IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13516

Wireless Sensor Network

Gampannagari Srinath

Department of Electronics and Communication Engineering, SJC Institute Of Technology, Chickballapur, Karnataka, India

Abstract: Wireless Sensor Networks (WSNs) are distributed and independent Sensors that are connected and worked together to measure quantities such as temperature. humidity, pressure. noise levels Or vibrations. JVS,'Vs measure vehicular movement (velocity. *location, etc.)* and monitor conditions such as lightning condition. soil makeup and morion. Nowadays. JVSNs are utilized in applications as vehicle applications, Some Of vehicle applications are: vehicle tracking and delecriom tire pressure monitoring. vehicle speed detection. vehicle direction indicator. traffic control. reversing aid sensors Such applications can be divided in major categories such as safety. security. environment logistics. TO implement in an application and have an efficient system. 've need 'o consider about WSN rechnologv. and its components. This paper is aimed ar providing reliable software architecture of WSW Ihar could be implementedfor performance and working.

Keywords: Wireless sensor network, Architecture, power unit, WSN design challenges.

I. INTRODUCTION

To provide comprehensive view Of WSN hardware, understanding of WSN components' structure is required. Wireless sensors are small microcontrollers equipped with wirelesscommunication device and an energy supplier. The architecture Of WSNs is illustrated in FigurcsAs Figure-I shows the components of WSNs are sensing unit. processing unit, power supplier and communication device. The sensing unit consists of sensors and Analog to Digital Converters (ADCs). ADCs are responsible for gathering the signals and converting them into digital signals data and transfer them through each other using network topology to the processor unit. In the sensing unit, each Sensor is called an •end and varies in Size and Cost. The mission of these multifunction Sensor nodes are to sense. process data and collaborate With Other nodes [81. Wireless sensor network can be positioned in two ways. either using a complex technique with the large sensors far from the Object or using several sensors with an engineered design on position and topology [51. In addition, each node provided with a wireless communication transceiver as a commumcatton component.In the process unit. the controller and small memory storage are responsible for managing the collaboration Within the Sensors to the assigning task. In addition, the communication device with a transceiver makes the network connection. Above all, the essential component of WSN is the power unit, which supports the power for all units [51.

One Of the unique characteristics Of sensor networks is that they are equipped With an on-board processor. This feature enables them to locally process some simple computations and broadcast only necessary processed data Network communication is complicated and needs years of study [81. but to be able to implement WSN, we need to know some basic primary concepts of communication technology such as; network topologies, network protocol and their standards and specifications.

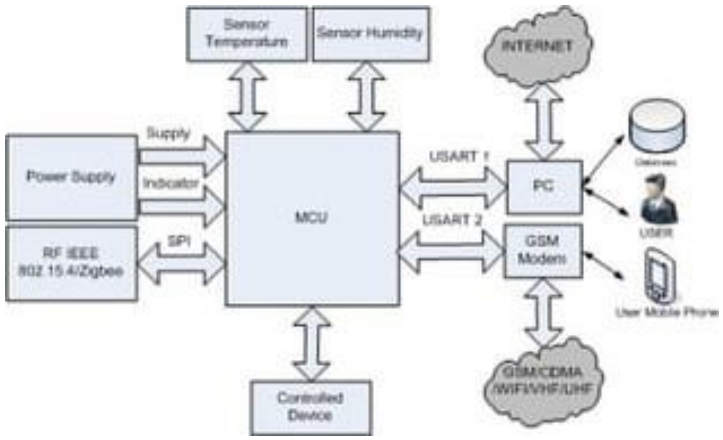

Figure-I WSN Architecture

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13516

II. TOPOLOGIES INWSN COMMUNICATION

In network communication, the big issue is how data transfers through nodes and nodes interconnect with each other. Several basic network topologies may be used for transmitting to and receiving from a node. The Alliance for Telecommunications Industry Solutions (AT IS) the standards organization of telecommunication industry - explained the network topology as "The physical, real, logical or virtual arrangement Of the nods'elements of a network" [9]. The topology shows the diameter and the number of nodes between any two nodes. Moreover how a data process and the data routing complexities are relied on the chosen topology. Consequently, some characteristics Of a sensor networks such as latency. robustness and capacity are changed by their topology [101.Despite having the Same topology, two networks can differ in transmission rates because Of their physical interaction, signal types and distance between nodes [9]. Table-1 describes the different types Of network topology.

