Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

The Paradigm of Major Issues and Challenges in Wireless Sensor Networks

Shruthi B S[1], Shaila K[2], Venugopal K R[3], L M Patnaik[4]
[1]Asst. Prof., Department of Electronics and Communication, Vivekananda Institute of Technology, Bangalore
[2]Prof. and Head, Department of Electronics and Communication, Vivekananda Institute of Technology, Bangalore, India
[3] Principal, University Visvesvaraya College of Engineering, Bangalore, India
[4]Honorary Professor, Indian Institute of Science, Bangalore, India

Abstract—Wireless Sensor Networks are composed of several thousands of sensor nodes which are capable of sensing, actuating, and relaying the collected information. The technologies that are involved in the design and implementation of Wireless Sensor Networks (WSN include the concepts of Micro-Electro-Mechanical Systems (MEMS), Digital Electronics and Wireless Communications. WSNs are infrastructure less but still they establish communication and form a network with the wireless interface that is inbuilt in the sensors. Due to its pervasive computing capabilities, currently WSNs are widely used in many applications specifically to monitor the real time environment. Thus, the design of WSNs is application specific and considers various parameters like environment, cost, hardware and system constraints. This paper presents an overview of the major research issues and challenges in the design of WSNs in general and compares the performance of the few existing algorithms

Keywords— Data aggregation, Data Dissemation, Hardware optimization, security, Wireless Sensor Networks.

I. INTRODUCTION

A. Wireless Sensor Networks

Wireless Sensor Networks (WSNs) is used for monitoring, recording the physical conditions of the environment and for communicating the information gathered from the monitored field through wireless links. A sensor network consists of collection of sensor nodes which can perform some specific task. The size of the sensor nodes can vary. Compared to other wireless networks, the number of nodes and density of nodes comprising of WSNs is more.

Wireless Sensor Networks consists of a large number of small scale nodes capable of limited computation, wireless communication and sensing. Each sensor node acts like a router which in turn consists of a transducer, micro-computer, transceiver and power source (electric or battery). These networks monitor and record conditions in various applications like temperature, pressure, wind speed, illumination intensity, voltages and chemical concentrations. The nodes in a sensor network collaborate to perform a common task like signal processing of collected sensor data. The transducer generates electrical signals based on the sensed physical quantities, the microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. These devices are equipped with a processor and wireless communication antenna that are powered by a battery. Sensor networks have been useful in many fields like military, health monitoring environment, industry, science, transportation, civil infrastructure, habitat monitoring, security, Video Surveillance, Traffic monitoring, Medical device monitoring, air traffic control and monitoring of weather conditions[1][2].

B. Motivation

Wireless Sensor Networks are constrained by scalability, cost, topology change and power consumption. New technologies are being devised to overcome these and to make sensor networks an integral part of our lives. For efficient and reliable transmission of communication of the sensed data from the sensor field to the sink node, the network has to fulfill the required data accuracy, aggregation delay, fault tolerance, optimum number of active sensors, coverage, energy efficiency, responsiveness, reliability, timeliness, robustness, self-configuration privacy and security. Hence, it is essential to overcome these challenges.

C. Contribution

While designing a WSNs for any particular applications the issues that affect the design and performance of a Wireless Sensor Networks are: (1) Hardware and Operating System for WSN (2) Wireless Radio Communication Characteristics (3) Medium Access Schemes (4) Deployment (5) Localization (6) Synchronization (7) Calibration (8) Design of Network Layer and Transport Layer (9) Data Aggregation and Data Dissemination (10) Database Centric and Querying (12) Programming Models for Sensor Networks (13) Middleware (14) Quality of Service (15) Security. Each of the issues are discussed in this paper.

II. LITERATURE SURVEY

With the widespread growth of application of Wireless Sensor Networks (WSNs), the need for reliable security mechanisms and energy efficiency without compromising QoS parameters of the network has increased.

An overview of the basics of Wireless Sensor Networks, issues, challenges are discussed in [1-2]. Xiaoxia et al.,[3] utilize multiple paths between the source and sink pairs for QoS provisioning and have proposed a probabilistic model of link state for Wireless Sensor Networks. Based on this model, an approximation of local multipath routing algorithm is explored to provide QoS under multiple constraints, such as delay and reliability.

