
D.Y.Patil Inst. Of Engg& Tech
Pune University (India)

Abstract - Smart home is the concept used for Home automation. Today one of the technologies used to implement Smart home is Wireless Sensor Network (WSN). Wireless sensor networks are gaining importance for their broad range of commercial applications such as home automation, health care and industrial automation. In WSN heterogeneous sensor nodes are deployed to serve this purpose. But Due to strict administrative control over the WSN domains, communication barrier, conflicting goal & economic interest different vendors of sensor node in WSN make it difficult to introduce a large scale federated WSN. By enabling heterogeneous wireless sensor Networks to coexist on a shared physical substrate, virtualization in sensor network may provide increased manageability, flexibility and security. In this survey paper we discuss current Smart Home Technologies involved and how sensor virtualization provides cost effective implementation of Smart home.

Keywords - Sensor Virtualization, wireless sensor network , sensor node, smart home, ZigBee

I. INTRODUCTION

A sensor network is formed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. This allows random deployment in inaccessible disaster relief operations. Sensor nodes have inbuilt processors. Instead of sending the raw data to the nodes responsible for the fusion, they use their own processing power to carry out simple computations locally and transmit only the required and partially processed data [1][7].There are many application in which sensor network are used in day to day life and some of the areas are health, military, and home and battle field surveillance etc.

1. In military, rapid deployment, self organization, and fault tolerance characteristics of sensor networks make them promising candidate for military command, control, communications, computing intelligence and surveillance.
2. In health, sensor nodes can be deployed to monitor patients and assist disabled. Other important commercial applications are inventory management, product quality monitoring, and disaster management.

Difference between sensor networks and adhoc networks are:

- The number of sensor nodes in sensor network can be several times more than the nodes in an ad hoc network.
- Sensor nodes are closely deployed.
- Sensor nodes are vulnerable to failures.
- The topology of a sensor network means the arrangement of the sensor network changes very frequently as per the demand.
- Sensor nodes uses broadcast communication paradigm, while adhoc networks are relied on point to point communications.
- Sensor nodes has limited power, computational capacities, and memory.

A. Sensor network communication architecture

The sensor nodes are usually scattered in a sensor field as shown in Fig. 1. Each of these sensor node has the capabilities to capture the data and route data back to the sink by using multihop architecture as shown in the Figure1.

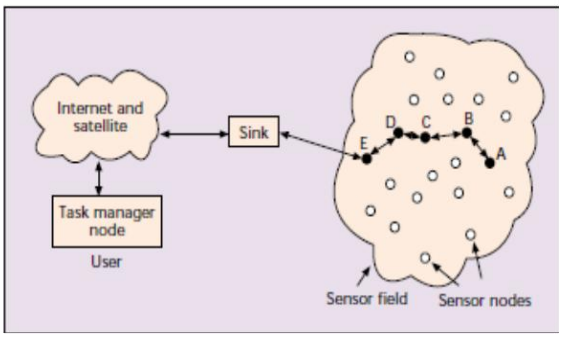

Figure 1.Sensor node scattered in a sensor field[1]

The sink may communicate with the task manager node via Internet or satellite. The design of the sensor network as shown in the above Figure, which is influence by factors like fault tolerance, scalability, production cost, operating environment, sensor network topology, hardware constraints, transmission media, and power consumption[1].

B. Design Factors

For the design of sensor networks and sensor nodes factors are important which they serve as a guideline to design a protocol or an algorithm for sensor networks, these influencing factors can be used to compare different schemes.

1. Fault Tolerance - Some sensor nodes may get failure or to be be blocked due to the lack of power, or have physical damage or environmental interference. The failure of any sensor node should not affect the overall task of the sensor network. This highlights the reliability or fault tolerance issue. Fault tolerance enables sensor network function properly without any interruption in the event of sensor node failures.
2. Scalability - The number of sensor nodes deployed in the order of hundreds or thousands and is governed by the requirement of the application. This number might go in millions and suggested schemes must be able to work with this number of nodes.
3. Production Cost - Sensor networks consist of a large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the network. If the cost of the whole sensor network is more expensive than deploying traditional sensors, the sensor network is not cost justified. This demands cost of each sensor node to be kept low. The cost of a sensor node should be much less than US $1 for the sensor network to be feasible.
4. Hardware Constraints - A sensor node is made up of four basic components, as shown in the Fig.2 which describe as a sensing unit, a processing unit, a transceiver unit, and a power unit.

