International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 474-480 www.ijaem.net ISSN: 2395-5252

Challenges and widespread review of the current Research in wireless sensor network

N. Sivashanmugam
School of Computer Science, TNOU.

Submitted: 05-11-2022 Accepted: 15-11-2022

ABSTRACT: A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, cost, and system constraints. The goal of survey is to present a comprehensive review of the recent literature in wireless sensor network. This paper reviews the major development and new research challenges in this area.

Keywords — wireless sensor network, environmental monitoring, target, tracking, design objectives, system constraints, research issues, challenges, network architecture.

I. INTRODUCTION

Wireless sensor networks (WSNs) have gained worldwide attention in recent years. Wireless multimedia sensor networks will not only enhance existing sensor network applications such as tracking, home automation, and environmental monitoring, but they will also enable several new applications such as:

- **Area monitoring:** In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors detects enemy intrusion.
- **Air pollution monitoring:** Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens. These can take the advantage of wireless links rather than that of wired installations, which also make them more mobile for testing readings in different areas.
- **Environmental monitoring:** Several projects on habitat monitoring that use acoustic and video feeds are being envisaged, in which information has to be conveyed in a time-critical fashion. For example, arrays of video sensors are already used by oceanographers to determine the evolution of sandbars via image processing techniques.
- **Forest fire detection:** A network of sensor nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and the gases which are produced by fire in the trees of vegetation.

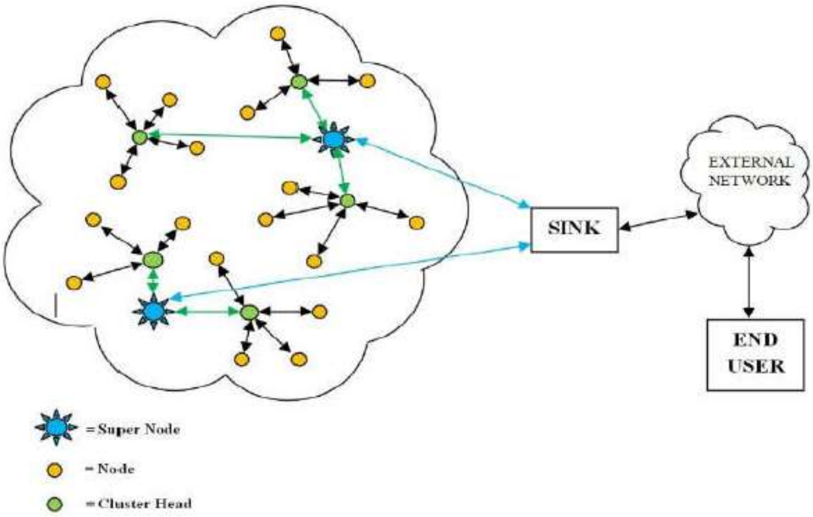

Fig 1. Wireless Sensor Networks

A. Characteristics

▪ Ability to cope with node failures.
▪ Some mobility of nodes.
▪ Heterogeneity of nodes.
▪ Homogeneity of nodes.
▪ Scalability to large scale of deployment.
▪ Ability to withstand harsh environmental conditions.

In this paper we opt to categorize the various strategies for positioning nodes in WSNs. We contrast a number of published approaches highlighting their strengths and limitations. We analyze the issues, identify the various objectives and enumerate the different models and formulations. We categorize the placement strategies into static and dynamic depending on whether the optimization is performed at the time of deployment or while the network is operational, respectively.

B. Assessment of Theoretical Properties and Analysis

New research in WSN is needed to:

1. Measure and assess how the theoretical properties of wireless communication are exhibited in today’s and tomorrow’s sensing and communication devices.

2. Establish better models of communication realities.

3. Account for the communication realities of real world environments.

Few analytical results exist for WSN. They go as follows.

1. What density of nodes is required to meet the lifetime requirements of the system?

2. What sensing and communication ranges are needed to detect, classify and report a target to a base station by a deadline?

3. What sensing range and what nodes need to be awake in order to guarantee a certain degree of sensing coverage for a system?

The next section deals with the strategies of static positioning of nodes.

II.RESEARCH ISSUES AND CHALLENGES IN WSN:

Energy: The first and often most important design challenge for a WSN is energy efficiency. Power consumption can be allocated to three functional domains: sensing, communication, and data processing, each of which requires optimization. The sensor node lifetime typically exhibits a strong dependency on battery life. The constraint most often associated with sensor network design is that sensor nodes operate with limited energy budgets.