	Name	Types	Description
Basic topo logy	point-to-point	Permanent	A permanent connection between two endpoints and
		Switched	A dynamic point-to-point circuit that can be dropped if needed.
	Bus topology	Linear topology	nodes are linked to a Common transmission medium (bus) which has exactly two endpoints and all data is able to transfer through all nodes.
		Distributed bus	All nodes of the network are linked like a branch to a main bus which causes more than two endpoints. Data goes in all directions to nodes connected on the bus cable until it finds unique addresse.g. the MAC address or IP address on the network and transmit the data.
	Ring topology		Each node is linked in a ring or loop to the closest node. The data travels in the ring only in one direction and each node Can transmit only one piece of data at a time. Ring topology used control access in the network and if one node fails entire network will fail.
	Star topology		Each node has exactly two branches linked to it. External nodes ate connected to a central node. The external nodes are only permitted to communicate With the Center node and a failure of an external node will cause it to be isolated from the others.
	topology		Each node is linked in different tree paths. In each branch, each node transfers the data to upper node. so, a node failure causes the whole connected branch to fail.
	Mesh topology	Partially connected	At least two nodes linked with two or more node in a network.
		Fully connected	Direct link between any two nodes. There will be links
Mix topology	Hybrid topology		An arrangement Of any two or more different basic network topologies.

Table 1-Topology TYPES

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13516

III. IEEE 1451 ANDSMART SENSORS

IEEE 1451 is a family Of standards that links sensors to users, similar to the way that IEEE 802 (Ethernet) provides connectivity for information systems. Currently, all working groups under the IEEE 1451 umbrella provide standard interfaces for sensors on tethered networks, But the demand for a wireless physical layer is growing. A Wireless IEEE 1451 standard should provide seamless connectivity among sensors and users. no matter what distance separates them. And it must do this Without rc%luiring the installation Of new Wires and With reasonable cost and size additions at each sensor node. Wireless sensor networks should satisfy many requirements. Desirable functions for sensor nodes include: ease of installation, self-identification, selfdiagnosis. reliability, time awareness for coordination With Other nodes, some software functions and DSP, and standard control protocols and network interfaces [IEEE 1451 Expo, 2001].

There are many sensor manufacturers and many networks on the market today. It is too costly for manufacturers to make special transducers for every network on the market. Different components made by different manufacturers should be compatible. Therefore, in 1993 the IEEE and the National Institute of Standards and Technology (NIST) began work on a standard for Smart Sensor Networks. IEEE 1451, the Standard for Smart Sensor Networks Was the result. The objective Of this standard is to make it easier for different manufacturers to develop smart sensors and to interface those devices to net•.vorks.