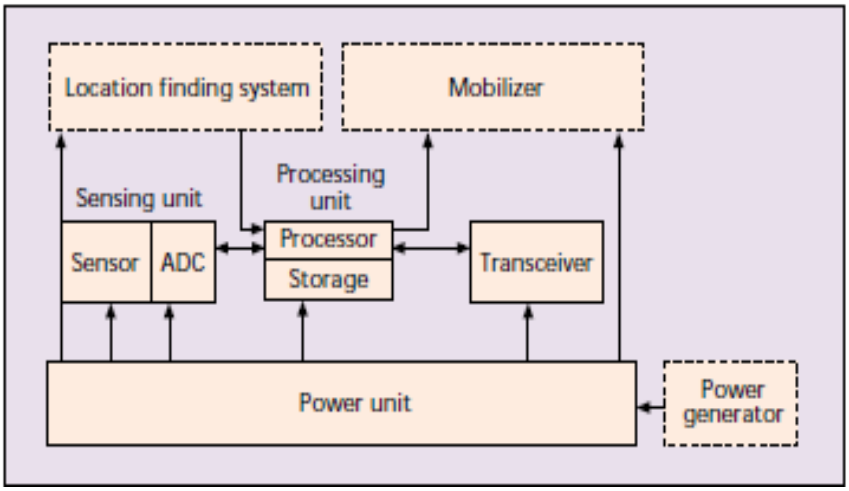

Figure 2.The Component of Sensor node[1]

They may also have an additional application - dependent components such as a location finding system, power generator, and mobilizer. Sensing units are generally composed of two subunits: sensors and analog to digital converters (ADCs). The processing unit, which is generally associated with a small storage unit, manages the procedures help sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the key components of a sensor node is the power unit. Solar cell can be used to support these power units for cost efficient infrastructure. A sensor node has allocation finding system to provide their accurate location to the applications. A mobilizer may sometime be needed to move sensor nodes when it is required to carry out the assigned tasks.

5. Transmission Media- In a multihop sensor network, communicating nodes are connected by a wireless medium such as radio, infrared, or optical media. To accessing the global operation of these sensor networks, the chosen transmission medium must be available over an internet. Another possible mode of inter nodes communication in sensor networks. Infrared communication is license free and full bodied to interference from electrical devices. Infrared transceivers are cheaper and easier to build. Smart Dust mote is another promising development. It is an autonomous sensing, computing, and communication system that uses the optical medium for transmission. Both infrared and optical require sender and receiver to be in line of sight.
6. Power Consumption - Here the wireless sensor node, being a microelectronic device, can only be equipped with a limited power source in 1.2V. In some application scenarios, replenishment battery might be impossible.

In a multihop adhoc sensor network, each node performs the dual role of data originator and data router. The malfunctioning of a few nodes can cause major topological changes and might require rerouting of packets and reorganization of the network. Hence, power conservation and power management holds high importance in sensor network.So it's a basic reason to focus on the design of power aware protocols and algorithms for sensor networks. The main job of a sensor node in a sensor field is to detect an events, performs quick local data processing, and then transmit the data. So the Main function of Power consumption unit is divided into three main domains as sensing, communication, and data processing.

C. Sensor Network Topology

In Sensor Network, several hundreds to thousands of nodes are deployed throughout the sensor network field within tens of feet of each other. The node densities may be in the range of 20 nodes /m3 but sometimes its higher than the defined. Deploying large number of sensor nodes densely requires the careful handling of topology maintenance. Some Issues related to topology maintenance and changes are in three phases:

• Pre deployment and deployment phase : Sensor nodes can be deploy in as a bundle or it can be placed one by one in the sensor field. They can be deployed by dropping from an airplane, delivered in an artillery shell, rocket, or missile, and placed one by one by either a human or a robot.

