Asian Journal of Multidisciplinary Research (AJMR) 2016

E-ISSN: 2395-1710 P-ISSN: 2395-1729
Volume 02- Issue 12-, pp-32-37

Research Paper Open Access

MIDDLEWARE CHALLENGES AND APPROACHES FOR WIRELESS SENSOR NETWORKS- A SURVEY

S.BOOVANESWARI[1], Dr.N.DANAPAQUAME[2], R.RAJADURAI[3]

M. Tech Student, 1Assoc.Prof[2], Asst.Prof
Dept of Computer Science and Engineering
Sri Manakula Vinayagar Engineering College
Boovanacse28@gmail.com [1], n.danapaquiame@gmail.com[2], king8153@gmail.com[3]

Abstract

A wireless sensor network is a group of specialize transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. WSN has been used in many of life changing applications such as area monitoring, healthcare monitoring, asset monitoring, infrastructure, security etc. The design issues of such applications must have some challenges around WSN characteristics on one side and applications on the other. This paper is about the study of work state research in middleware design architecture and reveals the full survey on issues in middleware and database design .It also deliver the various approaches in middleware and the challenges to be addressed while developing the solutions for WSN

Keywords: WSN, middleware, pollutant etc.

I INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. WSN has made an strongly developed applications through advance technology in distributed computing, Networking, Wireless communications, Sensor technology and Embedded system. these wide area has given spectacular opportunities to the WSN for developing wide array of applications like production lines controls, shipping, pollution monitoring, disaster prevention, infrastructure security, habitat monitoring, remote health monitoring, and traffic control, which are essential for the progress of different fields such as medicine, environment protection, manufacturing, engineering, and business.

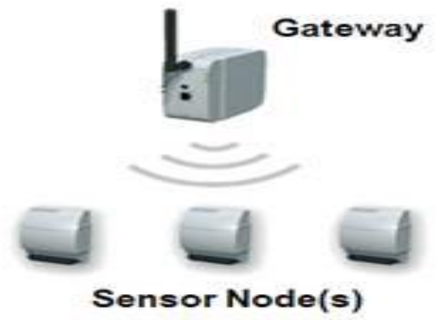


Figure1 WSN components, Gateway and Distributing nodes

One of the novel emerging approaches used to address these challenges is the design of middleware for WSN. Middleware refers to distributed software that can bridge the gap and remove impediments between the heterogeneous hardware platform and the backend applications requirements. In recent years, research has been carried out on WSN middleware from different aspects and for different purposes. These devices communicate through a variety of wireless/wired networking technologies. In addition, these devices are usually controlled by several software components developed by different vendors and implemented using different programming languages and models. Due to the high distribution, dynamic properties, and heterogeneity of the de-vices, communication technologies and software components used; implementing such applications is non-trivial. There are usually integration, scalability, reliability, security, usability, QoS, and operational issues to be considered. Incorporating a middleware layer is a novel approach to attempt to meet the design and implementation issues of WSN applications. There are different middleware approaches for WSN [1].Efficient software installation and data aggregation are the important functions of various WSN applications but there is in need of more advanced functions needed for middleware to reduces the design complexity

II WSN DESIGN PRINCIPLES

The design principle has already been proposed to provide flexible characteristics of WSN .These principles are in use for designing the middleware.

i. Localized algorithms are distributed algorithms that achieve a global goal by communicating with nodes in some neighborhood only. Such algorithms scale well with increasing network size and are robust to network partitions and node failures.

ii. Adaptive fidelity algorithms allow trading the quality of the result against resource usage and are thus a key element for resource efficiency. As an extreme case, the application can choose from a whole range of different algorithms which solve the same problem with different quality and resource requirements.

iii. Data-centric communication introduces a new style of node addressing by focusing on the data produced by nodes, since applications are unlikely to request the current sensor reading such as temperature at a specific node, but instead ask for locations where temperature exceeds a certain value Hence, at this early stage of WSN technology it is not clear on which basis future middleware for WSN can typically be built.

Scope and Functionality

The main purpose of middleware for sensor networks is to support the development, maintenance, deployment, and execution of sensing-based applications. This includes mechanisms for formulating complex high-level sensing tasks, communicating this task to the WSN, coordination of sensor nodes to split the task and distribute it to the individual sensor nodes, data fusion for merging the sensor readings of the individual sensor nodes into a high-level result, and reporting the result back to the task issuer. Moreover, appropriate abstractions and mechanisms for dealing with the heterogeneity of sensor nodes should be provided.[10]All mechanisms provided by a middleware system should respect the design principles sketched above and the special characteristics of WSN, which mostly boils down to energy efficiency, robustness, and scalability. The design and development of a successful middleware layer for WSN is not trivial. It needs to deal with many challenges dictated by the WSN characteristics on one hand and the applications demands on the other [4]. Following is a discussion of these challenges.

