

Review paper on Reliability of Wireless Sensor Networks

GAGANDEEP KAUR¹

Abstract - Wireless Sensor Network (WSN) has attracted many concerns in different domains because of its special features. A WSN is a set of a large number of resource constrained sensor nodes which have abilities for information detection, data processing, and short-range radio communication. WSN can be used for both military applications and civil applications with the tasks such as detection and monitoring of significant events in different environments or large areas. How to improve the reliability of WSN is one of the essential challenges for WSN from theoretical research to actual application. Reliability is the main issue in the Wireless Sensor Networks (WSN). Reliable data transport is an important facet of dependability and quality of service in wireless sensor networks. In this paper, the various techniques proposed for minimizing the energy consumption have been discussed. This is done primarily to give an overview of the various techniques known today for reliable data transport problem and minimizing the energy consumption in wireless sensor networks.

Keywords: BS, Reliability, WSNs,.

I. INTRODUCTION

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. The majority of WSNs described in the literature exhibit a (source, sink) architecture, which may include any number of:

Source nodes: which generate data, usually by using sensors to measure environmental factors such as temperature, humidity or radiation,

Sink nodes: which collect the data gathered by source nodes and

Intermediate nodes: which may include source nodes that aid the transmission from source to sink.

Wireless sensor networks (WSNs) are typically composed of hundreds to thousands of small collaborating wireless sensor nodes. The development of WSN has received increasing attention

from various industries. The main task of a wireless sensor network is to monitor the area concerned, collect data and transmit the data to the sink node. Sink node makes the decision based on the collected data from one or more source nodes. In wireless sensor networks, sensors are usually deployed in some harsh environment by aircrafts in order to achieve the specific quality of service. Sensors have only limited battery energy and communication capacities while they need to work for a long time. One essential requirement for sensor networks is the reliability of applications. [2] A key functionality of WSNs consists in obtaining and transporting the information of interest (e.g., events/status) required by the different applications having varied requirements on the reliability and timeliness of data delivery. While node redundancy, inherent in WSNs, increases the fault tolerance, no guarantees on reliability levels can be assured. Furthermore, the

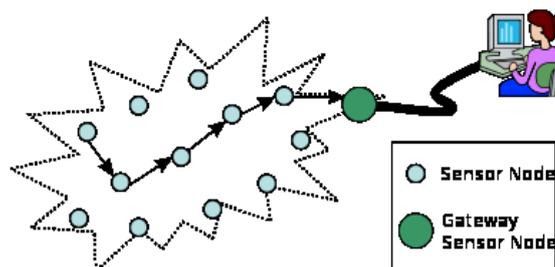


Figure 1: Structure of WSN

frequent failures within WSNs impact the observed reliability over time and make it more challenging to achieve the desired reliability. Unfortunately, a framework for modeling reliability of data transport protocols in WSNs is currently missing. [1]

II. RESEARCH CHALLENGES

We have introduced the features, concepts and state of art of a WSNs. Although advances have been made towards a mature WSN technology, we still have some more distance to travel to reach a pervasive WSNs in the daily life. To cover the remaining distance, several challenges has to be overcome. These challenges have to be beard in mind while tackling all the eleven topics introduced in the last section. They are not related to a specific protocol, but rather closely connected to user's key requirements to a WSN. The author of lists energy, reliability, standardization, cost, ease of use, and node size as major barriers. In the above challenges, we have chosen energy and reliability as the two major challenges to researchers while the others fall in the scope of engineers and policy makers. While the first one is concerned with the possible size and workload in a WSN, solving the later one accelerates the research. Thus we limit our self in this thesis to

these two challenges and discuss them in detail in the following sections.

Reliability:

Reliability is a big barrier for WSN to be commercialized. A wireless link is generally felt to be unreliable compared to wire. Due to attenuation, shadowing and interference, a packet transmitted on a wireless link can be lost. Since WSNs may be deployed in a harsh environment and operates in the the industrial, scientific and medical (ISM) band, they are prone to the above problems. The last but not the least, the imperfect hardware may also cause unreliability. By imperfection we do not mean malfunction of hardware. Instead we mean the problem arisen due to the low cost hardware which can not be miniaturized without compromising on some precisions. For example, clocks on the devices may drift with time; the coverage of antennas on these device is far from omni-directional, thus a common assumption of omni-directional antenna beam in WSN research is not valid anymore. This challenge has to be addressed when designing a WSN protocol.

