
Vibha Narwal\textsuperscript{1}, Anuradha\textsuperscript{2}

\textsuperscript{1,2}CSE Deptt., SSGI Bilaspur, Jagadhri

Abstract—Wireless Sensor Networks (WSNs) consist of thousands of tiny sensor nodes having the limited capability of sensing, computation, and wireless communication. WSNs send information to a central location called base station over wireless interface where data is analyzed and presented to useful applications. Energy efficiency is one of the most important design constraints in WSNs architecture. The lifetime of each sensor nodes depends on its energy dissipation. The core objective of proposed algorithm is to develop an energy-efficient network layer routing protocol to improve network lifetime. A routing technique in which the task of cluster formation is performed by base station itself on the basis of residual energy and the neighbor list of each individual node. The base station has information about the logical structure of the network i.e. the nodes location and their neighbors as well. In the case, when base station doesn’t receive data from particular node in the network then it will treat it as a malicious node.

Keywords—Wireless sensor networks, Survey, Energy efficiency, Power management, WSN

I. INTRODUCTION

A Sensor Node (SN) is a node in a WSN that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. The typical architecture \cite{1} of the sensor node is shown in Figure 1. The main components of a sensor node as seen from the figure are microcontroller, transceiver, external memory, power source and one or more sensors. Sensor nodes can be deployed in a WSN in two ways:

A. \textbf{Manual:} Location of each sensor node is planned with required level of precision e.g. fire alarm sensors in a building, habitat monitoring, sensors planted underground for precision agriculture.

B. \textbf{Random:} Locations of sensor nodes are random e.g. airdropped in a disaster hit area or war fields.

![Figure 1 : A typical architecture of the sensor node](image-url)
II. WIRELESS SENSOR NETWORK

Wireless sensor networks consist of many small compact devices, equipped with sensors that form a wireless network. Each sensor node in the network collects information from its surroundings, and sends it to a base station, either from sensor node to sensor node i.e. multi hop, or directly to a base station i.e. single hop. A wireless sensor network [3] may consist of hundreds or up to thousands of sensor nodes and can be spread out as a mass or placed out one by one. The sensor nodes collaborate with each other over a wireless media to establish a sensing network, i.e. a wireless sensor network. Because of the potentially large scale of the wireless sensor networks, each individual sensor node must be small and of low cost. The availability of low cost sensor nodes has resulted in the development of many other potential application areas, e.g. to monitor large or hostile fields, forests, houses, lakes, oceans, and processes in industries. The sensor network can provide access to information by collecting, processing, analyzing and distributing data from the environment. In many application areas the wireless sensor network must be able to operate for long periods of time, and the energy consumption of both individual sensor nodes and the sensor network as a whole is of primary importance. Thus energy consumption is an important issue for wireless sensor networks.

III. APPLICATIONS OF WSN

A. Environment and Habitat Monitoring: Environment and habitat monitoring [4] is a natural candidate for applying sensor networks, since the variables to be monitored, e.g., temperature, are usually distributed over a large region. Environmental sensors are used to study vegetation response to climatic trends and diseases, and acoustic and imaging sensors can identify, track, and measure the population of birds and other species. These networks generally require very low data rates and extremely long lifetimes. In typical usage scenario, the nodes will be evenly distributed over an outdoor environment. This distance between adjacent nodes will be minimal yet the distance across the entire network will be significant. After deployment, the nodes must first discover the topology of the network and estimate optimal routing strategies.

B. Security Monitoring: Our second class of sensor network application [4] is security monitoring. Security monitoring networks are composed of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors but it only has to transmit a data report when there is a security violation. The immediate and reliable communication of alarm messages is the primary system requirement.

C. Infrastructure Security: Sensor networks can be used for infrastructure security and counterterrorism applications. Critical buildings and facilities such as power plants and communication centers have to be protected from potential terrorists. Networks of video, acoustic, and other sensors can be deployed around these facilities. These sensors provide early detection of possible threats. Improved coverage and detection and a reduced false alarm rate can be achieved by fusing the data from multiple sensors. Even though fixed sensors connected by a fixed communication network protect most facilities, wireless ad hoc networks can provide more flexibility and additional coverage when needed. Sensor networks can also be used to detect biological, chemical, and nuclear attacks.