• Post deployment phase : After the deployment, topology of the sensor changes a due to the change in sensor nodes position, reach ability due to jamming, noise, moving obstacles, etc. and sensor reach ability depends on the available energy, malfunctioning, and task details.

• Redeployment of additional nodes phase : Additional sensor nodes are redeployed to topology to replace malfunctioning sensor node due to changes in task dynamics.

Environment - Sensor nodes are densely deployed very close or directly inside of the application to be observed. They may be working in the interior of large machinery, at the bottom of an ocean, in a biologically or chemically contaminated field, in battlefield beyond the enemy lines, and in home or large building more difficult. Communication in sensor networks is more crucial factor than in other computing domains. By Sending a single bit of data which can consume the energy of executing a thousands of the instructions. This has lead to investigation of passive networking systems.

II. SENSOR VIRTUALIZATION

It's a new advance technology which allows us to sharing a deployed WSN infrastructure by multiple applications including application which is designed after WSN deployment. Virtualization is a technique that present physical resources logically and enable their sharing and efficient usage. Virtualization in wireless sensor network can be defined as the clean separation of the function for the traditional WSN service provider into infrastructure provider and sensor virtualization network service provider.

A. Need of sensor virtualization

Sensor network virtualization is one of the best ways to utilize the physical sensor node. Most of the sensor node remains idle for the maximum period of lifetime, so here VSN is the virtualized sensor network is one of the best way to utilize the physical sensor node resource efficiently .VSN can provide a platform upon which novel sensor network architecture can be built and evaluated. VSN environment can be ensured from the existing heterogeneous WSNs architectures that are free from the limitations of existing multivendor sensor networks [8][10].The importance of sensor virtualization is diverse in this age of worldwide economic recession. New approach of VSN can provide the cost effective and the green technology solutions to build smart homes and cities. In a smart home, all patterns of state of the art technologies are used to deploy these technology. It requires a lot of sensor nodes in which individual sensor network performs individual task such as monitoring temperature, humidity, light, video/image, and movement. This is traditional approach of using WSNs incurs a huge cost involvement which is the main obstacle for an affordable business model of smart home. VSN may prove the most appropriate technology,in this regard where single federated WSNs can provide multiple Services for the smart home. By sharing a same physical substrate virtualization may provide flexibility, promote diversity, ensure security, cost effective solution,and increase manageability Instead of using individual application in wireless sensor network, here we are using VSN which can provide physical resources. By means of it we can reduce the cost of the application's is the collaborative form of WSN. So it's cost effective. It's formed by the logical connectivity in virtual sensor network based on the Phenomenon they track,the virtual sensor network protocol provide the functionality of sensor network formation, usage, adaptation and maintenance of subset of sensor collaborating on a specific task.

B. Benefits of smart home

Smart homes have the ability to make life easier, more convenient and provide peace of mind in the economic world of recession. Whether you are at work or on a vacation, the smart home will alert you to what's going on, and security systems can be built to provide an immense amount of help in an emergency. For example, not only would a resident be woken with notification of a fire alarm, but smart home system would also unlock doors, light the path to safety and dial the fire department [4].

Smart homes also provide energy efficiency to some extent. Because of the systems like Z-Wave and ZigBee set some devices at a reduced level of functionality, they can go to "sleep" and wake up when commands are given. Electric bills go down when lights are automatically turned off when a person leaves the room, and rooms can be heated or cooled based on who's there at any given moment. One smart home owner boasted his heating bill was about one third less than a same sized normal home. Smart devices can monitor energy use each appliance and command it to use less. Smart home technology promises considerable benefits for an elderly person living alone by notifying him when it was time to take medicine, alert the hospital in case of emergency and track eating habit. If the elderly person was a little forgetful, the smart home would perform tasks such as shutting off the water before a tub overflowed or turning off the oven if the cook had wandered away. It also allows adult children living away from their parents to participate in the care of their aging parent.

C. Limitation

As part of virtualization one may expect cost effective solution for their smart home but still maintenance cost remains the concern as one would be required to be over dependant vendor for technological assistance. Finding right vendor with the Virtualization expertise can limit adoption of virtualization in smart home.