Energy:

In WSNs, since devices are left untouched the energy consumption need to be taken into account. While the number of transistor on a chip doubling every 18-24 months, according to Moore's law, the energy capacity in a battery only increases 8-10% per year and this trend is continuing. It means that instead of two year, the battery energy capacity doubles every 10 years. This mismatch is driving researchers to explore how to extend the lifetime of WSNs.

Scalability:

A WSN may contain only a few nodes or hundreds of node. An event may be tracked with a frequency of once per day or once per second. An event may be reported only by a single node or by many nodes simultaneously. In the latter cases, scalability of the WSN is challenged. Since the devices operate in the same frequency, transmissions from different nodes may contend with each other or even collide. Applications such as fire monitoring can not tolerate consequences of the contention and collision, either delay or miss of detection leads to great damage. Since links suffer from contentions or collisions, routes can be unreliable due link variability. Researchers have been trying to select relatively more reliable links to build up a route. Although contentions and collisions in a large network can be alleviated by an advanced scheduling protocol, which coordinates node to access the medium at different times, more solutions are available. For instance, we can reduce transmission power of nodes so that less contentions are expected; nodes can also gather into groups, e.g. clusters, where only a head of the cluster participates in routing or management traffic, so that less traffic is generated and contentions and collisions are reduced.

Ease of use:

Ease of use is a key factor for WSNs to be deployed in large scales. Since many WSN applications are expected in consumer sector, such as agricultural monitoring, home and business building automation, health care, asset tracking etc. The users in these sectors normally do not have any experience to configure the network or diagnose in case of faults. Thus WSN has to be pre-configured or should have the ability to self-configuring, self-organizing and self-diagnosing. With respect to networking, self-

configuration and self-organization are normally interchangeable. Both the two concepts refer to the process that nodes learn the topology of a network automatically and cooperate together to achieve a common objective. In WSNs, the objective includes sensing a target, saving energy, etc. A self-organized WSN does not require any pre-configuration before deployment but configures itself based on the environment. Such configuration includes topology of the network, route construction, transmission range control, etc. After deployment, a WSN should be able to find out malfunctions then repair them or report to a control center. This challenge definitely sets a higher standard in protocol and algorithm design in WSNs.

Ease of set up in research:

Ease of use is a requirement from the point of view of end users. Researchers also have this demand. Instead of ease of use, the requirement in the academical world is more inclined to ease of set up. Researchers frequently have to check feasibility or evaluate performance of the proposed protocols or solutions. Two methods are available. Simulation is the first and the usual tool to study the communication capabilities and the configurations of WSNs, since experiments are difficult to perform. Although it is relatively convenient to setup, some characteristics of real world are hard to simulate. Thus when the researchers have to do a performance study, they face the choice between a simulation and a real world experiment. To ease the setting up of a WSN, collection of data, remote monitoring and changing the protocols during research is also a challenge for researchers.

III. RELIABILITY IN WIRELESS SENSOR NETWORK

Reliability in WSN reflects a functional unit's ability to meet performance specifications over a specified period of time and this is often expressed as a probability or mean time to failure (MTTF). Fault tolerance in WSN is the quality or ability of a functional unit to perform a required task in the presence of some number of faults or errors. The distinction is that the former is an attribute relating to the performance period until a fault is encountered while the latter is with regard to the system's performance in the presence of one or more failed components. Fault tolerance is applied to increase the reliability of a system.

IV. RESEARCH OBJECTIVES

The primary objectives of research are the following –

- Sensing the environment and sending the sensed data to a remote place via sink with greater reliability is the primary objective of WSNs.
- To study and analyze the problem of reliable data communication in wireless sensor networks.
- To study the advantages and drawbacks of the various schemes proposed in literature for reliable data communication.
- To propose and evaluate a approach for ensuring reliability and balanced energy consumption.
- The primary idea in this paper is to address and analyze the reliability issues to device a reliable and fault tolerance model for a sensor network system
- A sensor node is battery powered, so has limited power source and also it has small computational power and memory space. Therefore we can't play complicated

algorithm to achieve the reliability. We can't send many control packets to tune the network, nor can we run sophisticated algorithm in sensor nodes.

