Islamic university Of Technology
Department Of Computer Science and Engineering (CSE)

APPLICATION SPECIFIC ENERGY AWARE AND RELIABLE ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK

Authors:

Md Rashedur Rahman (114421)
Enam Ahmed Shahaz (114444)

Supervisor:

Dr. Md. Motaharul Islam
Assistant professor
Department of Computer Science and Engineering

A thesis submitted to the Department of CSE
in partial fulfilment of the requirements for the degree of
B.Sc. Engineering in CSE
Academic Year: 2014-2015

….to Almighty Allah

Acknowledgements

Thanks to Allah (SWT), the most gracious and most merciful. The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of the people whose ceaseless cooperation made it whose constant guidance and encouragement crown all efforts with success.

We would like to express our heartfelt thanks to our supervisor Dr. Md. Motaharul Islam for his continuous and invaluable support throughout our thesis work. His constructive ideas helped us a lot to find right way in our research.

Finally we are indeed very much grateful to our parents for continuous prayer, help and support.

MD. Rashedur Rahman (114421)

Enam Ahmed Shahaz (114444)

November, 2015.

Declaration of Authorship

This is to certify that the work presented in this thesis is the outcome of the analysis and investigation carried out by Md Rashedur Rahman and Enam Ahmed Shahaz under the supervision of Dr. Md. Motaharul Islam in the Department of Computer Science and Engineering (CSE), IUT, Dhaka, Bangladesh. It is also declared that neither of this thesis or any part of this thesis has been submitted anywhere else for any degree or diploma. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of reference is given.

Authors:

____

MD. Rashedur Rahman (114421)

____

Enam Ahmed Shahaz (114444)

Supervisor:

____

Dr. Md. Motaharul Islam

Assistant Professor

Department of Computer Science and Engineering

Islamic University of Technology (IUT)

Table of contents

Abstract

Wireless sensor network has brought a new era in wireless network. Its intense usage in different application area has led the designer as a new network architecture paradigm. Due to its uniqueness, traditional wireless ad hoc network mechanism does not suit well in this scenario. So the application developer has to develop new techniques that can suit better in this kind of network. Many new protocols, networking architectures etc. are being proposed. Wireless network architectures differ from application to application. Different application demands different mechanism. Recent advances in wireless sensor networks have led to many new protocols specifically designed for sensor networks where energy awareness is an essential consideration. But for health care application only energy awareness cannot achieve the ultimate goal of the sensor network. For that purpose, the reliability of links is also important in this kind of scenario. Many protocols like RPL, CTP etc. are proposed in this context. In this paper we proposed an application specific routing protocol for the health care application. Our proposed routing protocol is devoted to improve the throughput of data packet transmission in health-care application.

Chapter 1
Introduction

1.1 Background

In the world of sensor networks small is big and unity is strength. In this fascinating domain one needs to think at micro level rather than at the macro. The designer of this network needs to think one hundred times before he decides to introduce communication of few bytes of data. Even a three volt battery is considered to be considerably huge source of energy to a sensor node. And the sensor node itself is as big as a dollar. Wireless sensor network collects data utilizing a group of tiny sensor nodes and here the data as a whole is more important than the individual sensor node collecting the . Hence it is appropriate to say that "In sensor network small is big and unity is strength ".

Wireless sensor network consists of a group of tiny sensor nodes, distributed in a wide geographic area, forming an ad-hoc network, collecting and conveying information regarding the area under surveillance. The data collected by these sensor nodes is aggregated and analyzed at a more capable node called as sink or gateway or base station. Wireless sensor network combine simple wireless communication, minimal computation facilities and some sort of sensing of the physical environment and this leads to a new paradigm of networks that can be deeply embedded in our physical environment, fueled by the low cost and wireless communication facilities.

1.1.1 Schematic Diagram of a Sensor Node

Sensor Network is made up of many sensor nodes. These nodes are tiny in size. They have limited, power supply, memory and processing capability. Each sensor consists of, Transceiver, Power supply, Processor, Memory and Sensors. The overall architecture of a sensor node is shown in the diagram below.

Every sensor node should try to meet various design requirement of any sensor network, i.e. they should be inexpensive, small, less power consuming, robust, and equipped with right sensors to sense the environment. The node should be as small as 1 cc in size , weigh less than 100 g , be cheaper than 1$ and dissipate power less than 100 micro Watt. However it may not be possible in to meet all the above said requirements all cases or in many cases.

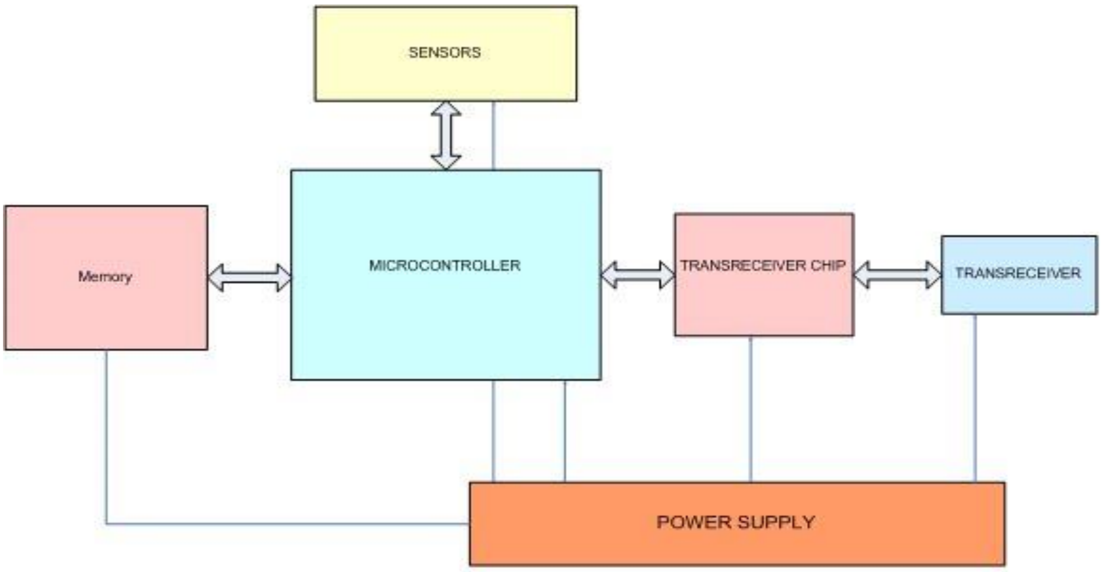

Figure 1.1: Overall Architecture of a Sensor Node

Power Supply: The power supply unit of the sensor node is responsible to provide power to all other components in the sensor node. The power supply can be rechargeable or non-rechargeable in nature, the later one being most common. The supply is generally from 3 to 5 V, in most cases it is DC battery. Having a power source which generates energy by some means (Using Solar energy), so that node is provided power for a longer time is more desirable, however it will be expensive.

Micro controller: It is the CPU of the sensor node. It is responsible for all processing and decision making. Many chip makers have produced micro controller for the purpose of sensor node. Intel is one of the leaders in the production. These are some of the processor that can be used ARM7, Atmel, AVRIntel, Xscale, Intel 8051, PIC, and TI MSP430. Micro controller will be interfaced to the transceiver and sensors.

Sensors: These are responsible to sense the surrounding environment and inform the controller about the phenomenon being observed. There are different sensors available they are Light Sensors, Pressure Sensors, Humidity Sensors, Gas Sensors, Temperature Sensors and many more. These sensors are further divided as active and passive sensors. Instead of sensors actuators also can be used. Sensors sense the physical quantity convert it to electrical signals process the same and obtain digital data and give it to the controller.

Transceiver: Transceivers are responsible to transmit and receive data to and from the communicating media. Communication media in most cases is air. Laser, Infrared and RF based Transceivers can be used according to what is used for communication. RF based communication is most preferred form, as laser and infrared require direct sight of communication. Generally transceivers work in ISM band, which is license free band. Transceivers are interfaced to micro controller using transceiver chip. The most commonly used transceivers chips are CC1000, CC1020, and CC2420.