III. SMART HOME TECHNOLOGY

In the smart home all the electronic appliances and devices are receivers, whereas every device is used for to controlling the system, such as remote controls or keypads, are transmitters. In some cases, if you want to turn off a lamp in another room, then that time the device transmitter will issue a message in numerical code that includes the following:

- It gives to pointed to the system where you issuing the command.
- An identification code for the device that should receive the command.
- A code that contains the actual command, such as "turn off."

All of this is designed to happen in less than a second, but X10 does have some limitations. Communicating through electrical lines is not always reliable as the lines get noisy from powering other devices. An X10 device might interpret electronic interference as a issued command and react in undesired way. While X10 devices are still around, new technologies have emerged providing more reliable and cost effective smart home solutions. Instead of power lines ,some systems use radio waves as communication channel which is also how Wi-Fi and cell phone signals operate. However, home automation networks don't need all the juice of a Wi-Fi network because automation commands are short messages. The two most important radio networks in home automation are ZigBee and Z-Wave. Both of these technologies are mesh networks, meaning there is more than one way for the message to get to its destination.

A. Z-Wave

Z-Wave is one of the technology used in smart home where we used a Source Routing Algorithm to finding the fastest route for messages. Each Z- Wave device is embedded with a code, and when the device is plugged into the system, the network controller recognizes the code, find out its location and adds it to the network. When a command receives from the controller where we have already uses the algorithm which can find out how the message should be sent. Due to this routing algorithm can take a lot of memory on a network, Z-Wave has developed a hierarchy between devices: Some controllers initiate messages, and some are behaves like a slaves ie means they can only carry and respond to the messages.

B. ZigBee

ZigBee is the mesh networking concept which pass messages from the transmitter zigzag like bees, looking for the best path to the receiver. While Z- Wave uses a proprietary technology for operating its system, ZigBee's platform is based on the standard set by the Institute for Electrical and Electronics Engineers (IEEE) for wireless personal networks. This means any company can develop a ZigBee compatible product without paying licensing fees for the technology behind it, which may eventually give ZigBee an advantage in the marketplace [4].

C. Insteon

Wireless network provides more flexibility for positioning devices, but like electrical lines, they might have interference as well. Insteon addresses this challenge and offers a way for your home network to use both communication channels electrical wires and radio waves. This creates a dual mesh network. If the message isn't getting through on one platform, it will try the other. Instead of routing the message, an Insteon device will broadcast the message, and all devices pick up the message and broadcast it until the command is performed. The devices act like peers, as opposed to one serving as an instigator and another as a receptor. This means that the more Insteon devices that are installed on a network, the stronger the message will be[4].

D. Bluetooth

Bluetooth invented by the Bluetooth Special Industrial Group (SIG), provides a comparably low cost solution wireless communication among portable or handheld devices at a maximum data rate of 1Mbps within up to 10 meters. It operates in the 2.4GHz ISM band with as low as 0dBm transmission power, spectrum techniques to overcome interference and multi path fading in the wireless channel. Bluetooth adopts Forward Error Correction and Automatic Repeat request to improve reliability by reducing errors in data transmission. The issues including authentication encryption are addressed at the physical layer in Bluetooth. Bluetooth devices cannot depend on the Public Key Infrastructure (PKI) approach to deal with authentication due to the essence of adhoc networking. Hence, Bluetooth provides a challenge response mechanism with a commonly shared secret and a link key produced by a user provided Personal Identification Number (PIN) in such a way to enable a user to establish a trust domain among personal Bluetooth devices for authentication. Moreover, the link key is intended for generating a sequence of Encryption keys for later data transmission after the device authentication.

IV. PLATFORM

1. SenShare

In the design of SenShare require two user roles- (i) The infrastructure owner, and (ii) The application developers. The infrastructure owner is considered to have full control over the physical infrastructure. The application developers are assumed to have an understanding of the geography of the target environment and the sensing modalities offered by the network.