Limited bandwidth: In the wireless sensor networks, much less power is consumed in processing data than transmitting it. Presently, wireless communication is limited to a data rate in the order of 10–100 Kbits/second. Bandwidth limitation directly affects message exchanges among sensors, and synchronization is impossible without message exchanges. Sensor networks often operate in a bandwidth and performance constrained multi-hop wireless communications medium. These wireless communications links operate in the radio, infrared, optical range.

Node Costs: A sensor network consists of a large set of sensor nodes. It follows that the cost of an individual node is critical to the overall financial metric of the sensor network [6]. Clearly, the cost of each sensor node has to be kept low for the global metrics to be acceptable. Depending on the application of sensor network, large number sensors might be scattered randomly over an environment, such as weather monitoring. If the overall

Cost was appropriate for sensor networks and it will be more acceptable and successful to users which need careful consideration. Deployment Node deployment is a fundamental issue to be solved in Wireless Sensor Networks. A proper node deployment scheme can reduce the complexity of problems. Deploying and managing a high number of nodes in a relatively bounded environment requires special techniques. Hundreds to thousands of sensors may be deployed in a sensor region. There are two deployment models at present:

- Static deployment: The static deployment chooses the best location according to the optimization strategy, and the location of the sensor nodes has no change in the lifetime of the WSN.
- Dynamic deployment: The dynamic deployment throws the nodes randomly for optimization.

Design Constraints: The primary goal of wireless sensor design is to create smaller, cheaper, and more efficient devices. A variety of additional challenges can affect the design of sensor nodes and wireless sensor networks. WSN have challenges on both software and hardware design models with restricted constraints.

Security: One of the challenges in WSNs is to provide high security requirements with constrained resources. Many wireless sensor networks collect sensitive information. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. The security requirements in WSNs are comprised of node authentication and data confidentiality [3] .To identify both trustworthy and unreliable nodes from a security stand points, the deployment sensors must pass a node authentication examination by their corresponding manager nodes or cluster heads and unauthorized nodes can be isolated from WSNs during the node authentication procedure. As a consequence, sensor networks require new solutions for key establishment and distribution, node authentication, and secrecy.

- **Scalability**: In some applications, tens of thousands of sensors might be deployed. At any time numbers of nods can be increased or decreased. A synchronization scheme should scale well with increasing number of nodes and/or high density in the network.
- **Robustness**: A sensor network is typically left unattended for long times of operation in possibly hostile environments. If any node in the network is break down or go out of then it does not affect the working of other nods in the network and synchronization scheme.
- **Lifetime:** The synchronized time among sensor nodes provided by a synchronization algorithm may be instantaneous, or may last as long as the operation time of the network.
- **Cost and Size:** Wireless sensor nodes are very small and inexpensive devices due to advanced technologies. So its results that synchronization algorithm should not have too much cost and too much large in the size.

III. COMMUNICATION FOR TIME SYNCHRONISATION:

Nodes communicate with each other through sending messages. For instance, nodes that mainly transmit their own sensor readings and nodes that mainly relay messages from other nodes. Sensor readings are routed from the source nodes to the sink via the relay nodes, thus creating a multi-hop topology. However, single-hop communication is slightly different from multi-hop.

- **Single-hop communication**: A sensor node can directly communicate and exchange messages with any other sensor in the single-hop network. However, many wireless sensor network applications span several domains or neighbourhoods. (Nodes within a neighbourhood can communicate via single hop message transmission.) The network is often too large, making it impossible for each sensor node to directly exchange messages with every other node.

- **Multi-hop communication**: The need for multi-hop communication arises due to the increase in the size of wireless sensor networks. In such settings, sensors in one domain communicate with sensors in another domain via an intermediate sensor that can relate to both domains. Communication can also occur as a sequence of hops through a chain of pair wise adjacent sensors.

IV. ALGORITHM AND SURVEY:

This proposed approach includes four phases.

▪ Key pre-distribution
▪ Topology forming /Routing algorithms
▪ Cluster based re-keying
▪ Hierarchical authentication

● **Key pre-distribution:** The first step of our integrated security scheme is key pre-distribution. Suppose we drop a bunch of sensors from the plane to a battlefield, how can we make sure any of two sensors can find a shared key to encrypt/decrypt their messages, i.e. they have a pair wise key? Currently two schemes are proposed to address key pre-distribution problem in sensor networks: key-pool approach and probabilistic approach. We prefer the latter approach since it needs too much memory and calculation overhead of we build a key chain in each sensor and make sure any two sensors share a key at (at least) 50% probability.

● **Topology forming /Routing algorithms:** After sensors are deployed randomly in an area, to reduce key generation overhead (a flat topology can lead an exponential increase of pair wise key generation frequency with the increase of network density we choose some sensors to become cluster heads. The choosing probability decreases with the increase of sensor density [7].