Memory: Sensor nodes will have programmable Flash memory and RAM in most cases. The flash memory used in MSP430 is 48KB and it has 10KB RAM. So the protocols that are designed for the sensor network should be simple enough to be loaded into the available memory.

Some sensor node may also have Location Finding system such as GPS and mobilizers (which assist the sensor node to move from one place to another if the application requires it).

1.1.2 Application of WSN

Wireless sensor networks have many wide variety of applications. Some of the examples being

- Military Applications: In battlefield sensor network can be used to monitor enemy movements, to monitor various defense equipment to detect biological and chemical attacks and to evaluate damage caused by the war.
- Environmental Applications: Sensor networks can be used, to monitor habitats, to monitor forest fire, to monitor the pollution caused, to monitor weather conditions etc.
- Traffic Surveillance: WSN can be used to monitor traffic on land or water or in air.
- Industrial Applications: WSN can be used to monitor equipment, processes, and conditions inside a factory and also can be used to detect leakage of gas/chemicals etc.
- Home Applications: The applications at home that can be built using WSN range from home automation to intruder detection.
- Health Applications: Another branch called Body Area Networks is carved specifically to concentrate on health applications using senor network.
- Precision Agriculture: Examples for this include monitoring of fertility and humidity in soil using sensor network.

Each wireless sensor network needs to be designed according to the applications for which it will be used. The number of nodes present in the network, the redundancy required, the precision necessary, the periodicity of collection of data all depends on the application to which the sensor network is used. Wireless sensor networks are self-organizing, autonomous, fault tolerant, scalable, long lasting and are able to survive with less energy consumption and are generally low cost.

A typical sensor node in a WSN is made up of, a micro controller such as MSP430FG4618 which is specially designed for low power consumption, a transceiver such as CC2420 which works in ISM band, sufficient memory, power supply and sensors such as temperature sensor, photo sensor, IR sensor.

If we see from software perspective then a sensor node has necessary drivers, a tiny operating system such as TinyOS, MAC layer modules such as 802.15.4 or S-MAC or STEM, Network Layer modules such as Zigbee Specification or LEACH or gossiping or SPIN, Security modules for data confidentiality, authentication, data integrity and Applications such as data aggregation apps, in node processing apps, senor collaboration module.

1.1.3 Energy Usage in Sensor Nodes

Data transmission and reception, and sensing are the prime consumers of power in a sensor node. In other words Transceiver, Controller, Sensors and to some extent the memory are the components that feed on the available energy in a sensor node.

Transceiver is costliest in terms energy usage. A bit transmitted or received is equal to 1500-2700 instructions being executed. Hence it is advisable to put sensor nodes (transceivers) to sleep when not use is. There are three states, sleep state, operational state and idle sate. Operational state consumes the max, idle state being next and sleep state consumes the least. The energy required to change state from sleep to active is considerable, so one has decide on when a sensor node should sleep and when should it be awake.

The energy consumption of each components:

Microcontroller: The MSP430 family features a wider range of operation modes: One fully operational mode, which consumes about 1.2 mW (all power values given at 1 MHz and 3 V). There are four sleep modes in total. The deepest sleep mode, LPM4, only consumes 0.3 μW, but the controller is only woken up by external interrupts in this mode. In the next higher mode, LPM3, a clock is also still running, which can be used for scheduled wake ups, and still consumes only about 6 μW.

Memory: The main consumer in memory is the Flash Memory. Reading, Writing and Erasing flash memory all consume energy. Among them writing consumes the most energy.

Transceiver: Energy is consumed in transceiver during transmission, reception, start up (switch off to switch on). The following example explains the energy consumption pattern. µAMPS -1 consumes 279mW for reception, 151 mW for transmission and 58.7mW for startup.

Sensors: Predicting power consumption of sensors is not easy task, as variety of sensors consume different amount of energy. Passive sensors consume very less energy and the energy consumed by them is negligible compared to other energy consumption however active sensors consume considerable amount of energy.

1.1.4 Save Energy - The Buzz Word in Sensor Network

WSN (Wireless Sensor Network) applications use sensor nodes which are mostly powered using a 3 V battery. Sensor networks are supposed to last at least for six months, hence the available energy needs to be used very prudently. This is similar to usage of available financial sources during recession, every penny needs to be spent after much thought. Lot of research has been done and is being done in the field of optimal usage of energy in sensor networks.

Dynamic Power Management (DPM) specifies five modes of operations for each sensor node. Each mode consumes different amount of power. The mode of operation of sensor node varies from being fully active to deep sleep state. Maximum energy is consumed in fully active state and least is consumed in deep sleep state. A method called as Dynamic Voltage Scaling (DVS) is also proposed, the operating frequency and operating voltage is varied according to the sensor node's mode. The components in sensor node such as transceiver, processor, and sensors are dynamically switched off or put to sleep in different modes. By these dynamic changes in the sensor nodes energy conservation achieved in the sensor nodes.

After DPM let's see how a protocol called "LEACH" to uses energy optimally. **LEACH** is one of the well-known protocol in WSN. In this protocol data aggregation is done at Cluster heads before further forwarding data, this in turn reduces the amount of data being transferred and saves lot of energy, which would be otherwise consumed for transmission and reception of the un-aggregated data. In WSN data transmission or data reception is the most energy consuming activity compared any other activity so data aggregation at various levels helps in conservation of energy. LEACH also saves energy by making all nodes (other than cluster head) go to sleep when they do not having anything to communicate. All nodes are allocated different time slots to communicate by the cluster head hence the nodes are awake only during their time slot. The figure below shows Cluster Heads, normal nodes and Sink in LEACH protocol.

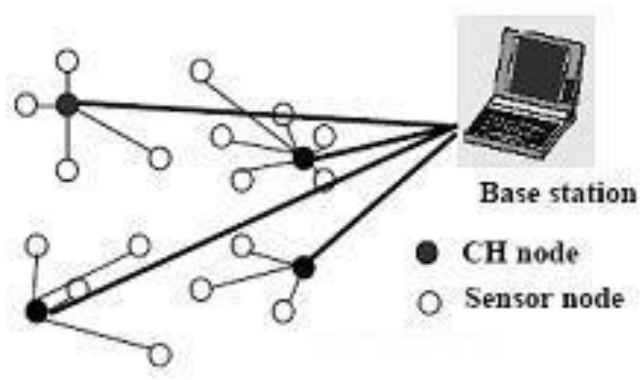

Figure 1.2: Cluster head and normal node in leach protocol

In paper titled "Power Efficient Organization of Wireless Sensor Network" authors try to use only the optimal number of sensor nodes from all available sensor nodes to cover a given area. By this unnecessary sensor nodes are made to sleep and unnecessary redundant data is avoided and also one can rotate between sleeping and active sensor nodes.

In paper titled "Power efficient Topologies for Wireless Sensor Networks" authors propose a method to find a sensor network topology which consumes least power to cover given area, in other words the sensor nodes are placed such that they cover the given area by utilizing minimum number of sensor nodes.

1.1.5 Design Issues in WSN

Wireless sensor networks are made of large number of tiny sensor nodes, which have limited power and less processing capability. The life time of the individual sensor node is not easily predictable and also the network needs to be formed autonomously as it is not possible to manually set up the sensor network for all applications. The sensor network also consists of several different kind of nodes hence heterogeneity needs to be supported. The number of sensor nodes in the network is not constant throughout the life time of the network it may vary because of addition of senor nodes or reduction of nodes due to their death. The major factors that need to consider while designing sensor network are listed below.