D. Military Applications: Because most of the elemental knowledge [2] of sensor networks is basic on the defense application at the beginning, especially two important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) form the Defense Advanced Research Project Agency (DARPA), sensor networks are applied very successfully in the military sensing. Now, wireless sensor networks can be an integral part of
military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. In the battlefield context, rapid deployment, self-organization, fault tolerance security of the network should be required. The sensor devices or nodes should provide following services:

- Monitoring friendly forces, equipment and ammunition
- Battlefield surveillance
- Reconnaissance of opposing forces
- Targeting
- Battle damage assessment
- Nuclear, biological and chemical attack detection reconnaissance

IV. TRAFFIC PATTERNS IN WSN

A. Local Communication. It is used to broadcast the status of a node to its neighbors. Also it is used to transmit the data between the two nodes directly.

B. Point-to-Point Routing: It is used to send a data packet from an arbitrary node to another arbitrary node. It is commonly used in a wireless LAN environment.

C. Convergence: The data packets of multiple nodes are routed to a single base node. It is commonly used for data collection in WSN.

D. Aggregation: The data packets can be processed in the relaying nodes and the aggregate value is routed to the base node rather than the raw data.

E. Divergence: It is used to send a command from the base node to other sensor nodes. It is interesting to investigate the traffic patterns in WSN along with the mobility of the nodes, as node mobility has been utilized in a few WSN applications such as healthcare monitoring.

V. ROUTING ARCHITECTURE

In WSN a large number of low-power nodes have to be networked together, and conventional techniques such as direct transmissions from any specified node to a distant base station have to be avoided. In the direct transmission protocol [6], the base station serves as the destination node to all the other nodes in the network where the end user can access the sensed data. When a sensor node transmits data directly to the base station, the energy loss incurred can be quite extensive depending on the location of the sensor nodes relative to the base station. In such a scenario, the nodes that are farther away from the base station will have their power sources drained much faster than those nodes that are closer to the base station. On the other hand, utilizing a conventional multi hop routing scheme such as the Minimum Transmission Energy (MTE) routing protocol will also result in an equally undesirable effect. In MTE, the nodes closest to the base station will rapidly drain their energy resources since these nodes engage in the routing of a large number of data messages to the base station. The routing protocols developed for WSN can be classified in several categories. Flat routing architecture, hierarchical routing architecture, and location based architecture are one of those.
A. **Flat routing architecture:** The first category of routing protocols is the multihop flat routing protocols [7]. In flat routing, each node typically plays the same role and sensor nodes collaborate to perform the sensing task. Due to the large number of such nodes, it is not feasible to assign a global identifier to each node. This consideration has led to data-centric routing, where the BS sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data.

B. **Hierarchical routing architecture:** Hierarchical or cluster-based routing methods [7], originally proposed in wire line networks, are well-known techniques with special advantages related to scalability and efficient communication. As such, the concept of hierarchical routing is also utilized to perform energy efficient routing in WSN.

C. **Location based routing architecture:** In this kind of routing [8], sensor nodes are addressed by means of their locations. The distance between neighboring nodes can be estimated on the basis of incoming signal strengths. Relative coordinates of neighboring nodes can be obtained by exchanging such information between neighbors. Alternatively, the location of nodes may be available directly by communicating with a satellite using GPS if nodes are equipped with a small low-power GPS receiver.

**Initial gradient setup:** Directed Diffusion [9] makes use of gradient values that are located in the interest message to establish the paths between the sink node and the sources of the data. Several paths can be established, but one will be reinforced by the sink sending the interest again.

**Data delivery:** Data aggregation [10] is performed by the nodes, thereby increasing energy efficiency. A sensor node will generate the traffic at the required rate; will transmit this data to the sink via the established path. The duration and the expiration values received from the interest will control the flow of the traffic from the sensor node.

VI. **CONCLUSION**

Recent advances in WSN have led to many new routing protocols specifically designed for WSN. To prolong the lifetime of the WSN, designing efficient routing protocols is critical. Even though sensor networks are primarily designed for monitoring and reporting events, since they are application dependent, a single routing protocol cannot be efficient for sensor networks across all applications.

**REFERENCES**