● **Cluster based re-keying:** Between different clusters, to find out low-energy secure path, we propose a concentric topology forming architecture each cluster head maintains a cost level that is determined by the hop number and required communication energy consumption between itself and base station. Cluster-based routing scheme can greatly save communication overhead.

● **Hierarchical authentication:** We adapt a hierarchical broadcast authentication scheme. First we divide the whole lifetime into big time frames. Each frame has a 'frame key' and a pseudo-random function. Inside each 'frame', we further divide it into sub-intervals. The sub-intervals have corresponding authentication keys and a common pseudo-random function.

A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it [3]. The position of sensor nodes need not be engineered or predetermined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities.

Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited to the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad hoc networks are:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification because of the large amount of overhead and large number of sensors. Many researchers are currently engaged in developing schemes that fulfill these requirements.
- In this article we present a survey of protocols and algorithms proposed thus far for sensor networks. Our aim is to provide a better

understanding of the current research issues in this emerging field. We also attempt an investigation into pertaining design constraints and outline the use of certain tools to meet the design objectives. The remainder of the article is organized as follows. We discuss the communication architecture of the sensor networks as well as the factors that influence sensor network design. We provide a detailed investigation of current proposals in the physical, data link, network, transport, and application layers, respectively. We then conclude our article.

V. SENSOR NETWORKS COMMUNICATION ARCHITECTURE

The design factors are addressed by many researchers as surveyed in this article. However, none of these studies has a fully integrated view of all the factors driving the design of sensor networks and sensor nodes. These factors are important because they serve as a guideline to design a protocol or an algorithm for sensor networks. In addition, these influencing factors can be used to compare different schemes.

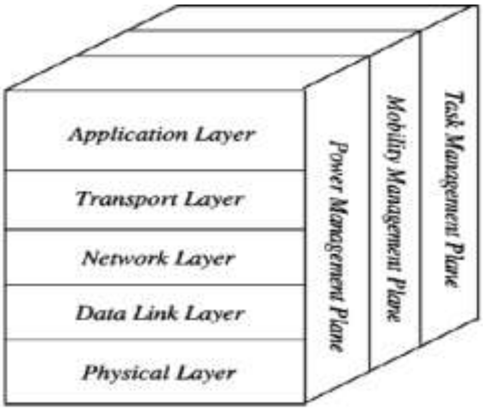

Fig 2. Network Architecture

Fault Tolerance: Some sensor nodes may fail or be blocked due to lack of power, or have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures [1, 2]. The reliability Rk(t) or fault tolerance of a sensor node is modelled in [2, 4] using the Poisson distribution to capture the probability of not having a failure within the time interval :

R k (t) = e – λ k t, (1)

Where, λ k is the failure rate of sensor node k and t is the time period.

The Physical Layer: The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. Thus far, the 915 MHz industrial, scientific, and medical (ISM) band has been widely suggested for sensor networks. Frequency generation, signal detection, modulation, and data encryption. Thus far, the 915 MHz industrial, scientific and medical (ISM) band has been widely suggested for sensor networks. Frequency generation and signal detection have more to do with the underlying hardware and transceiver design and hence are beyond the scope of our article. In the following discussion, we focus on signal propagation effects, power efficiency, and modulation schemes for sensor networks. It is well known that long distance wireless communication can be expensive, in terms of both energy and implementation complexity. While designing the physical layer for sensor networks, energy minimization assumes significant importance, over and above the propagation and fading effects. In general, the minimum output power required to transmit a signal over a distance d is proportional to d n, where 2 < =n < 4. The exponent n is closer to four for low-lying antennae and near-ground channels [6], as is typical in sensor network communication. This can be attributed to the partial signal cancellation by a ground-reflected ray. Measurements carried out in [5] indicate that the power starts to drop off with higher exponents at smaller distances for low antenna heights. While trying to resolve these problems, it is important that the designer is aware of inbuilt diversities and exploits this to the fullest. For instance, multi hop communication in a sensor network can effectively overcome shadowing and path loss effects, if the node density is high enough. Similarly, while propagation losses and channel capacity limit data reliability, this very fact can be used for spatial frequency reuse.

The Data Link Layer: The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network.

In the following two subsections, we discuss some of the medium access and error control strategies for sensor networks.

Network Layer: Sensor nodes are scattered densely in a field either close to or inside the phenomenon, as shown in Fig. 2 Special multi hop wireless routing protocols between the sensor nodes and the sink node are needed. Traditional ad hoc routing techniques do not usually fit the requirements of the sensor networks due to the reasons explained earlier. The networking layer of sensor networks is usually designed according to the following principles:

a. Power efficiency is always an important consideration.

b. Sensor networks are mostly data-centric.

c. Data aggregation is useful only when it does not hinder the collaborative effort of the sensor nodes.

d. An ideal sensor network has attribute-based addressing and location awareness.