- **Fault Tolerance:** Possibility of node failure and change of topology of network is quite high in case of WSN. Hence the designer of network should make the network robust and reliable even in case of node failures and topology changes. The network should function smoothly and normally irrespective of node failures and topology changes.
- **Life Time:** WSN are supposed to work for a quite long time with low power consumption. They are supposed to last at-least for 6 months to 1 year. We need to keep in mind that every node in WSN may be powered using just a 3 V battery and this should be sufficient for the entire life time of the node. The design of protocols of WSN should be such that the node consumes as less energy as possible. This will help in making the WSN last longer.
- **Scalability:** The design of WSN should support addition of new nodes any time and also the design should support large number of nodes because some applications in WSN may require quite a huge number of sensor nodes.
- **Data Aggregation:** The sensor nodes in WSN are located close to each other hence the possibility of similar data being generated by the nodes next to each other is quite high. So the data needs to be aggregated and the duplicate data needs to be avoided because the transmission and reception data is the most costly affair in WSN. The data needs to be aggregated at different levels in WSN so that only the necessary data is transmitted and received and the redundant data is not communicated.
- **Cost:** The cost of each sensor node is supposed to be 1$, as WSN can have large number of sensor nodes the total cost of the network can become a quite expensive affair. So the designer of WSN needs to decide on the optimal number of nodes necessary for the application.
- **Environment:** The environment in which the WSN is deployed can be very demanding, so the design of WSN should be such that WSN should be able to survive regardless of the conditions in which WSN s deployed.
- **Heterogeneity Support:** The protocols designed for WSN should support different kinds of sensor nodes and also be able to support variety of applications.
- **Autonomous Operations:** The WSN should be able to organize, reorganize and operate autonomously because sometimes WSN deployed in places where human habitation is not possible.

- **Limited Memory and Processing Capability:** The sensor nodes have very limited memory, power and processing capabilities, so all designs of WSN should not be demanding in terms of processing requirements or memory requirements.

1.1.6 Routing in WSN:

Most of the data in the sensor network will be directed towards the sink. Special multi hop routing protocols are needed between sink and sensor nodes for wireless sensor networks. Most of the data conveyed to the sink form a sensor node will pass through many intermediate nodes before reaching the sink. Communicating data directly from the node to sink will be very energy expensive, so multi hop communication is preferred in wireless sensor network. The figure below makes the concept clearer.

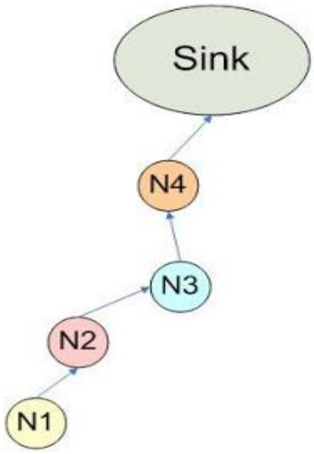

Figure 1.3: Data form node N1 reaches sink through multiple intermediate nodes, N2, N3, and N4.

The network layer for sensor network is designed considering the following

1. Every protocol designed should be power efficient.

2. The protocol should support dynamic nature of sensor networks.

3. The sensor network protocols should make sensor network self-configurable.

4. Data aggregation should be done, if it is advantageous.

5. Data centric design is more preferred, rather than address centric or location centric architecture.

There are several protocols and papers written regarding different issues in network layer for sensor networks, we shall understand a few in the proceeding sections.

A route form source to destination can be found based on many different criteria.

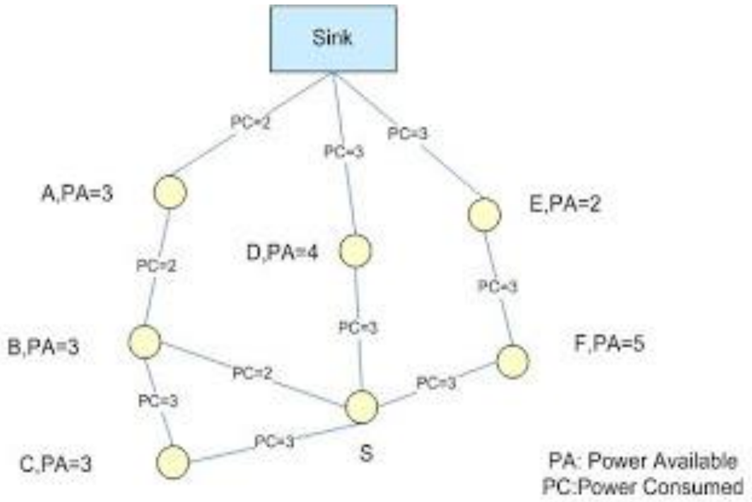

Figure 1.4: A routing scenario

A scenario to explain different criteria that can be used to select a route form source (S) to Sink.

One may choose a route which has maximum available power; in that case the route form source (S) to sink in the above diagram will be S-C-B-A- Sink. This is so because the power available in this route is 9, which is the highest compared to other routes.

One may go for route which consumes least power, and then the route selected can be S-B-A-Sink or S-D-Sink. S-D-Sink is preferred because less number of hops is present.

If the criterion to select is minimum number of hops then, the route S-D-Sink is selected.

There may other criteria that can be used, like a route with less probability of failure, a route less congested.

The routing may also be data centric routing. In this type of routing sink advertises the interest, and all nodes which have the data reply back to sink. Or it may be that all nodes advertise what kind of data they have, and other nodes which require that data request the node to give the data. In this type of routing, there is no importance given to a particular node but importance is given to the data or attribute. This type routing differs from the conventional routing schemes. Many papers and authors prefer data centric routing than conventional routing for sensor networks.

Data aggregation is done in sensor network to reduce the redundant data and hence save energy. For example in the figure shown before data from S and C is aggregated at node B, if the data form both C and S are almost similar. This reduces the amount data sent form B to A, hence conserves energy at B. Similarly data form A, D, E is aggregated at sink and sent further by sink, if the data has to be sent further. Data aggregation introduces delay in forwarding the data, as the node which aggregates the data has to wait for data from all nodes, to which the node aggregates the data. Even the process of aggregation consumes some amount of time.

1.1.7 Some routing protocols used in WSN

SPIN stands for Sensor Protocol for Information via Negotiation. There is family of protocols called as SPIN; they come in different flavors and features. These protocols are designed to address the deficiency of flooding and gossiping.

SPIN uses three types of messages, ADV, REQ and DATA. The ADV message is broadcasted by a node which has some data. This message is broadcasted by the node. This message will say about type of data contained by the advertising node. Interested nodes which got the ADV message send REQ message requesting for the data. The node having the data sends the data to the interested nodes. The nodes after receiving data send ADV message, and the process continues. This can be seen in figure below.

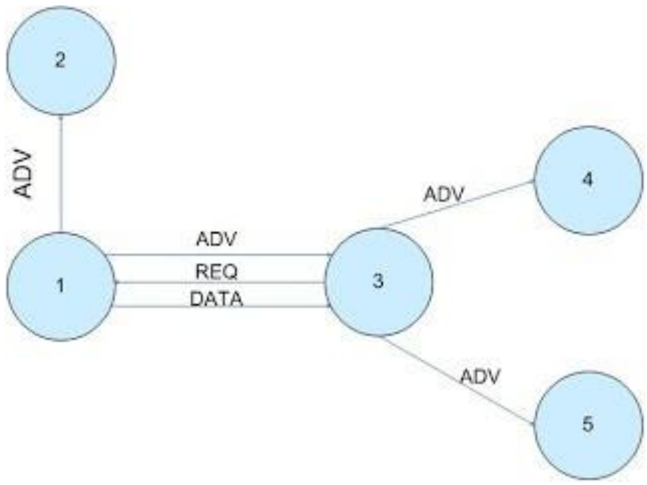

Figure 1.5: SPIN protocol

Node 1 sends ADV message to all its neighbors, 2 and 3.Node 3 requests for the data using REQ message, for which node 1 send data using message DATA to node 3. After receiving the data Node 3 sends ADV message to its neighbors 4 and 5 and the process continues. It does not send to 1 because 3 knows that it received data from 1.

The data is described in the ADV packet using high level data descriptors, which are good enough to identify the data. These high level data descriptors are called meta-data. The meta-data of two different data's should be different and meta-data of two similar data should be similar. The use of meta-data prevents, the actual data being flooded throughout the network. The actual data can be given to only the nodes which need the data. This protocol also makes nodes more intelligent, every node will have a resource manager, which will inform each node about the amount various resources left in the node. Accordingly the node can make a decision regarding, whether it can as forwarding node or not.