Jianwei et al., [4] have presented R3E, which augments most existing reactive routing protocols in WSNs to provide reliable and energy-efficient packet delivery against unreliable wireless links. It can effectively improve robustness, end-to-end energy efficiency and latency.

Doo et al., [5] describes the vehicular wireless base station for in-vehicle Wireless Sensor Network system and proposes in-vehicle Wireless Sensor Network system applying Wireless Sensor Network Technologies. The in-vehicle WSN system greatly consists of the vehicular wireless base-station, vehicular wireless sensor nodes and wireless OBD (On-Board Diagnostics) module. The vehicular wireless base-station carries out roles which process ECU (Electronics Control Unit) information obtained from wireless OBD module and sensor information received from a number of vehicular wireless sensor nodes.

Brownfield et al., [6] analyzes the energy resource vulnerabilities of WSNs, models the network lifetimes of leading WSN medium access control (MAC) protocols and proposes a new MAC protocol which mitigates many of the effects of denial of sleep attacks. The progression of computer networks extending boundaries and joining distant locations, WSNs emerge as the new frontier in developing opportunities to collect and process data from remote locations like IEEE 802.3 wired and IEEE 802.11 wireless networks, remote WSNs are vulnerable to malicious attacks. While wired and infrastructure-based wireless networks have mature intrusion detection systems and sophisticated firewalls to block these attacks, WSNs have only primitive defenses. WSNs rely on hardware simplicity to make sensor field deployments both affordable and long-lasting without any maintenance support. Energy-constrained sensor networks periodically place nodes to sleep in order to extend the network lifetime. In Denying sleep attacks each sensor node's critical energy resources are rapidly drains and decreases the network's lifetime.

Yamasaki et al., [7] have derived the mutual information in a WSNs with i) censoring sensors, ii) on-off sensors and iii) censoring and on-off sensors. Under the constraint on the average-cost of each sensor, the optimum censoring and sleeping probabilities with respect to the mutual information in the sensor networks is derived and show that the largest mutual information in the sensor network with censoring and on-off sensors can always be achieved. It is shown that the mutual information in the sensor networks with on-off sensors and with censoring and on-off sensors are larger than that in the sensor network with censoring sensors when the average cost of each sensor is small and the observation cost is large.

Fenye et al., [8] have proposed a hierarchical dynamic trust management protocol for cluster-based Wireless Sensor Networks and have considered two aspects of trustworthiness, namely, social trust and QoS trust. A probability model is developed for utilizing stochastic Petri nets techniques to analyze the protocol performance and validate subjective trust against objective trust obtained based on ground truth node status.

Hui et al., [9] describes Network Lifetime Optimization in Wireless Sensor Networks. In this protocol, design of physical, medium access control and routing layers are done in such a way that their network lifetime can be increased. An iterative algorithm is also proposed for large planar networks. Time Division Multiple Access technique is adopted to address the problem of network lifetime. Kareesh-Kuhn-Tucker (KKT) conditions also provide network lifetime maximization for cross layer network design. A unique algorithm is designed which increases the network lifetime for both small and large planar networks.

Leandro et al., [10] proposes DRINA: A Lightweight and Reliable Routing Approach for In-Network Aggregation in Wireless Sensor Networks which reduces the energy consumption of various high density nodes. Data fusion and data aggregation methods can remove the redundancy in the data and can reduce the energy consumption and cost. Reduced number of messages are used for setting up a routing tree, maximized number of overlapping routes, high aggregation rate, reliable data aggregation and transmission. The proposed algorithm includes the Information Fusion-based Role Assignment (InFRA) and Shortest Path Tree (SPT) algorithms. These algorithm provide good performance in aggregation of data.

Ankit et al., [11] elaborates on Cluster Head Election for Energy and Delay Constraint Applications of Wireless Sensor Network and proposes cluster formation that results in good performance with respect to energy and delay constraints of the network. In this cluster formation, cluster head collects and aggregates the data from member nodes and send it to other cluster head or base station, thus achieving good scalability. Analysis of the proposed algorithm has been perfomed by considering two distances Euclidean distance and multi Hop-count distance. Energy consumption was more for Euclidian distance than the multihop count distance. The Hop count exhibited higher delay when compared to Euclidean distance.