III MIDDLEWARE CHALLANGES FOR WSN

Middleware sits between the operating system and the application. On traditional desktop computers and portable computing devices, operating systems are well established, both in terms of functionality and systems. For sensor nodes, however, the identification and implementation of appropriate operating system primitives is still a research issue [2]. In many current projects, applications are executing on the bare hardware without a separate operating system component.

A.HARDWARE RESOURCES

One major challenge in a WSN is to produce *low cost* and *tiny* sensor nodes. There are an increasing number of small companies producing WSN hardware and the commercial situation can be compared to home computing in the 1970s. Many of the nodes are still in the research and development stage, particularly their software. Also inherent to sensor network adoption is the use of very low power methods for radio communication and data acquisition. A middleware should provide mechanisms for an efficient use of the processor and memory while enabling lower power communication

B. CHANGES IN NETWORK TOPOLOGIES AND SIZE

The topology of the network is subject to frequent changes due to different factors such as device failure, device mobility, moving obstacles, and interferences. Furthermore, the middleware should be able to adjust network devices properties such as transmission ranges and sleep periods to adjust to any changes in the topology.

a) Bus topology
b) Star topology
c) Ring topology
d) Circular topology
e) Tree topology
f) Mesh topology
g) Grid topolog

C. SCALABILITY

Scalability is the property of being able to cope up with network cells as small as a few nodes to cells of thousands or even tens of thousands of nodes as well as increasing the size of existing network by order of magnitude without employing expensive cellular communication or other long range solutions.

D. HETEROGENEITY

Heterogeneous wireless sensor network (heterogeneous WSN) consists of sensor nodes with different ability, such as different computing power a sensing range. Compared with homogeneous WSN, deployment and topology control are more complex in heterogeneous WSN. It should establish system mechanisms interfacing with the various types of hardware and networks, only supported by basic distributed primitive operating system abstractions. As a result, this should make it easier to develop the applications using the network without worrying about the low-level details.

E.SECURITY

Security [18] is a term that is broadly encompassed by its characteristics such as authentication, integrity, privacy, non repudiation and anti-playback [5]. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. For the secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known. In this section, we discuss the network security fundamentals and how the techniques are meant for wireless sensor networks.

i. Data confidentiality: The security mechanism should ensure that no message in the network is understood by anyone except intended recipient. In a WSN, the issue of confidentiality should address the following requirements
(i) a sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so
(ii) key distribution mechanism should be extremely robust,
(iii) public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks.

ii. Data integrity: The mechanism should ensure that no message can be altered by an entity as it traverses from the sender to the recipient.

iii. Availability: This requirements ensures that the services of a WSN should be available always even in presence of an internal or external attacks such as a denial of service attack (DoS). Different approaches have been proposed by researchers to achieve this goal. While some mechanisms make use of additional communication among nodes, others propose use of a central access control system to ensure successful delivery of every message to its recipient.

iv. Data freshness: It implies that the data is recent and ensures that no adversary can replay old messages.

IV MIDDLEWARE APPROACHES IN WSN

Middleware has been proposed with five approaches each of which provide efficient implementation in sensor nodes. Existing middleware's are classified based on the physical approach and types of programming. Some of the different middleware approaches are given below Virtual Machine Middleware Approach This approach is flexible and contains virtual machines (VMs), interpreters, and mobile agents. It basically allows developers to write applications in separate small modules.

i. Modular Programming Approach In this approach, applications are divided as modular programs to facilitate injection and distribution through the network using mobile code

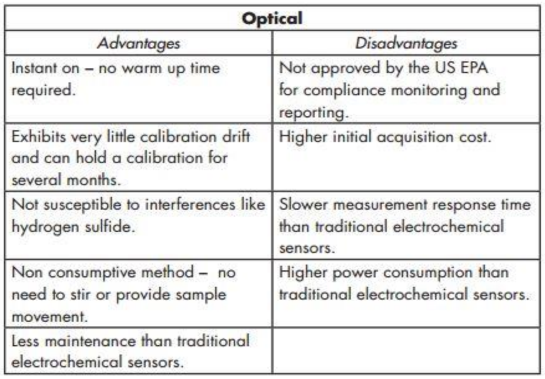
ii. Database Approach[20] This middleware approach treats the whole sensor network as a distributed database. It has an easy to use interface, using SQL like queries to collect target data [8]. It is good at regular queries, but it lacks the support for real time applications, so sometimes it only provides approximate results i.e. data rendering in real time is not applicable.