Gossiping is similar to flooding except that, a node receiving a packet, instead of broadcasting, the node sends it to only one of its randomly selected neighbor, and the neighbor in turn sends the packet to one of its randomly selected neighbor, this continues until the packet reaches its destination. Gossiping reduces the number of packets in the network but the delay to reach destination in some cases may be very large. The diagram below shows gossiping.

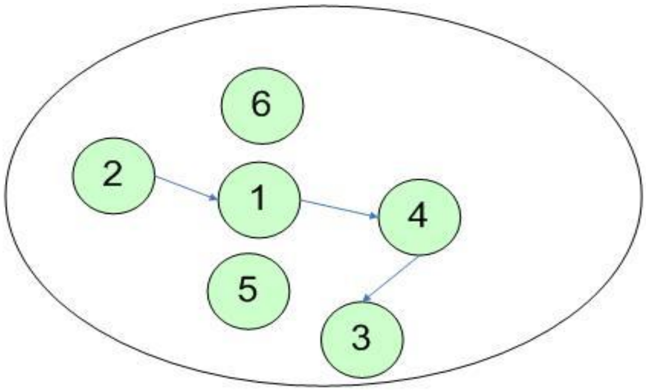

Figure 1.6: Gossiping in WSN

Node 2 randomly selects node 1 among its neighbor to forward the packet, similarly node 1 selects node 4 among its neighbors, 2, 6, 5 and 4. Node 4 forwards the packet to 3.

Flooding can be used for routing wireless sensor networks. In flooding, a node sends a packet received, to all its neighbors other than the neighbor which sent the packet to it, if the packet is not destined to itself or the maximum number of hops a packet can pass is not crossed. Flooding is very simple to implement, and it is reactive protocol, as it does not maintain any routing table (topology maintenance) and does not require discovering any routes. But this technique has several disadvantages, the most important being, it is responsible for large bandwidth consumption and it wastes valuable energy. This is not an energy aware protocol also. This protocol is not designed specifically for sensor networks. Similar data produced by nodes in the same region are also flooded, i.e. there is no data aggregation done. The diagram below gives an example for flooding.

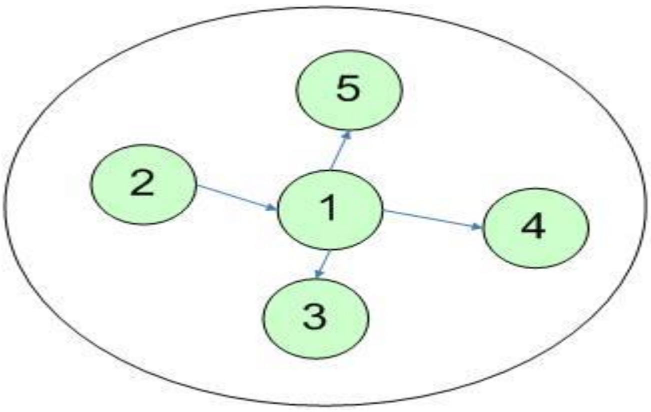

Figure 1.7: Flooding

Node 2 sends a packet to node 1, which in turn sends the packet to all its neighbors, i.e. to node 3, node 4, and node 5. Node 1 does not send the packet to node 1 because node 1 knows that node 2 only sent the data to it.

Chapter 2

Literature Review

2.1 Introduction

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions [11]. More precisely, a group of sensor nodes joins inside a network and collectively perform their task by transmitting real time data from one node to another and processing the data to create a meta-data from it, is called wireless sensor network. WSN is a new edition in wireless networking paradigm. It is completely different from the ad hoc networking architecture. So architecture, protocols etc. followed in ad hoc networking is not applicable here. In ad hoc network there is no energy constraints, number of nodes are few, not densely populated and nodes are not prone to failure. All these features are available in WSN. So application designer has to think differently to create an effective architecture, topology, protocols etc.

Wireless sensor network is being employed in almost every application sector. Every application is unique from one another. For example, in case of home automation system we can think that the channel will be less noisy than that of battlefield. In health care application we need throughput of data more than energy efficiency. Actually we cannot use same mechanism for all the application areas. This concept has led the idea of application specific protocol. This kind of protocols are only applicable for a certain application field and cannot be used in any other areas. Some developers like [12] has proposed this types of protocols for WSN which define the network architecture, routing protocols, routing metric selection etc. of a specific application scenario. Many routing protocols are also proposed in this context like [13].

A routing protocol is a set of rules used by routers to determine the most appropriate paths into which they should forward packets towards their intended destinations [13]. Routing is a very important term in Wireless sensor network. Because in ad hoc network the channel is more reliable than that of wireless sensor network. The nodes are having energy constraint. So we cannot use the same node for transmitting data for a long time. The route is to be changed after a period of time. These scenarios have led the necessity of new kinds of routing protocols for wireless sensor network. As different application has different scenarios, the routing protocol for them should be application specific.

In this paper we proposed an application specific routing protocol for health-care application. The main focus we have given on this paper is the lifetime of the network and the reliability. We have already discussed that wireless sensor network has energy constrains. If we consider the health care application scenario, we can say that, only energy efficiency doesn't reach the goal of the application. Here we need almost every data. As every data is necessary, we have to achieve maximum throughput in our system. For this purpose, in considering routing metrics for calculating routing path we consider expected Transmission count (ETX) along with residual energy. ETX helps to minimize the number of packet delivery in a wireless network [5]. So the channel can be less congested and chance of packet drop can be decreased. By measuring ETX of a path, we can also determine the reliability of the path that can help to select the most reliable path for packet delivery. We also proposed a definite architecture for the health-care application. Many routing protocols like RPL [6, 7], CTP [8], TEEN [13] etc. are proposed in this context. Our main goal is to create an energy efficient and reliable routing protocol for health-care application.

In the section 2 we discussed related work and section 3 our proposed architecture. In section 4 the routing protocol is defined and section 5 focuses on the routing metrics. In section 6 we have shown our routing algorithm. In the section 7 we concluded our work. In section 8 references are provided.

2.2 Related Works

Routing protocol is a set of rules used by the routers (in WSN nodes) to determine the most appropriate path to which can be used to send the data packet [16]. In WSN, selection of an appropriate routing protocol is very crucial. Here we not only think about the channel quality to send the data packet, but also consider the energy level of the node and network lifetime. WSN uses broadcast paradigm to send a data packet and have less computational power [1]. So the researcher needs to consider these scenarios to develop a routing protocol.

Many routing protocols are developed in this context. In the early stages gossiping and flooding [17], SPIN [18] etc. were proposed. Due to many deficiencies, they were further developed to create more effective protocol. Low-Energy Adaptive Clustering Hierarchy (LEACH) [19] is also a famous routing protocol that uses hierarchical mechanism to disseminate data packet. All these protocols were developed considering the overall WSN scenario, not based on the application demand.

To ensure the reliability, robustness and efficiency in selecting the routing path Connection Tree Protocol (CTP) [8] is proposed. Unlike other routing protocol, this protocol focuses more on the path reliability than the energy constraints. This protocol uses Expected Transmission Count (ETX) as a routing metric to select the routing path. ETX is defined as the expected number of transmission to send a data packet [5]. CTP decreases the number of transmission in a WSN network by avoiding the less reliable routes. But in some application field where reliability is not necessary, CTP cannot be used in those cases.

One of the most popular protocol that is prevalent now is Routing Protocol for Low-power and Lossy Network (RPL) [6,7] proposed by Internet Engineering Task Force(IETF) ROLL. It is actually a distance vector routing protocol [6]. The main focus of this protocol was to eliminate creation of loop inside the network. This protocol is good enough for point to multipoint (P2MP) and multipoint to point (MP2P) communication, but was not good enough to support point to point traffic well [15]. RPL has a mechanism to adapt to any kind of application using appropriate routing metrics for that application. But RPL was not proposed based on any kind of application. So it does not reflect the application scenario.

Chapter 3

Proposed Architecture

3.1 Introduction

Architecture is from the Latin word architectura, which is formed from the words for architect. In information technology, especially computers and more recently networks, architecture is a term applied to both the process and the outcome of thinking out and specifying the overall structure, logical components, and the logical interrelationships of a computer, its operating system, a network, or other conception. An architecture can be a reference model, such as the Open Systems Interconnection (OSI) reference model, intended as a model for specific product architectures or it can be a specific product architecture, such as that for an Intel Pentium microprocessor or for IBM's OS/390 operating system.