Xiaohua et al., [12] have proposed an efficient distributed algorithm that produces a collision-free Schedule for data aggregation in WSNs. Data aggregation scheduling and distributed aggregation scheduling are used to minimize the delay (or latency) in WSNs. Shaojie et al., [9] have described optimum routing strategy for the static sensor network. A number of motion stratifies for the mobile sink(s) to gather real time data from static sensor network, to maximize the network lifetime.

Liu et al., [13] have proposed a novel data aggregation scheme that exploits compressed sensing (CS) to achieve both recovery fidelity and energy efficiency in WSNs with arbitrary topology. Diffusion wavelets were used to find a sparse basis that characterizes the spatial (and temporal) correlations well on arbitrary WSNs, which enables straight forward CS-based data aggregation as well as high-fidelity data recovery at the sink and achieved minimum-energy compressed data aggregation. The compressed data aggregation scheme is capable of delivering data to the sink with high fidelity while achieving significant energy saving.

Chris et al., [14] proposed threat models and security goals for secure routing in Wireless Sensor Networks. They introduce two novel classes of previously undocumented attacks against sensor networks-sinkhole attacks and Hello floods. They have shown, how attacks against ad-hoc wireless networks and peer-to peer networks are adapted into powerful attacks against sensor networks. Security analysis of all the major routing protocols and energy conserving topology maintenance algorithms are proposed for sensor networks.

Shu et al., [15] introduced mechanisms considering single domain that generate randomized multipath routes. Routes taken by the *shares* of different packages change over time. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of overcoming black holes. The proposed algorithms can be applied to selective packets in WSNs to provide additional security levels against adversaries attempting to acquire these packets. However, adjusting the random propagation and secret sharing parameters, different security levels are achieved at different energy costs.

Ming et al., [16] illustrates a new (SRP) Secure Routing Protocol with (QoS) Quality of Service support, called (TQOS) Trustworthiness-based Quality of Service Routing, which includes secure route discovery, secure route setup and trustworthiness-based QoS routing metrics. The routing control messages are secured by using both public and shared keys, which can be generated on-demand. The message exchanging mechanism detect attacks against routing protocols.

Boriello et al., [17] describes the hardware components for a wireless sensor node, is specific with regard to size, costs and energy consumption of the nodes – communication and computation facilities that are considered to be an acceptable quality, but the trade-offs between features and costs is crucial. Potie et al., [18] mentioned the use of different architectures for defining the wireless sensor nodes with change in MAC layer design and use of Hoc Ultra network for low power consumption of the nodes.

Berrou et al., [19] describes the packets destination protocol address. The router determines that it either knows or does not know how to forward the packet to the next hop. If the router does not know how to forward the packet, it typically drops the packet. If the router knows how to forward the packet, it changes the destination physical address to that of the next hop and transmits the packet. Jung et al., [20] describes the distributed data compression where in the distributed nodes are held with protocol with less unevenness.

III. ISSUES AND CHALLENGES IN THE DESIGN OF WSN

(i) Hardware and Operating System for WSN:

A Sensor is a device which senses the information and passes the information gathered on to a mote. Sensors are used for measuring the changes in the physical environment like pressure, humidity, sound, vibration and changes in the health of a person like blood pressure, stress and heartbeat. A Mote consists of processor, memory, battery, A/D converter for connecting to a sensor and a radio transmitter for forming an ad hoc network.

Sensor Node consists of a Mote and Sensor[11]. The structure of the sensor node is as shown in Fig 1. There can be different Sensors for different purposes mounted on a Mote.

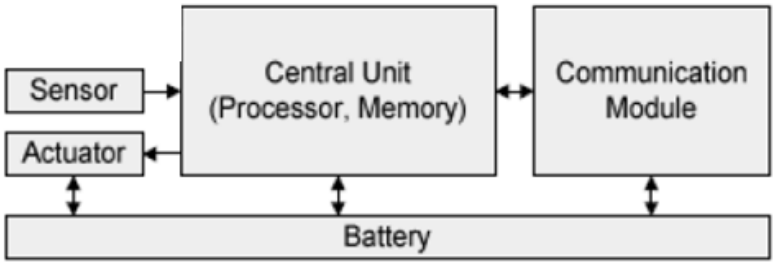

Fig 1. Structure of Sensor node

The design issues of sensor nodes are:

1) In many networks the nodes may not establish connection for many days or may go out of range after establishing the connection. So, the Radio Range of nodes should be high (1-5 kilometers).
2) Energy/Power Consumption of the sensing device should be minimized and sensor nodes should be energy efficient since their limited energy resource determines their lifetime.
3) Sensor Networks consists of thousands of nodes where the cost of the nodes has to be less.