- Packets has to be transported in a reliable way and in time through the sensor network and thus data reliability becomes very relevant for the proper functioning of the network. Most of the solutions available in literature address a specific reliability and fault tolerance problem but ignore other issues like fast delivery and successful transmission of packets in presence of some missing and mistaken bits due to noise, etc. in the communication channel.
- Number of algorithms have studied the use of encoding techniques to enhance the reliability of the communications like Reed-Solomon encoding, data encoding to combat channel fading and distributed classification fusion approach using error correcting codes. There is still scope to enhance the reliability of communications by using neural network based encoding and clustering techniques.
- There is a need of some mechanism to overcome the problems coming from wireless communication medium and limited resources. In WSNs, the medium of communication is wireless which is more unreliable than wired system as wireless channel is more noisy. Because of disturbances/ noise, the information of interest may not be delivered successfully at the destination.

VI. CONCLUSION

Poles apart WSN applications necessitate unusual positions of reliability. Communication protocols for WSN should be reliable and energy-efficient to keep away from unproductive stabbing of energy resources through minimization of control and retransmission overhead. In this paper, WSN reliability research fields are discussed. Future directions and technical challenges are proposed. These objectives can be obtained by developing the efficient mechanism for clustering the sensor nodes in heterogeneous WSNs. We can have cluster based efficient data aggregation technique which considers both energy and reliability.

REFERENCES

- [1] Paulo Rogério Pereira, António Grilo, Francisco Rocha, Mário Serafim Nunes, Augusto Casaca, Claude Chaudet, Peter Almström and Mikael Johansson, "End-To-End Reliability in Wireless Sensor Networks: Survey and Research Challenges", in EuroFGI Workshop on IP QoS and Traffic Control, P. Pereira (Ed.), Lisbon, Portugal, December 6-7, 2007.
- [2] Nan Yao, Shaoping Wang, Yaoxing Shang*, Jian Shi "Reliability of Wireless Sensor Network: Hotspot and Critical Challenges" Science and Technology on Aircraft Control Laboratory, School of Automation Science and Electrical Engineering Beihang University ©2012 IEEE
- [3] Dhanashari N Wategaonkar, Vivek S. Deshpande "Characterization of Reliability in WSN" ©2012 IEEE
- [4] Vijay Kumar (Member, IEEE), R. B. Patel (Member, IEEE), Manpreet Singh (Member, IEEE) and Rohit Vaid Reliability Analysis in Wireless Sensor Networks Vijay Kumar et al. / International Journal of Engineering and Technology Vol.3 (2), 2011, 74-79
- [5] Hao Wen, Chuang Lin, Fengyuan Ren, Yao Yue, Xiaomeng Huang, "Retransmission or Redundancy: Transmission Reliability in Wireless Sensor Networks", in Proceedings of the IEEE 2007.
- [6] Andreas Willig, Holger Karl "Data Transport Reliability in Wireless Sensor Networks — A Survey of Issues and Solutions"

- [7] Muhammad Adeel Mahmood and Winston Seah Reliability in Wireless Sensor Networks: Survey and Challenges Ahead School of Engineering and Computer Science, Victoria University of Wellington, Wellington, New Zealand
- [8] Vivek Katiyar, Narottam Chand, Surender Soni, "A Survey on Clustering Algorithms for Heterogeneous Wireless Sensor Networks", in Int. J. Advanced Networking and Applications", Volume: 02, Issue: 04, Pages: 745-754 (2011).

Author's Profile



Gagandeep Kaur received the B.Tech degree in Information and Technology in 2012 from N.C. Institute of Technology and Management, Panipat, India. Currently he is pursuing his M.Tech degree in Computer Science and Engineering, KITM, Kuk, India. Her area of research is Wireless Sensor Networks.