In Wireless Sensor Network, Architecture is a very important term. Every application designer has to think of the limitation of this kind of network which makes life tough. The architecture in WSN application must fulfill the application demand. So in our proposed routing protocol we also proposed our own architectural model.

3.2 Architecture

6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. .6LoWPAN technology is rapidly gaining popularity for its extensive applicability, ranging from healthcare to environmental monitoring. In order to provide more reliable and effective IPv6 connectivity on top of LoWPAN, the 6LoWPAN WG (Working Group) has defined some key technologies. [9]. In general, 6LoWPAN supports the use of biomedical sensors and are characterized by its [1] very low transmit power to coexist with other medical equipment and provide efficient energy consumption, [2] high data rate to allow applications with high QoS constraints, [3] low cost, low complexity and miniature size to allow real feasibility.

Our proposed architecture divide the total health care system into two tiers. In the system proposed in [4], they divided this architecture in three tiers. Fig 1 shows the overall architecture of our system. But in our architecture we are using 6LowPAN technology in human body which is delimitating the redundancy of using extra layer. Our proposed first tier involves the user or patient and second tier involves Global network between the user and the Hospital.

3.3 First tier

The main purpose of this tier is to collecting the health information from the user/patient body. The sensor node deployed inside the patient's body will periodically disseminate data. The smart phone or smart device will store the data in the local storage. There will be an application that will help the user to be updated with his/her health data. The patient can also contact with the doctor for any convenient advice.

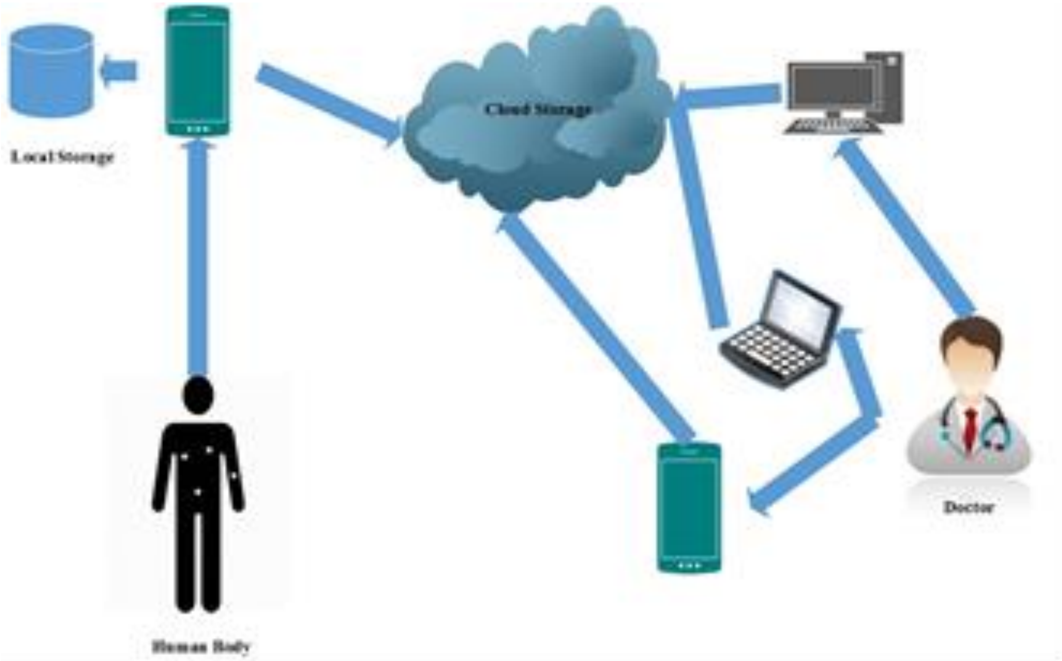

Figure 3.1: Proposed Architecture

3.4 Second tier

The second tier indicates the global connectivity of the hospital and the patient. The smart phone or smart devices in the patient side will store the health condition data in the cloud storage. In our system everyday huge amount of data should be handled. Using GSM network to handle this huge amount of data should be a huge disadvantage. So we proposed cloud storage for this purpose. The hospital can monitor the data of the patient from the cloud storage. The doctors can also monitor the patient data from his smart phone.

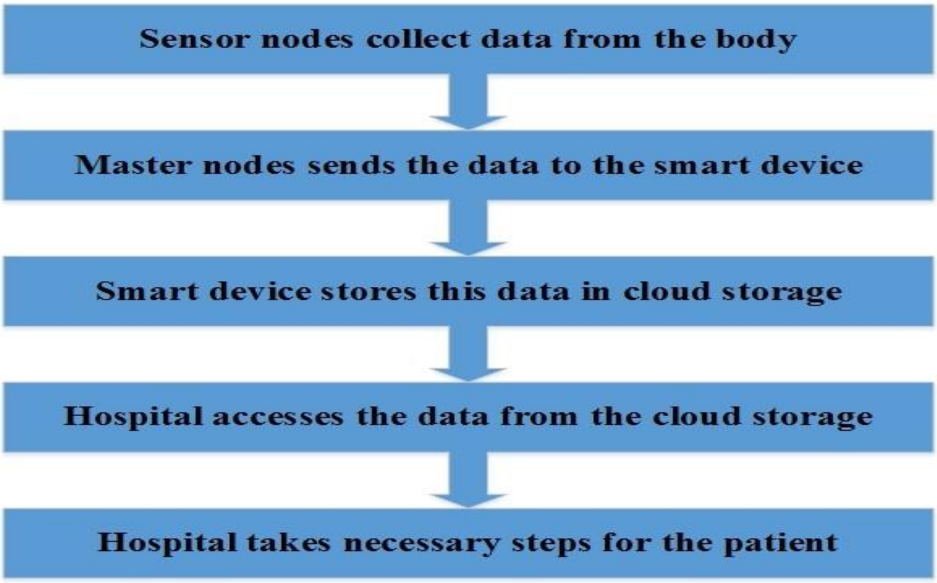

Figure 3.2: Data Flow Diagram

Chapter 4

Routing Protocol

4.1 Introduction:

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

Routing in very important term in Wireless sensor network. The nodes are having energy constraints and other difficulties. So without efficient routing it is not possible to overcome these situations. In our proposed routing protocol we think both of reliability and energy constraints.

4.2 Routing Protocol

Routing has been considered as one of the key issues in 6LoWPAN networks that are worth investigation [10]. Most of the attention, however, has been given to the routing protocols since they might differ depending on the application and network architecture [2]. A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. To support effective communications, the design of a routing protocol must be based on the characteristics of its target network and applications. For example, the mobility of nodes in ad-hoc networks demands routing protocols that can converge rapidly and maintain connectivity in an efficient manner, the severe energy constraints of WSNs demand the design of energy-efficient routing protocols and heavy traffic load in mesh networks requires load-balancing routing schemes.

In the routing protocol we have proposed, the body has been divided into several areas. The sensor node will be deployed in all areas. Every area will have a border node (Figure 2). The sole responsibility of the border node is to send the data packet to the master node (smart-phone). But if a single node is assigned as a master node for all the time it would deplete its energy at a great level which may cause to the failure in very early time. So the border node will not be selected statically. Rather at a period of time the border node will be changed.