Operating System: An operating system framework for a sensor node should be able to provide memory management and resource management in a constrained environment. The various issues in designing an Operating System (OS) for sensor networks are:

1) In sensor networks a sensor node is mainly responsible for computation of the extracted data from the local environment. It processes the extracted data and manipulates the data as per the requirement of a particular application. All these activities requires the data to be processed and routed. So, concurrency management is needed in sensor nodes.
2) An OS for sensor nodes should be hardware independent and application specific. It should support multihop routing and simple user level networking abstractions.
3) The OS should have inbuilt features to reduce the consumption of battery energy.
4) The OS should have an easy programming model.

(ii)Wireless Radio Communication Characteristics: Performance of Wireless Sensor Networks depends on the quality of wireless communication. The main design issues for communication in WSNs are:

1) To enable long operating lifetime by facilitating low duty cycle operation, local signal processing and low power consumption is must.
2) The effective radio range should not be reduced by various factors like reflection, scattering and dispersions.
3) In order to reduce communication link range and increase density of sensor nodes multihop networking must be accommodated.
4) Long range communication is typically point to point and requires high transmission power, with the danger of being eavesdropped.
5) Communication systems should include error control subsystems to detect errors and to correct them[13][14].

(iii)Medium Access Schemes: MAC protocols should be designed for regulating energy consumption, which in turn influences the lifetime of the network. The various design issues of the MAC protocols that are suitable for sensor network environment are:

1) The design of the MAC protocol should have this switching mechanism to decide when and how frequently the on and off mechanism could be carried out which helps in conserving the energy.
2) A MAC protocol should avoid collisions from interfering nodes, overemitting, overhearing, control packet overhead and idle listening.
3) Scalability, Adaptability and decentralization is another important criterion in designing a MAC protocol.
4) A MAC protocol should have minimum latency and high throughput when the sensor networks are deployed in critical applications.
5) A MAC protocol should include Message Passing.
6) There should be uniformity in reporting the events by a MAC protocol. Since the nodes are deployed randomly, nodes from highly dense area may face high contention among themselves when reporting events resulting in high packet loss.
7) The MAC protocols should take care of the well know problem of Information Asymmetry, which arises if a node is not aware of packet transmissions two hops away.
8) MAC Protocols should satisfy the Real-time requirements[21].

(iv)Deployment: It is to set up an operational sensor network in a real world environment

When sensor nodes are deployed in real world, node die due to energy depletion either caused by normal battery discharge or due to short circuits is a common problem which may lead to wrong sensor readings. Deployment of sensor networks results in network congestion due to many concurrent transmission attempts made by several sensor nodes. Another issue is the physical length of a link. Low data yield is another common problem in real world deployment of sensor nodes. Low data yield means a network delivers insufficient amount of information[22].

(v) Localization: Sensor localization is a fundamental and crucial issue for network management and operation. The sensors are deployed without knowing their positions in advance and also there is no supporting infrastructure available to locate and manage them once they are deployed. Determining the physical location of the sensors after they have been deployed is known as the problem of localization. The following requirements has to be met by localization algorithm:

1) The localization algorithm should be distributed since a centralized approach requires high computation at selective nodes to estimate the position of nodes in the whole environment.
2) To implement energy efficient message routing protocols in sensor networks the awarenesss of the node location can be used.
3) Localization algorithms should be robust enough to localize the failures and loss of nodes. It should be tolerant to error in physical measurements.
4) The precision of the localization increases with the number of beacons. The main problem with increased beacons is that they are more expensive than other sensor nodes and once the unknown stationary nodes have been localized using beacon nodes then the beacons become useless.
5) Methods that depend on measuring the ranging information from signal strength and time of arrival require specialized hardware that is typically not available on sensor nodes.
6) The algorithm should be precise, scalable and support mobility of nodes[23].