Transport Layer: The need for a transport layer is pointed out in the literature [4]. This layer is especially needed when the system is planned to be accessed through the Internet or other external networks. However, to the best of our knowledge there has been no attempt thus far to propose a scheme or discuss the issues related to the transport layer of a sensor network in literature. TCP with its current transmission window mechanisms does match the extreme characteristics of the sensor network environment. An approach such as TCP splitting may be needed to make sensor networks interact with other networks such as the Internet.

In this approach, TCP connections are ended at sink nodes, and a special transport layer protocol can handle the communications between the sink node and sensor nodes, as shown in Fig. 1. As a result, communication between the user and the sink node is by UDP or TCP via the Internet or satellite; on the other hand, communication between the sink and sensor nodes may be purely by UDP-type protocols, because each sensor node has limited memory.

The Application Layer: To the best of our knowledge, although many application areas for sensor networks are defined and proposed, potential application layer protocols for sensor networks remain a largely unexplored region. In this survey, we examine three possible application layer protocols: Sensor Management Protocol (SMP), Task Assignment and Data Advertisement Protocol (TADAP), and Sensor Query and Data Dissemination Protocol (SQDDP), needed for sensor networks based on the proposed schemes related to the other layers and sensor network application areas. All of these application layer protocols are open research issues.

VI. OPEN RESEARCH ISSUES FOR DIFFERENT LAYERS:

The physical layer is a largely unexplored area in sensor networks. Open research issues range from power-efficient transceiver design to modulation schemes:

- **Modulation schemes:** Simple and low-power modulation schemes need to be developed for sensor networks. The modulation scheme can be either baseband, as in UWB, or pass band.
- Strategies to overcome signal propagation effects.
- **Hardware design:** Tiny, low-power, low-cost transceiver, sensing, and processing units need to be designed. Power-efficient hardware management strategies are also essential. Some strategies are managing frequencies of operation, reducing switching power, and predicting work load in processors.

• The development of transport layer protocols is a challenging effort because the sensor nodes are influenced by the factors explained in an earlier section, especially the hardware constraints such as limited power and memory. As a result, each sensor node cannot store large amounts of data like a server in the Internet, and acknowledgments are too costly for sensor networks.

Therefore, new schemes that split the end-to-end communication, probably at the sinks, may be needed where UDP-type protocols are used in the sensor network and traditional TCP/UDP protocols in the Internet or satellite network.

VII. CONCLUSION:

The flexibility, fault tolerance, high sensing fidelity, low cost, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment, and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required. Many researchers are currently engaged in developing the technologies needed for different layers of the sensor networks protocol stack. Along with the current research projects, we encourage more insight into the problems and intend to motivate a search for solutions to the open research issues described in this article.

REFERENCES:

[1]. Singh, M., & Khilar, P. M. (2017). A Range Free Geometric Technique for Localization of Wireless Sensor Network (WSN) Based on Controlled Communication Range. Wireless Personal Communications, 94(3), 1359-1385.

[2]. Lee, S., Park, C., Lee, M. J., & Kim, S. (2014). Multihop range-free localization with approximate shortest path in anisotropic wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, 2014(1), 80.

[3]. Sharma, G., & Kumar, A. (2017). Dynamic Range Normal Bisector Localization Algorithm for Wireless Sensor Networks. Wireless Personal Communications, 97(3), 4529-4549.

[4]. Sharma, G., & Kumar, A. (2017). Improved DV-Hop localization algorithm using teaching learning based optimization for wireless sensor networks. Telecommunication Systems, 1-16. Doi: 10.1007/s11235-017-0328-x

[5]. Sharma, G., & Kumar, A. (2017, May). 3D Weighted Centroid Localization Algorithm for Wireless Sensor Network Using Teaching Learning Based Optimization. In International Conference on Information, Communication and Computing Technology (pp. 117-127). Springer, Singapore.

[6]. Sharma, G., & Kumar, A. (2017). Fuzzy logic based 3D localization in wireless sensor networks using invasive weed and bacterial foraging optimization. Telecommunication Systems, 1-14. Doi: 10.1007/s11235-017-0333-0

[7]. Sheu, J. P., Chen, P. C., & Hsu, C. S. (2008). A distributed localization scheme for wireless sensor networks with improved grid-scan and vectorbased refinement. IEEE transactions on mobile computing, 7(9), 1110-1123.