Border node can be selected on the basis of the remaining energy of the node. When handing over the duty of border node, the node having the highest remaining energy will be assigned

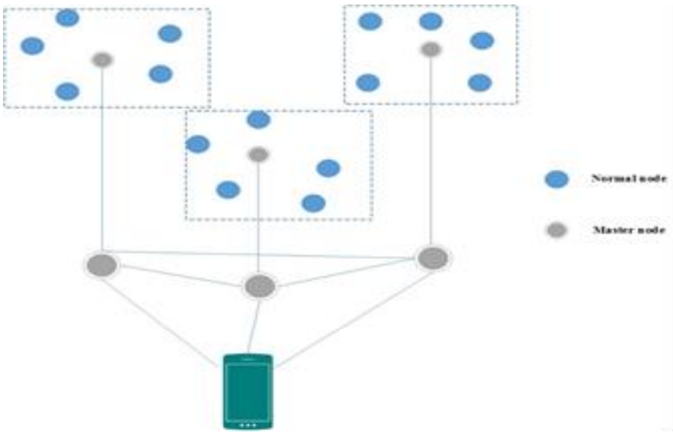

Figure 4.1: Routing Protocol

as the border node. Then every node will calculate the optimal path from itself to the border node. Whatever data the node perceive it will send the data to the border node.

Two kind of message will be generated in our routing scenario. One is periodic message and another is triggered message. The periodic message will be generated at a definite period of time for example 10 minute. In periodic message along with data the remaining energy of the node and the transmission count information will be also be sent.

4.3 Routing Metrics

To meet the application's requirements while respecting the characteristics and limitations of the WSN, appropriate routing metrics have to be adopted by the routing protocol (3). WSNs imposes different Quality of Service requirements on the underlying network with respect to delay, reliability and loss. At the same time, WSNs present intricacies such as limited energy, node and network resources. To meet the application's requirements while respecting the characteristics and limitations of the WSN, appropriate routing metrics have to be adopted by the routing protocol. These metrics can be primary (e.g. expected transmission count) to achieve a specific goal or composite (e.g. combining latency with remaining energy) to satisfy different applications needs and WSNs requirements (e.g. low latency and energy consumption at the same time).

We are using composite routing metrics. Primary routing metric is remaining energy (RE) and Secondary routing metric is Expected Transmission Count (ETX).

In energy-aware routing, the routing decisions depend on considerations of the available energy of the nodes. In sensor network we have think of the energy constraint at the starting of any architecture. If the initial energy level of any node i is and the current energy level is then (3)

$$RE^{i} = \frac{V^{i}_{\max}}{V^{i}_{now}} \geq 1 \ldots\ldots\ldots\ldots\ldots \textit{(1)}$$

ETX or Expected Transmission Count (ETX) detects the reliability of the link. The ETX of a link is the predicted number of data transmissions required to send a packet over that link, including retransmissions. The ETX of a link is calculated using the forward and reverse delivery ratios of the link. At the very first time probe packets will be sent throughout the network to determine the path loss ratio. Forward path ratio can be calculated by dividing the no. of packet sent and the no. of acknowledgement found. In the similar manner we can determine the reverse forward ratio of the same link. If for any node *i* it sends packet to node *j* the forward path ratio is df and the reverse forward ratio is dr. Then we can say (5):

$$ETX = \frac{1}{d_f \times d_r} \ldots\ldots\ldots\ldots\ldots \text{(2)}$$

The delivery ratio can be determined using the following formula (5):

$$r(t) = \frac{count(t-\omega, t)}{\omega/\tau} \ldots\ldots\ldots\ldots \text{(3)}$$

Count (t − w, t) is the number of probes received during the window *w*, and *w/τ* is the number of probes that should have been received. In the case of the link *i→ j*, this technique allows X to measure *dr*, and Y to measure *df*. Because Y knows it should receive a probe from X every *τ* seconds, Y can correctly calculate the current loss ratio even if no probes arrive from X.

As we are combining these two routing metrics, the weight of them should be taken into important account. In our proposed protocol this value can be static or dynamic. For static, the value of the weights will remain same all the time. But in dynamic case this value will vary according to the type of the message. For example, if the message is triggered message it will emphasis more on the ETX than residual energy. For any path a from node X to Y (3),

$$w(a) = w_1 * R.E + w_2 * (ETX)^{-1} \ldots\ldots\ldots \text{(4)}$$

w(a) is the weight of the path and w_1, w_2 are two constants which determine the weight of the metrics used in this scenario. Value of the weight can be dynamic or static. In dynamic case this value will be determined based on the importance of the message. In static case, this value will be provided at the early stage of the setup phase.

4.4 Routing Algorithm

1) *//initialize w1,w2*
2) *check (w1+w2=1)*
3) *for all nodes v*
4) *fpr= check_FPR (u, v)*
5) *Bpr= check_BPR (u, v)*
6) *ETX (u , v) =1/(fpr*Bpr)*
7) *V_max(u)=check_initial_energy_level()*
8) *V_now (u)=check_current_energy_level ()*
9) *RE(u)=V_max/V_now*
10) *w (u, v)=w1*RE(u)+w2*(1/ETX(u , v))*

Chapter 5

Performance Evaluation

5.1 Introduction

Performance evaluation is necessary in any system. This process gives the idea of how the proposed system cope up with the current scenarios. It also gives the comparison between existing systems and the proposed one. Performance evaluation can lead the improvement of the system by identifying the problem areas and solving them. In terms of Wireless sensor network performance evaluation is very important.

We have also gone through this section carefully. Our main focus was to compare with the most prominent routing protocol called RPL.

5.2 Theoretical Evaluation

Our proposed protocol is different from RPL in many senses. RPL is developing a well-defined routing protocol for all WSN application. But it not application specific. Routing metrics is on application demand. It also ensures reliability based in application.

CTP developed a reliable routing protocol for WSN. It is not application specific. Routing metrics that is used here is called ETX. ETX is used to ensure the reliability of the network. In some case ETX can deal with energy constraints by delaminating unnecessary packet flow in sensor network.

In our routing protocol we developed an energy aware and reliable routing protocol for health care application. It is application specific unlike RPL and CTP. It can ensure reliability as we used ETX as a secondary routing metrics. Unlike other routing protocols we also provided with an architectural diagram for the application purpose.

In the table we have shown the differences between our proposed protocol and the existing ones.

Factors	RPL	CTP	Proposed
1. Target	1. Developing a well-defined routing protocol for all WSN application.	1. Developing a reliable routing protocol for WSN application.	1. Developing a energy efficient and reliable routing protocol for Health-care application.
2. Application specific	2. No.	2. No.	2. Yes.
3. Routing metrics	3. Based on the application demand	3. ETX	3. Composite(Residual Energy and ETX)
4. Reliability	4. Can ensure based in application demand	4. Can ensure.	4. Can ensure.
5.Tree based	5. Yes	5. Yes	5. No

Table 5.1 Theoretical comparison

5.3 Performance Evaluation

We compare RPL and CTP when each member of a 50-node generates a packet every 5 and 10 seconds. The results are the average of two 24- hour runs for each network configuration. The PRR and routing control packet overhead of RPL is comparable with that of CTP.

Protocol	RPL		CTP	
Packet Interval	5 sec	10 sec	5 sec	10 sec
PRR	99.88%	99.96%	99.94%	99.99%
Control Traffic	8.96	9.01	8.29	8.02

Figure 5.1: Packet reception ratio (PRR) and the average number of routing control packets generated at each node per hour with varying traffic rates.

The results indicate that RPL and CTP both select links with very good quality and also that the path that CTP selects are slightly more efficient than the path that RPL selects.

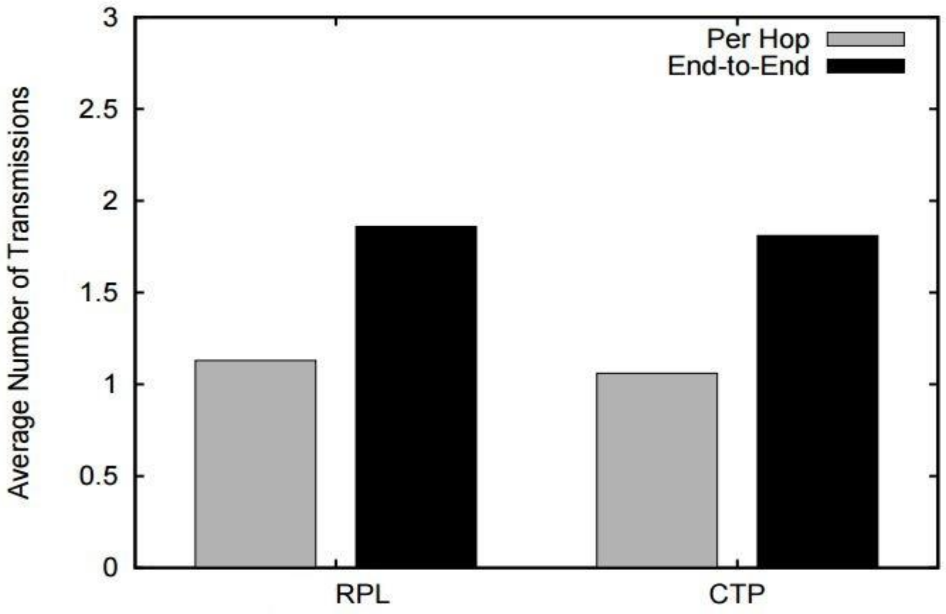

Figure 5.2: Average number of packet transmissions required at each hop (gray bars) and over the entire end-to-end path (black bars) for RPL and CTP.