(vi) Synchronization: Time Synchronization in a sensor network aims to provide a common timescale for local clocks of nodes in the network. A global clock in a sensor system will support to process and analyze the data correctly and predict future system behavior. Some applications that require global clock synchronization are environment monitoring, navigation guidance, vehicle tracking etc[24]. Due to some equipments like GPS (Global Positioning System) receivers or NTP (Network Time Protocol) consumes more energy. The lifetime or the duration for the nodes which are spread over a large geographical area needs to be taken into account. Sensor nodes need to coordinate and collaborate to achieve a complex sensing task like data fusion. If the sensor nodes lack synchronization among themselves then the data estimation will be inaccurate. Traditional synchronization protocols try to achieve highest degree of accuracy. The higher the accuracy, more the requirement of resources. The algorithm needs to achieve multihop synchronization even in the presence of high jitter.

(vii) Calibration: It is the process of adjusting the raw sensor readings obtained from the sensors into corrected values by comparing it with reference values. Manual calibration of sensors is a time consuming and difficult task due to failure of sensor nodes and random noise which makes manual calibration of sensors costly. Different issues in Calibration of sensor networks are:

1) Access to individual sensors in the field can be limited.
2) Reference values might not be readily available.
3) Different applications require different calibration.
4) Calibration is required in a complex dynamic environment with many observables like aging, decaying, damage etc.
5) Calibration include accuracy, resilience against random errors, ability to be applied in various scenarios and to address a variety of error models[25].

(viii) Network Layer and Transport Layer Challenges

***Network Layer Issues*:** Over the past few years sensor networks are being built for specific applications and routing is important for sending the data from sensor nodes to Base Station (BS). Various issues at the network layer are:

1) Different techniques have to be developed to minimize energy conservation otherwise, the lifetime of the network is reduced.
2) Routing Protocols should incorporate multi-path design technique.
3) Fault tolerance is another desirable property. The protocols should aim to find a new path at the network layer even if some nodes fail or block due to some environmental interference.
4) In the network layer in order to maximize energy savings a flexible platform is to be provided for performing routing and data management.
5) The data traffic that is generated will have significant redundancy among individual sensor nodes since multiple sensors may generate same data within the vicinity. The routing protocol should exploit such redundancy to improve energy and bandwidth utilization.
6) Due to the adhoc routing infrastructure, a routing protocol should have the property of multiple wireless hops.
7) Routing Protocols should take care of heterogeneous nature of the nodes because each node is different in terms of computation, communication and power[26].

***Transport Layer Issues*:** Transport layer provides End to End reliable communication. The various design issues for Transport layer protocols are:

1) A transport protocol should ensure orderly transmission of the fragmented segments.
2) The limited bandwidth affects the normal data exchange and may lead to packet loss and traffic congestion.
3) Bit error rate results in packet loss and more energy consumption. A transport protocol should be reliable for delivering data to potentially large group of sensors under extreme conditions.
4) End to End communication may suffer since the placement of nodes is not predetermined and external obstacles may cause poor communication performance between two nodes.
5) The data that flows from sink to source is sensitive to message loss[26].

(ix) Data Aggregation and Data Dissemation: Data gathering involves systematically collecting the sensed data from multiple sensors and transmitting the data to the base station for further processing. But the data generated from sensors is often redundant and also the amount of data generated may be very huge for the base station to process it. Hence, mechanisms have to be developed for combining the sensed data into high quality information and this is accomplished through Data Aggregation. It is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and estimating the desired result about the sensed environment, then providing fused information to the base station.

Few of the design issues in data aggregation are:

1) Sensor networks are unreliable and few information may be unavailable or expensive to obtain; like the number of nodes present in the network and the number of nodes that are responding and also it is difficult to obtain complete and upto date information of the neighboring sensor nodes to gather information.
2) The energy conservation can be performed by activating few nodes to transmit the data directly to the base station or to have less transmission of data to the base station.

3) Meta data negotiations is done to eliminate transmission of redundant data..
4) Improving the clustering methods for data aggregation to conserve energy of the sensors.
5) Improving In-Network aggregation techniques to achieve energy efficiency.