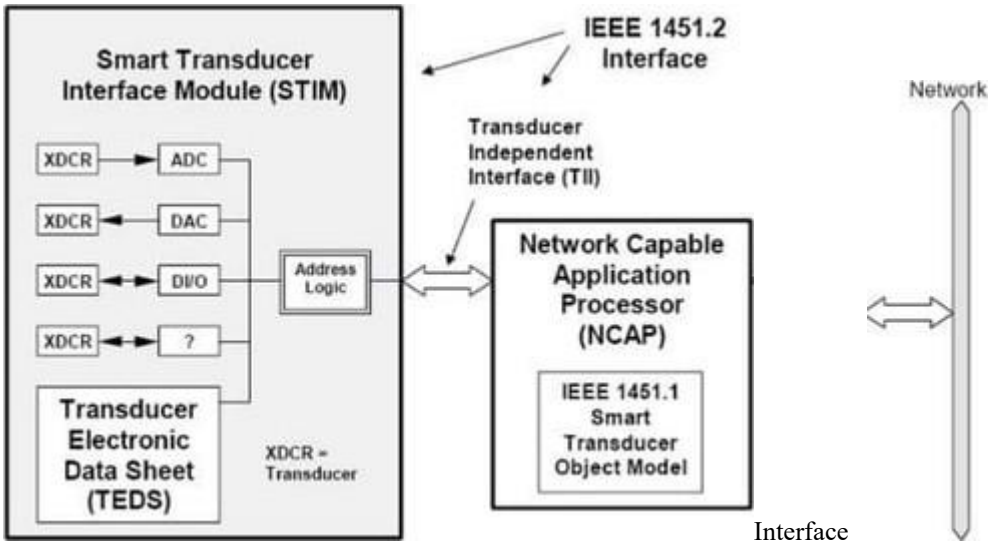

Figure-2 IEEE 1451 Standard for Smart Sensor Network

IV. SOFTWARE ARCHITECTURE COMPONENTS

Figure 3 shows an example Of a simple service architecture applicable to a sensor network. In this special ease, the client wants to acquire information about the surface conditions in the area of interest. First, the client requests the surrogate proxy via standardized protocols for the surface profile Of a part Of the observed area. The proxy communicates With the distributed nodes using a proprietary protocoL The nodes located in the target area try to determine the surface profile using cooperative algorithms and send it to the proxy. The proxy translates the information into standardized protocols and sends them back to the client.

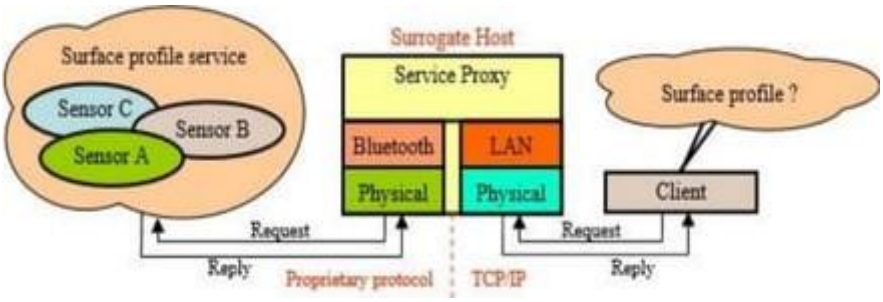

Figure-3: Example Of Surrogate Architecture in Sensor Networks

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13516

The different requirements and Objectives for Sensor networks Can be achieved only by using a flexible architecture Of the node software. Therefore. a node software is divided into three parts according to the main tasks (Figure 4)_ The Operating System handles the devicwspecific tasks. This contains bootup, initialization Of the hardware, scheduling, and memory management as well as the process management. The OS consists of special tailored parts only needed by the specific application of the node. The second part is the Sensor Driver. It initalizes the sensor hardware and performs the measurements in the sensor. It encapsulates sensor hardware and provides an optimized Application Programming Interface (API) to the middleware.

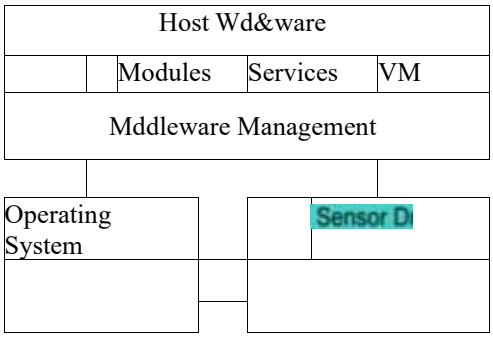

Figure 4: Structure of a Node Application

The Host Middleware is the superior software layer. Its main task is to organize the co- operation Of the distributed nodes in the network. The Middleware Management handles four optional components, which can be implemented and exchanged according to the node's task. Modules are additional components that increase the functionality Of the niddleware.Typical modules are routing modules or security modules. Algorithms describe the behavior of modules. For example, the behavior of a security module can vary if the encryption algorithm changes. The services component contains the required software to perform local and cooperative services. This component usually cooperates with other nodes to fulfill its task. Virtual Machines (VM) enable an execution ofplatform independent programs.

The software components in a node can be linked together statically or dynamically. Statical linking facilitates an optimization Of interfaces between several components within a node. This optimization is called software sealing. It performs in faster and smaller programs. The dynamic link process is used for components exchanged during runtime, e.g. algorithms downloaded from Other nodes. This procedure results in system-wide interfaces With significant overhead.

Figure 5 shows the logical view on a sensor network application. The nodes can be contacted only through services Of the middleware layers. They do not perform any individual tasks. The Distributed Middle.vare coordinates the cooperation of the services within the network. It is logically located in the network layer but it exists physically in the nodes. All layers together in conjuction With their configuration compose the sensor network application. The AdministrationTerminal is an external entity to configure the network and evaluate the results. It can be connected to the network at any location.