The power consumption represents the average energy consumed of each node in the network. Fig. 5.3 shows the average power consumption for different network sizes. A straightforward observation is that the power consumption increases with the number of nodes, which is expected. We also observe that the multiple broadcast domain consumes more power in the network than the single broadcast domain does. However, the gap becomes smaller as the number of nodes increases and the average consumed energy converges towards 2 mW for both scenarios. This demonstrates that the number of nodes represents the major factor of energy dissipation.

Figure 5.4 shows that the packet loss ratio for 1 and 2 hops is relatively low (between 1% and 4%). However, this ratio significantly increases with greater hop counts reaching 20% for 4 hops. This is due to the following reasons: (i) packet losses have a cumulative effect when the number of hops increases, due to increasing chances for a packet to get lost from one hop to another, (ii) link quality fluctuations of low-power and lossy links, which results in temporary losses of connectivity. This was the case of large hop counts in our experiment. These results raise questions about the effectiveness of the default Objective Function relying on the ETX metric to select routes. So, combined routing metric is much better solution.

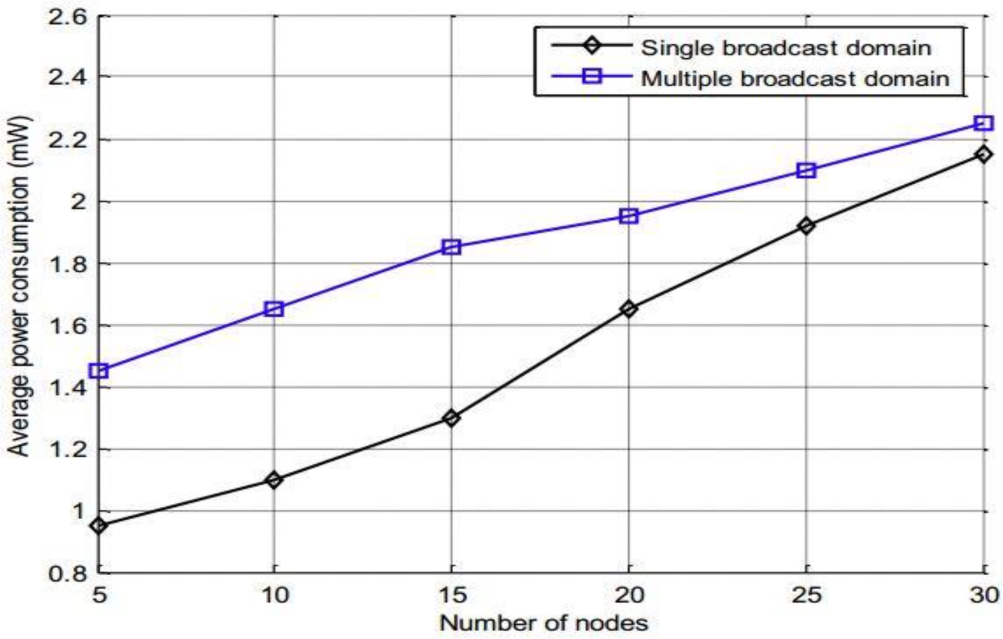

Figure 5.3: Average power consumption

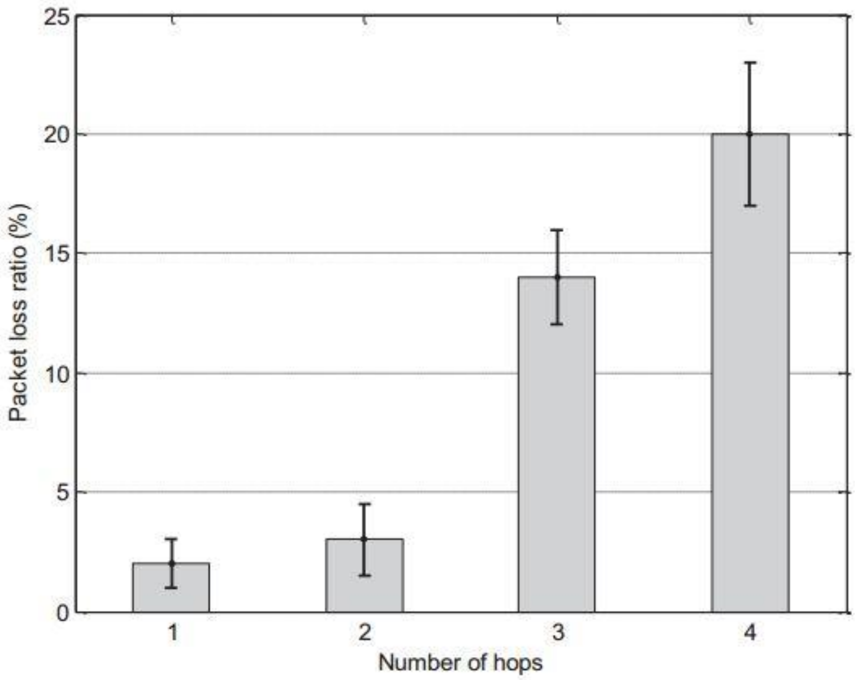

Figure 5.4: Packet Loss Ratio for different hops.

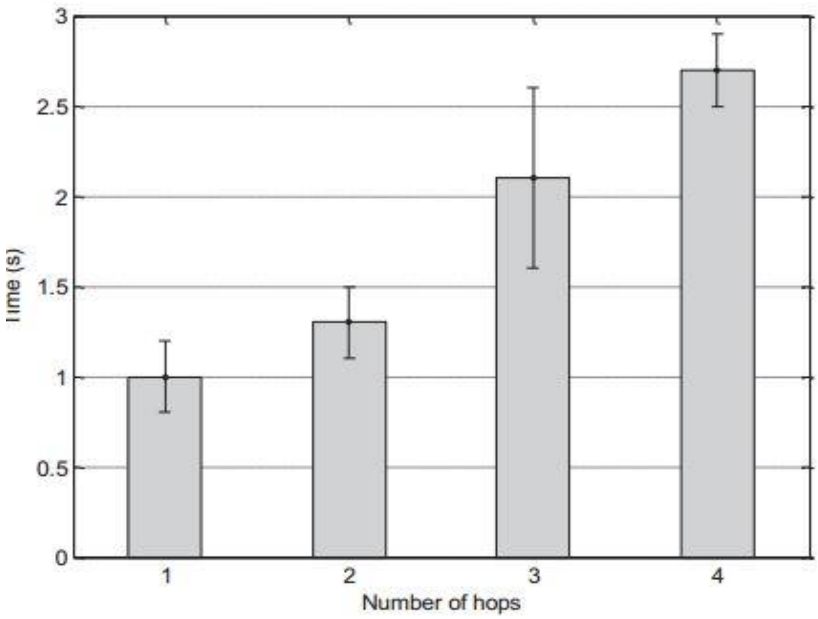

Figure 5.5: Packet delay for different hop count.