Data dissemination is a process by which data and the queries for the data are routed in the sensor network. It is a two step process. In the first step, if a node is interested in some events, like temperature or humidity, then it broadcasts its interests to its neighbors periodically and then through the whole sensor network. In the next step, the nodes that have the requested data sends the data back to the source node after receiving the request. In data dissemination all the nodes including the base station can request for the data while in data aggregation all the aggregated data is periodically transmitted to the base station. Flooding is one important protocol which includes data dissemination[14][15].

(x) Database Centric and Querying: Wireless Sensor Networks have the potential to span and monitor a large geographical area producing massive amount of data. So, sensor networks should be able to accept the queries for data and respond with the outcome. The design issues and requirements of a sensor network are.
1) Data collection should not be interrupted.
2) Sensor data exposes more errors due to interference of signals and device noise.
3) The data has to be updated frequently since it is produced continuously on large scale.
4) Another important constraint that needs to be taken care in a sensor network database is storage and scarce of energy [27].

(xi) Architecture**:** The key issues that must be addressed in the sensor architecture are:
1) Several operations like data calculations, monitoring of the communication channel, encoding of data and transferring of bits need to be executed parallely.
2) It should allow topological changes with minimum update messages being transmitted.
3) The system must be capable to meet wide range of applications since the Wireless Sensor Networks do not have a fixed set of communication protocols.
4) It should must provide precise control over radio transmission timing.
5) It should decouple the data path, speed and the radio transmission rate.

(xii) Programming Models for Sensor Networks
Considerable research activity has been taken place in designing the programming models for sensor networks: A reactive, event driven programming model is required to achieve efficient bandwidth. Since resources in a sensor network are very scarce, programming models should help programmers in writing energy efficient applications. The run time errors and complexity should be reduced since the applications in a sensor network need to run for a long duration without human intervention [19][20].

(xiii) Middleware: Middleware for Wireless Sensor Network should aid in development, maintenance, deployment and execution of sensing-based applications. WSN middleware can be considered as a software infrastructure that binds together the network hardware, operating systems, network stacks and applications. Middleware should provide an interface to the various types of hardware and networks supported by primitive operating systems. Middleware should provide new programming paradigm to provide application specific API's rather than dealing with low level specifications. Middleware solutions should deal with the complexity involved in configuring individual nodes based on their capabilities and hardware architecture. The mechanisms should provide real time services by dynamically adapting to the changes in the environment and data. There should be transparency in the middleware design and should incorporate real time priorities. Priority of a message should be assigned at runtime by the middleware and should be based on the context. It should support quality of service considering many constraints which are unique to sensor networks like energy, data, mobility and aggregation. Security has become a paramount importance with sensor networks being deployed in mission critical areas like military, aviation and in medical field[23].

(xiv) Quality of Service is the level of service provided by the sensor networks to its users. Various Quality of Service issues in sensor networks includes: It is difficult to achieve QoS in WSN because the network topology may change constantly and the available state information for routing is inherently imprecise. Sensor networks need to be supplied with the required amount of bandwidth so that it is able to achieve a minimal required QoS. Traffic is unbalanced in sensor network since the data is aggregated from many nodes to a sink node. QoS mechanisms should be designed for an unbalanced QoS constrained traffic. Many a time routing in sensor networks need to sacrifice energy efficiency to meet delivery requirements. Also, redundant data makes routing a complex task for data aggregation affecting Quality of Service in WSN. Multihop routing requires buffering of huge amount of data. This limitation in buffer size will increase the delay variation that packets incur while traveling on different routes and even on the same route making it difficult to meet QoS requirements. QoS designed for WSN should be able to support scalability. Adding or removing of the nodes should not affect the QoS of the WSN[12].

(xv) Security in sensor networks is an important factor and it is very challenging. Some of the basic security requirements that has to be taken care are: Confidentiality is to be maintained to protect sensitive information. Authentication

techniques verify the identity of the participants in a communication. Lack of integrity may result in inaccurate information. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function. Sensor network should be designed for freshness; so that the packets are not reused thus preventing potential mix-up. In sensor networks secure management is needed at the base station level. Challenges like Key distribution to sensor nodes in order to establish encryption and routing information need secure management. Also, clustering techniques require secure management, since each group of nodes includes a large number of nodes that need to be authenticated with each other and exchange data in a secure manner. Security mechanisms like encryption should be light weight so that the overhead is minimized and should not affect the performance of the network[15][16].