V. CHARACTERISTICS OF A MIDDLEWARE FOR SENSOR NETWORKS

The term middleware refers to the software layer between operating system and sensor application (As shown in Figure 4 and 5 above) on the one hand and the distributed application which interacts over the network on the other hand. The primary objective of the middleware layer is to hide the complexity of the network environment by isolating the application from protocol handling. memory management, network functionality and parallelism [14]. A middleware for sensor networks has to be:

• scalable • genenc • adaptive • reflective

The resource constraints (memory, processing speed, bandwidth) Of available node hardware requires the optimization of every node application. The optimization is performed at compile time. •Illereby, the application is reduced to all essential components and datatypes as well as interfaces are customized (scalable middleware).

The components of the middleware require a generic interface in order to minimize the customization effort for Other applications or nodes. The use Of identical middleware components in different applications leads to a higher number of

DOI: 10.17148/IJARCCE.2024.13516

complex interfaces. Reducing this overhead is the objective Of a generic middlcnvare. It is important to customize the interfaces to the application in contrast to customize the application to common interfaces. As example, a dlewarefunction SetBaudrate(int transmitter, long baudt•ate) identifies the network interface with the first parameter. However, a node that has only one interface, does not need this parameter. Consequently, the knowledge of this information at compile time can be used for optimization.

Another possibility is to change the semantics of data types. A potential use case is the definition Of accuracy Of addresses that results in a change Of data type's Width. The width Of a data type has vital influence on the network trame. Besides hardware-oriented optimization, an application specific data type optimization exists.

The mobility of nodes and changes in the infrastructure requires adaptations of the middleware at runtime depending on the network application. The middlcnvare must be able to dynamically exchange and run components (adaptive middleware).

Reflection covers the ability of a System to understand and influence itself. A reflective system is able to present its own behaviour. Thereby, two essential mechanisms are distinguished — the inspection and the adaptation Of the own behaviour Inspection covers ways to analyze the behavior, e.g., with debugging or logging. The adaptation allows modifying the internal layers to Change the behaviour presented to the application. In Contrast to an adaptive middleware, a reflective middleware does not exchange components but changes the behaviour of some components. An example of reflective behavior is the modification of the routing strategy depending on mobility. The interface between the software layers remains constant.

VI. SERVICES IN SENSOR NETWORKS

Besides the native network functions, such as routing and packet forwarding, future service architectures are required enabling location and utilization of services. A service is a program which can be accessed about standardized functions over a network. Services allow a cascading without previous knowledge ofeach other, and thus enables the solution of complex tasks.

A typical service used during the initialization Of a node is the localization Of a data sink for sensor data. Gateways or neighboring nodes can provide this service. To find this service, the node a service discovery protocol.

JIM is an emerging technology for desktop applications, but for sensor networks unsuitable due to resource requirements. Sun Microsystems suggests the surrogate host architecture for embedded systems [91. This is primarily suitable for systems that are controlled by an IP based network, The Client Can non-standardized services in a Sensor network by inquiring a proxy Server. The surrogate host translates the standardized protocol to the proprietary proteol and vice versa. It acts as the service provider to the IP based network. Service architectures for sensor networks are part Of the sensor application and operate in contrast to the 'Went-driven node application on the client-server principle.

VII. CONCLUSION

Based on the requirements of sensor networks, this article describes aspects of software engineering. The main objective is the simplification of development of service applications in sensor networks. A key issue is to separate the software from the underlying hardware. The presented serviceoriented software concept facilitates the programming On high abstraction layers. Our current research activities concentrate on the realization of the proposed architecture embedded in a framework. It simplifies the development of sensor-. node-. and sensor network applications. Besides that, it provides functionalities to configure and manage the whole network, whereby the scalability and portability of applications increases.