We evaluated the end-to-end delays to understand its timeliness behavior. The packet delay is defined as the duration between the transmission time of the Ping Request message and the reception time of the Ping Reply message. Fig. 5.5 shows the measured packet delays for different hop counts between the source and destination with a confidence interval of 90%. Fig. 5.5 shows that the packet delay increases almost linearly with the number of hops between the source and destination. It varies from 1 s for single hop distant motes to 2.7 s for motes that are 4 hops away. The measured packet delays represent an acceptable real-time performance considering the low-power and resource limitation nature of sensor nodes. Lower delays can be observed with better links and lower packet loss ratios. However, it is needed to further improve the timeliness performance of lossy networks through the adoption of more sophisticated QoS mechanisms to optimize the route selection process and reduce end-to-end delays.

We have simulated our proposed protocol with two other protocol RPL and CTP. Each node simulated in SpeckSim has the following characteristics: Battery: capacity - 1mAh, voltage-3V; MCU: active current - 0.005mA, sleep current -0.001mA, off current - 0mA and Power up delay: Min=0s, Max=1s. We now present the results that have been gathered by running the application in SpeckSim, for the different routing protocols. The results presented are the average of six runs.

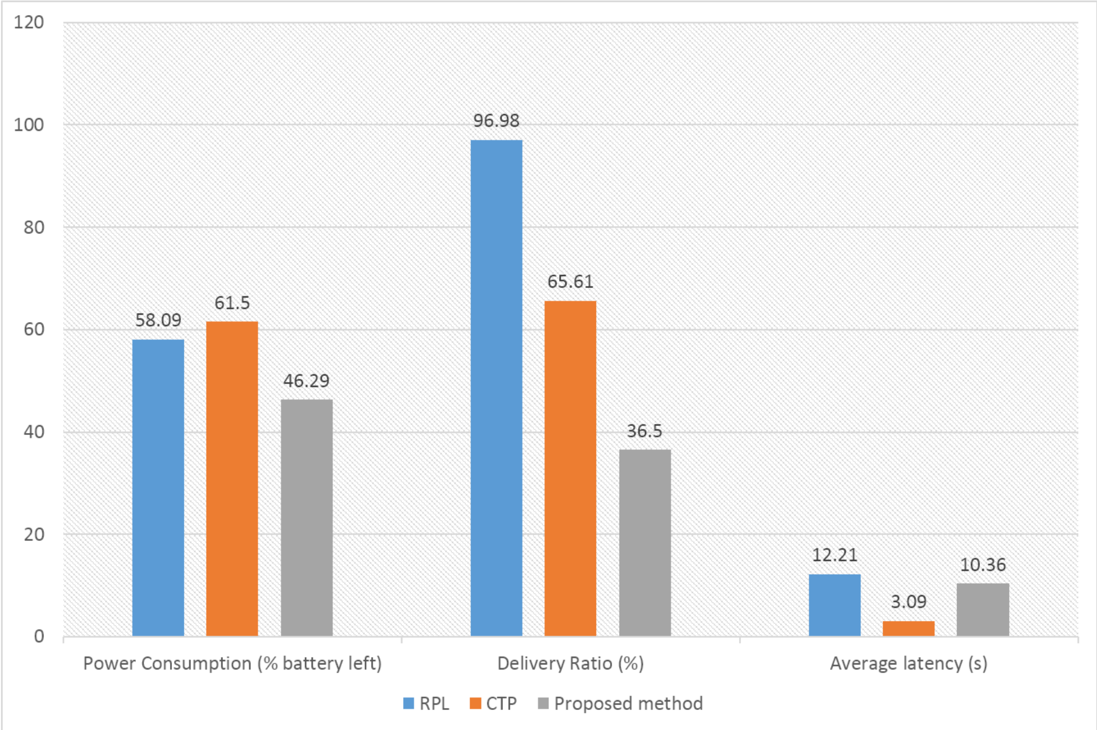

Figure 5.6: Comparison of RPL, CTP and our proposed method.

Single routing metrics vs Composite routing metrics

The composite metric is supposed to be a linear blend of many different factors that might influence routing within a domain. As we are consider both ETX and Residual Energy both as a routing metric so we can guarantee two things here ETX ensures the path which is more reliable and residual energy ensures the efficient path by which more energy will be consumed. Thus our proposed routing metric ensures a routing path which will be very effective for tiny energy constrained devices like body sensors.

6. Conclusion and Future Work

Wireless sensor network is getting popular day by day. Its mobility and capability of real time communication has led many application use this technology. Many developers and researchers are providing their support to enhance this sector. Many new protocols, architectures are being proposed in this purpose.

Among many application areas, Health-care application is very important. These types of application deals with the life of the people. So necessary actions should been taken to make it more reliable. It is been found that, a lot of patient dies due to failure in this application areas. So careful development is needed here. The most important factor needed here is early detection of the disease. The most fatal disease like cancer can even be cured if it is detected at early stage.

Using WSN technology in health-care application can create a new era in patient caring system. The status of the patient can be known very easily and can be provided with proper care at proper time. Many fatal diseases can be figured out at early stages. Doctor can easily monitor his/her patients and provide necessary advices.

The routing protocol we proposed can enhance the performance in a good proportion. In the future, we are going to implement the packet format, evaluation scheme with existing routing protocol, enhance the protocol to make it well suited with the existing scenario.

7. References

[1] I.F. Akyildiz, W. Su , Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey"- Computer Networks: The International Journal of Computer and Telecommunications Networking archive Volume 38 Issue 4, 15 March 2002

[2] Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks" - Ad Hoc Networks Volume 3, Issue 3, May 2005

[3] Panagiotis Karkazis, Panagiotis Trakadas, Helen C. Leligou, Lambros Sarakis, Ioannis Papaefstathiou & Theodore Zahariadis, "Evaluating routing metric composition approaches for QoS differentiation in low power and lossy networks "- Wireless Networks August 2013, Volume 19, Issue 6, pp. 1269-1284

[4] Jamila Ben Sliman, Ye- Qiong Song, Anis Koubˆaa, Mounir Frikha. A Three-Tiered Architecture for Large-Scale Wireless Hospital Sensor Networks. Workshop MobiHealthInf 2009 in conjunction with BIOSTEC 2009, January 2009

[5] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, Robert Morris , "Wireless Networks - Special issue: Selected papers from ACM MobiCom 2003 archive Volume 11 Issue 4, July 2005 Pages 419-434 ", July 1993.

[6] Tsvetko Tsvetkov, "RPL: IPv6 Routing Protocol for Low Power and Lossy Networks" Seminar SN SS2011, Network Architectures and Services, July 2011

[7] T. Winter, Ed et. al , "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" - Internet Engineering Task Force (IETF), Request for Comments: 6550,Category: Standards Track, ISSN: 2070-1721

[8] Rodrigo Fonseca, Omprakash Gnawali, Kyle Jamieson, Sukun Kim, Philip Levis, and Alec Woo," The Collection Tree Protocol (CTP)". TinyOS Developer List tinyos-devel at 2009-01-16

[9] Dr.H S Ramesh Babu,Urmila Dey, "Routing Protocols in IPv6 enabled LoWPAN: A Survey," International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014, ISSN 2250-3153

[10] Olfa Gaddour, Anis Koubâa, "RPL in a nutshell: A$survey", CISTER-TR-130203 Date: 02-14-2013

[11] http://www.ni.com/white-paper/7142/en/ PhD. Emilian Necula. Faculty "Dynamic traffic flow prediction based on GPS Data"- 2014 IEEE 26th International Conference on Tools with Artificial Intelligence, ACM SIGCOMM 1989 Symposium, September 1989.

[12] HEINZELMAN et al.: "AN APPLICATION-SPECIFIC PROTOCOL ARCHITECTURE FOR WIRELESS MICROSENSOR NETWORKS Yaqin Wang and Yue Chen", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 1, NO. 4, OCTOBER 2002

[13] Arati Manjeshwar and Dharma P. Agrawal, “TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks”, 0-7695-0990-8/01/$10.00 (C) 2001 IEEE

[14] S. Hedetniemi and A. Liestman, “A survey of gossiping and broadcasting in communication networks,” Networks, Vol. 18, No. 4, pp. 319-349, 1988.

[15] W. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive protocols for information dissemination in wireless sensor networks,” in the Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’99), Seattle, WA, August 1999.

[16] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," in theProceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.