IV. COMPARISON OF PERFORMANCE

The performance of existing algorithms are compared in Table 1 with respect to various parameters

TABLE. I: COMPARISON OF THE PERFORMANCE OF DIFFERENT PARAMETERS OF WSNS

Author	Algorithm/protocol	Concept	Performance
Hui Wang et al., [17]	Kareesh –Kuhn-Tucker(KKT)	Optimal design is done on power control at the physical layer. The design is based on cross layer approach	Optimization of network lifetime. Power controlling is increased
Traynor et al., [24]	Hybrid security Mechanism	proactive and reactive key establishment mechanism for networks using balanced method of key management.	Adaptive security in infrastructure and infrastructureless environment
Wang et al., [28]	Efficient code dissemination protocol	Dynamically configures the packet sizes and accurately selects the sender	Shortens the time spent in selection of sender avoids transmission collision and transmission over poor links
Leandro et al., [16]	DRINA	Redundant data is aggregated. Shortest path is established between the source and the sink	High and reliable data aggregation. Maximum number of overlapping routes.
Ozgur B Akhan et al., [25]	Event to sink Reliable transport	Sink will collect the information of the sensor nodes within the event radius no end-to-end reliability.	Congestion control is achieved. Maximization of reliability and conservation of energy
Ghazi Bouabene et al., [26]	Autonomic Network Architecture	designing and developing a network architecture	maximize the degree of flexibility to support functional scaling.
Jianwei et al., [27]	R3E	routing protocols for energy-efficient packet delivery against unreliable wireless links	improve robustness, end-to-end energy efficiency and latency
Ming et al., [13]	SRP and TQOS	secure route discovery, secure route setup and trustworthiness-based QoS routing metrics	routing control messages are secured by using both public and shared keys

V. CONCLUSIONS

Wireless Sensor Networks (WSN) are used in variety of fields which includes military, healthcare, environmental, biological, home and other commercial applications. The literature survey on Wireless Sensor Networks gives an insight that designing a sensor node is a challenging task and assessments of different parameters which includes range, antenna type, target technology, components, memory, storage, power, life time, security, computational capability, communication technology, power, size and programming interface. In this paper, we have discussed a comprehensive

list of various issues associated with WSN. The future prospects of WSN applications are highly promising to revolutionize our everyday lives. The performances of existing algorithms are compared with respect to various parameters.

REFERENCES

[1] Ahmad Sardouk and Leila Merghem-Boulahia,"Data Aggregation in WSNS:A Survey", in International Journal of Computer Applications, vol. 54, no. 15, pp. 2688-2710, October 2010.

2] V Akila1 and T Sheela," Overview of Data Aggregation Based Routing Protocols in Wireless Sensor Networks", in International Journal of Emerging Technology and Advanced Engineering, vol. 4, no. 10, pp. 765-771, June 2013.

[3] Jaydip Sen, "A Survey on Wireless Sensor Network Security", in International Journal of Communication Networks and Information Security (IJCNIS), vol. 1, no. 2, pp. 55-78, August 2009.

[4] S Lindsey, C Raghavendra and K.M.Sivalingam, "Data Gathering Algorithms in Sensor Networks using Energy Metrics," in IEEE Trans. on Parallel and Distributed Systems, vol. 13, no. 9, pp. 924-935, September 2002.

[5] H O Tan and I Korpeoglu, " Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks", vol. 32, no. 4, pp. 66-71, December 2003.

[6] P. Ji, Wu Chengdong, Yunzhou Zhang, "DAST: A QoS-Aware Routing Protocol for Wireless Sensor Networks", in Proceeding of International Conferences on Embedded Software and Systems Symposia, *Sichua*n, pp. 259-264, July 2008.

[7] Ulya Sabeel and Saima Maqbool, "Categorized Security Threats in the WSNs: Counter Measures and Security Management Schemes", in International Journal of Computer Applications (0975-8887), vol. 64, no. 16, pp. 19-28, February 2013.

[8] E S Jung and N H Vaidya, A Power Control MAC Protocol for Ad Hoc Networks, in Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking 2002 (MobiCom), Atlanta, Georgia, vol. 5, no. 2, pp. 212-217, September 2002.

[9] C Berrou and A Glavieux, Near Optimum Error Correcting Coding and Decoding: Turbo-Codes, in IEEE Transactions on Communications, vol. 3, no. 1, pp. 44–53, 1996.