iii. Integration with other systems this approach allows us to fine tune the network and to take into account resource minimization and maximum data utilization i.e. this approach basically introduces a new dimension in middleware design by supplementing an architecture that reaches the network protocol stack.

iv. Message-oriented Approach Message-oriented middleware uses the Publish-Subscribe mechanism to facilitate message exchanging

TABLE *COMPARISON OF MIDDLEWARE APPROACHES FOR WSN*

Approaches	Scalability	Heterogeneity	Mobility
Virtual Machine Approach	Full	Partial	Full
Modular Programming	Full	Little	Full
Database Approach	Little	Little	Little
Application Driven Approach	Full	Little	Little
Message Oriented Approach	Full	Partial	Partial



Optical	
Advantages	*Disadvantages*
Instant on – no warm up time required.	Not approved by the US EPA for compliance monitoring and reporting.
Exhibits very little calibration drift and can hold a calibration for several months.	Higher initial acquisition cost.
Not susceptible to interferences like hydrogen sulfide.	Slower measurement response time than traditional electrochemical sensors.
Non consumptive method – no need to stir or provide sample movement.	Higher power consumption than traditional electrochemical sensors.
Less maintenance than traditional electrochemical sensors.	

V CONCLUSION

Wireless sensor networks, an emerging technology, is ex-pected to change our lives in the near future. In this survey, we went through the design principles, the different middleware approaches and some existing middlewares for WSN and then compared the different approaches by including suggestions about where each approach could be used. In this process we observed that, while scalability and power saving issues can be compensated, it comes at a trade-off with QoS. Therefore, from this survey we can safely conclude that although middleware has been able to compensate for most of its issues by trade-offs with QoS, there is a lot of research yet to be carried out before a perfect middleware for WSN can be built and tested.

REFERENCES

1. M. Hadim S, “Middleware challenges and approaches for wireless sensor networks,” IEEE Distributed Systems Online, vol. 7, pp. 1–23, 2006.
2. N. Mohamed and J. Al-Jaroodi, “A survey on service-oriented middle-ware for wireless sensor networks,” Service Oriented Computing and Applications, vol. 5, pp. 71–85, 2011.
3. J. L. Miaomia Wang, Jiannong Cao and S. K. Dasi, “Middleware for wireless sensor

networks: A survey," Journal of Computer Science and Technology, vol. 23, pp. 305–326, may 2008.

4. M. Hadim S, "Middleware for wireless sensor networks: Asurvey," 1–7, 2006.
5. A.-J. J and A.-D. A, "Security issues of service-oriented middleware," International Journal Computer Science Network Security, vol. 11, 153–160, 2011.
6. e. a. Yu, Y., "Issues in designing middleware for wireless sensor networks," IEEE Network Magazine, vol. 18, pp. 15–21, 2004.
7. On Decentralized In-Network Aggregation in Real-World Scenarios with Crowd Mobility
8. R. J and M. S, "Middleware approaches for wireless sensor networks:
9. An overview," International Journal of Computer Science Issues IJCSI,vol. 9, pp. 224–229, 2012.
10. L. P and C. D, "Mate: A tiny virtual machine for sensor networks,"2002.
11. L. T and M. M, "Impala: A middleware system for managing autonomic,parallel sensor systems," vol. 38, pp. 107–118, 2003.
12. S. J. C and S. C. C, "Sensor information networking architecture,"vol. 18, pp. 23–30, 2000.
13. C. H. Heinzelman W, Murphy A and P. M., "Middleware to support sensor network applications," IEEE Network, vol. 18, pp. 6–14, 2004.
14. H. K. Hitha Alex and B. Shirazi., "Midfusion: An adaptive middleware for information fusion in sensor network applications," vol. 9, pp. 332–343, 2008.L. Linnyer Beatrys Ruiz, Isabela G. Siqueira and B.E.Oliveira, "Fault management in event driven wsn," pp. 149–156, 2004.
15. L. R. L. P. Flavia C. Delicate, Paulo F. Piers and J. F. de Rezende,"Refelective middleware for wireless sensor networks," pp. 1155–1159,2005.
16. M. a. T. Mohesen Shariff and A. Taherkordi, "A middleware layer mechanism for quos support in wireless sensor networks," pp. 118–1124, 2006.
17. N. Y. Nan Hua and Y. Guo, "Research on service oriented and middleware based active qos infrastructure of wireless sensor network,"pp. 208–213, 2009.