VIII. RESEARCH CHALLENGES

The Severe constraints and demanding deployment environments Of Wireless Sensor networks make computer security for these systems more challenging than for conventional networks. wever,several properties of sensor networks may help address the challenge of building secure networks. First. we have the opportunity to architect security solutions into these systems from the outset, since they are still in their early design and research stages. Second, many applications are likely to involve the deployment of sensor networks under a single administrative domain, simplifying the threat model. Third, it may be possible to exploit ndancy,scale. and the physical characteristics of the environment in the solutions.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13516

If we build sensor networks so they continue operating even if some fraction Of their sensors is compromised, we have an opportunity to use redundant sensors to resist further attack. Ultimately, the unique aspects of sensor networks may allow novel defenses not available in conventional networks. Many other problems also need further research. One is how to secure wireless communication links against eavesdropping, tampering, tramc analysis, and denial of service. Others involve resource constraints. Ongoing directions include asymmetric protocols where most of the computational burden falls on the base station and on public-key cryptosystems emcient on low- end devices. Finally, finding ways to tolerate the lack of physical security. perhaps through redundancy Or knowledge about the physical environment. will remain a continuing overall challenge. We are optimistic that much progress will bc made on all of them.

REFERENCES

[1]. Perrig, A., Sze•.vuyk, R., Wen, V., Culler, D, and Tygar, J. SPINS: Security protocols for Sensor networks. J. Wireless Nets. 8, 5 (Sept. 521—534.

[2]. Przydatek. B.. Song. and Perrig. A. SIA: Secure information aggregation in sensor networks. In Proceedirws of the 1st ACM International Conference on Embedded Networked sensor systems (Sensys 2003) (Los Angeles. Nov. 5-7). ACM Press, New York. 2003, 255-

[3]. Wood, A., Stankovic, L, and Son, S. JAM: A mapping service forjammed regioms in sensor networks. In Proceedings of the IEEE Real-Time Systems Symposium (Cancun, Mexico, Dee.3-5, 2003).

[4]. Wood, A. and Stankovie. J. Denial Of service in sensor networks. IEEE Comput. (Oct. 2002),

[5]. E. Altman, T. Basar, T. Jimenez, and N. Shimkin. "Competitive routing in net•.vorks with polynomial costs," IEEE Trans. Automat. Control . vol. 47. no. I, pp. 92-96.2002.

[6]. R. Bronson and G. Naadimuthu, Operations Research , 2 Schaum's Outlines, McGraw Hill, New York, 1997.

[7]. N. Bulusu, J. Heidemann, D. Estrin, and T. Tran, "Self- configuring localization systems: design and experimental evaluation," pp. 1-31, ACM TECS special Issue on Netuorked Embedded Computing, Aug. 2002.

[8]. J. Cao and F. Zhang, "Optimal configuration in hierarchical net•.vork routing," proc.Canadian Conf. Elect. and Comp. Eng., pp. 249-254, Canada 1999.

[9]. T.-S. Chen. C.-Y. Chang. and J.-P. Sheu, "Emeient path- based multicast in wormhole-routed mesh networks," J, Sys. Architecture, vol. 46, pp. 919-930, 2000.

[10]. J. Choi, C. Conrad, C. Malakowsky. J. Talent, C.S. Yuan, and R.W. Graey. "Flavones from Scutellaria baicalensis Georgi attenuate apoptosis and protein oxidation in neuronal cell lines," Biochemica et Biophysica 1571: 201-210 (2002).

[11]. C.W. de Silva. Control Sensors and Actuators. Prentice- Hall, New Jersey, 1989.

[12]. J. Duato, "A necessary and sufficient condition for deadlock-free routing in cut-through and store-and-forward networks," IEEE Trans Parallel and Distrib. Systems , vol. 7, no. 8, pp. 841854,Aug.1996.

[13]. R. Frank, Understanding Smart Sensors, 2nd Ed., Anech House, Norwood, MA, 2000.

[14]. M.R. Garey, and D.S. Johnson, Computers and Intractability. a Guide to the Theory ofNPcompleteness. Freeman, San Francisco, CA, 1979.

[15]. F. Giulietti. L Pollini, and M, Innocenti. "Autonomous Connation flight." IEEE Control Systems Mag.. pp. 34-44, Dec. 2000

[16]. Flu, Y.-C_, Perrig, A., and Johnson, D. packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In Proceedings Of IEEE Infoeom 2003 (San Francisco, Apr. 1—3, 2003).

[17]. Karlof, C. and Wagner, D. Secure routing in Wireless Sensor networks: Attacks and countermeasures. In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (Anchorage, AK, May I l, 2003).