[10] G J Pottie and W J Kaiser, Embedding the Internet: Wireless Integrated Network Sensors, in Proceedings of Communications of the ACM, pp. 43-47, 2000.

[11] Boriello and R Want, Embedded Computation Meets the World Wide Web, in Proceedings of Communications of the ACM, pp. 43-47, 2000.

[12] T Shu, M Krunz and S Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," in IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954, July 2010.

[13] Ming Yu and Kin K Leung, "A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks," in IEEE Transactions on Wireless ommunications, vol. 8, no. 4, pp. 1023- 1038, April-2009.

[14] Chris Karlop and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in Proceedings of the First IEEE Communications, Elsevier, pp. 113-127, 2003.

[15] Liu D and Ning P (2003) 'Establishing Pairwise keys in Distributed Sensor Networks', In Proceedings of Tenth ACM Conference on Computer and Communications Security (CCS '03), pp.52–61, Washington DC, USA, October.

[16] Leandro Aparecido Villas, Azzedine Boukerche, Heitor Soares Ramos, Horacio A.B. Fernandes de Oliveira, Regina Borges de Araujo, and Antonio Alfredo Ferreira Loureiro "DRINA: A Lightweight and Reliable Routing Approach for In-Network Aggregation" in IEEE Transactions on Computers, vol. 62, no. 4, pp. 676-689, April 2013.

[17] Hui Wang, Nazim Agoulmine, Maode Ma, and Yanliang Jin "Network Lifetime Optimization in Wireless Sensor Networks" in IEEE Journal on Selected Areas in Communication, vol. 28, no. 7, pp. 1127-1137, September 2010.

[18] Ankit Thakkar, Ketan Kotecha, "Cluster Head Election for Energy and Delay Constraint Applications of Wireless Sensor Network", in IEEE Transactions on Computers, vol. 62, no. 4, pp. 676-689, April 2013.

[19] Fenye Bao, Ing-Ray, MoonJeong and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," in IEEE Transactions on Networks and Service Management, vol. 9, no. 2, pp. 169-183, June 2012.

[20] Wong, Tsuchiya and Kikuno. T, "A Self-organising Algorithm for Sensor Placement in Wireless Mobile Microsensor Networks", in International Journal of Wireless and Mobile Computing, Inderscience, vol. 3, no. 1–2, pp. 69–78, 2008.

[21] I F Akyildiz, W Su, Y Sankarasubramaniam and E Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, pp. 393-422, 2002.

[22] F Stann and J Heidemann, "RMST: Reliable Data Transport in Senor Networks," in Proceedings of IEEE , Anchorage, Alaska, USA, pp. 75-79, 2003.

[23] Ali Chamam and Samuel Pierre, "On the Planning of Wireless Sensor Networks: Energy-Efficient Clustering under the Joint Routing and Coverage Constraint", in IEEE Transaction on Mobile Computing, vol. 8, no. 8, pp.89-95, August 2009.

[24] Traynor P, Kumar R, Saad H B, Cao G and La Porta T, "LIGER: A Hybrid Key Management Scheme for Heterogeneous Sensor Networks", in Proceedings of ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys '06), pp.15–27.

[25] Özgür B Akan and Ian F Akyildiz, " Event-to-Sink Reliable Transport in Wireless Sensor Networks" in IEEE/ACM Transactions on Networking , vol. 13, no. 5, pp. 1033-1066, October 2005.

[26] Ghazi Bouabene, Christophe Jelger, Christian Tschudin, Stefan Schmid, Ariane Keller and Martin May,"The Autonomic Network Architecture (ANA)", in IEEE Journal on Selected Areas in Communications, vol. 28, no. 1, pp. 33-39, January 2010.

[27] Jianwei Niu, Long Cheng, Yu Gu, Lei Shu and Sajal K Das, " R3E: Reliable Reactive Routing Enhancement for Wireless Sensor Networks" in IEEE Transactions on Industrial Informatics, vol. 10, no. 1, pp. 784 – 794, February 2014.

[28] C Wang, Xiaoxing Li "A Survey of Transport Protocols for Wireless Sensor Networks", in IEEE Network, Vol. 20, Issue 3, pp 34 – 40, June 2006.