The main challenge in shared sensing is to allow newly developed applications to be deployed over the infrastructure without disrupting the operation of previously installed applications. Considering the case of a smart building one of the main reasons for the deployment of sensing technologies is to monitor the environmental conditions in the building and adjust the HVAC (Heating Ventilation Air Cooling) system accordingly. The dynamic deployment of a newly developed application that uses humidity sensors to estimate room occupancy should operate without disrupting the pre existing environmental monitoring sensing application. In design terms, addressing the challenge requires the support of multiple applications to operate on the same network (even coexisting on the same node), by offering protection isolation of sensing applications both in terms of the runtime environment inside the sensor node and the network traffic over the sensing infrastructure[6].

2. TinyOS

It's an operating system designed specifically for use in sensor networks combined with a family of wireless sensor devices, several challenges and the limitations of TinyOS produces a set of requirements for a flexible and concise sensor network programming model TinyOS is an open source, flexible, component based, and application- specific operating system designed for sensor networks .It can support concurrent programs with very low memory requirements. The TinyOS component library includes network protocols, distributed services, sensor drivers, and data acquisition tools [2].

1.Resource Sharing

TinyOS uses two mechanisms for managing shared resources: Virtualization and Completion Events. A virtualized resource appears as an separate instance and is used by the application as independent resource. Resources that cannot be virtualized are handled by the completion events. The GenericComm communication stack of Tiny OS is shared among different threads and it cannot be virtualized. GenericComm can only send one packet at a time, send operations of other threads fail during this time. Such shared resources are handled through completion events that inform waiting threads about the completion of a particular task[2].

3. Mate Virtual machine

It's a byte code interpreter that runs on tiny OS. It is a single tiny OS component that sits on the top of several system component including sensor , the network stack and nonvolatile storage. Code is broken down into capsule of 24 instruction each of which is a single byte long. The larger program composed of multiple capsules. Mate has two stack an operand stack and return address stack. Most of the instruction operate solely on the operand stack but the few instruction control program flow and several have embedded operand. These are three execution context that can run concurrently at instruction granularity[3]. For the designing of Mate to run on both mica and the rene2 hardware platform this means that mate and all of its subcomponents must fits in 1 KB of RAM and 16KB of the instruction memory.

V. CONCLUSION

In this paper we have presented a survey of sensor virtualization current methodologies in wireless sensor network Virtualization in sensor network can be effective in smart home application. The realization of sensor network needs to satisfy the constraint introduced by factors such as fault tolerance, scalability, topology change ,cost, environment and power consumption. These constraint are highly stringent and specific for sensor network. Our future interest is to run multiple application on one single Sensor node utilizing the power of virtualization.

REFERENCES

[1] IanF.Akyildiz,Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci Georgia Institute of Technology "A survey on Virtualization on sensor network", 2012.
[2] Muhammad Omer Farooq and Thomas Kunz."Operating Systems for Wireless Sensor Networks:A survey",2011.
[3] Philip Levis, David Culler, "Mate: a tiny virtual machine for sensor networks", In Proceedings of the 10th international conference on Architectural support for programming languages and operating systems, San Jose, California, October 05-09, 2002.
4] Rosslin John Robles1 and Tai-hoon Kim, "Applications, Systems and Methods in Smart Home Technology: A Review" ,2010.
[5] Rosslin John Robles1 and Tai-hoon Kim1"A Review on Security in Smart Home Development",2010.
[6] Ilias Leontiadis, Christos Efstratiou, Cecilia Mascolo, Jon Crowcroft University of Cambridge,"SenShare: Transforming Sensor Networks Into Multi-Application Sensing Infrastructures",2012.
[7] Md.Motaharul Islam,Mohammad Mehedi Hassan,Ga-Won Lee and Eui-Nam Huh,"A Survey on Virtualization of Wireless Sensor Networks",2012.
[8] Imran Khan, "Design and Analysis of Virtualization Framework for Wireless Sensor Networks", 2013.
[9] Imran Khan, FatnaBelqasmi,"AMulti-Layer Architecture for Wireless Sensor Network Virtualization",2013.
[10] Md. Motaharul Islam, Jun Hyuk Lee, and Eui- Nam Huh1,"An Efficient Model for Smart Home by the Virtualization of Wireless Sensor Network",2013.

