TRUST BASED ENERGY-EFFICIENT AND SECURED PROBABILISTIC ROUTING ALGORITHM FOR IoT

B.Tech. Final Year Project Report

BY

Subhajit Mahata

Ankur Barick

Saikat Pal

Bikramjit Dutta

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
RAMKRISHNA MAHATO GOVERNMENT ENGINEERING COLLEGE
AGHARPUR, RAMAMOTI, JOYPUR, PURULIA- 723103, WB (INDIA)

JULY, 2020

TRUST BASED ENERGY EFFICIENT PROBABILISTIC ROUTING ALGORITHM FOR IoT

A Major Project Report

submitted in partial fulfillment of the requirements for the award of the degree

of

Bachelor of Technology

in

COMPUTER SCIENCE AND ENGINEERING

BY

Subhajit Mahata	**35000116007**	**CSE (4th Year)**
Ankur Barick	**35000116050**	**CSE (4th Year)**
Saikat Pal	**35000116023**	**CSE (4th Year)**
Bikramjit Dutta	**35000116044**	**CSE (4th Year)**

Under the Supervision of

Dr. Abdur Rahaman Sardar

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

RAMKRISHNA MAHATO GOVERNMENT ENGINEERING COLLEGE

AGHARPUR, RAMAMOTI, JOYPUR, PURULIA- 723103, WB (INDIA)

JULY, 2020

CERTIFICATE OF ORIGINALITY

I hereby certify that the work which is being presented in the B.Tech. Final Year Project Report entitled **"Trust Based Energy Efficient and Secured Probabilistic Routing Algorithm for IoT",** in partial fulfillment of the requirements for the award of the **Bachelor of Technology in Computer Science & Engineering** and submitted to the Department of Computer Science & Engineering of Ramkrishna Mahato Government Engineering College, Purulia, West Bengal is an authentic record of my own work carried out during a period from July, 2019 to July, 2020 under the supervision of **Dr. Abdur Rahaman Sardar, CSE Department**.

The matter presented in this thesis has not been submitted by me for the award of any other degree elsewhere.

Signature of Candidate	*Signature of Candidate*	*Signature of Candidate*	*Signature of Candidate*
Subhajit Mahata	**Ankur Barick**	**Saikat Pal**	**Bikramjit Dutta**
35000116007	**35000116050**	**35000116023**	**35000116044**
CSE (4th Year)	**CSE (4th Year)**	**CSE (4th Year)**	**CSE (4th Year)**

CERTIFICATE OF RECOMMENDATION

This is to certify that the Project entitled **"Trust Based Energy Efficient and Secured Probabilistic Routing Algorithm for IoT"** has been submitted by **Subhajit Mahata, Ankur Barick, Saikat Pal, and Bikramjit Dutta** under my guidance in partial fulfillment of the degree of Bachelor of Technology in Computer Science & Engineering of Ramkrishna Mahato Government Engineering College, Purulia, WB during the academic year 2019-2020.

Signature of Supervisor(s)

Name & Designation
Project Supervisor(s)

Head of the Department
Department of Computer Science & Engineering
Ramkrishna Mahato Government Engineering College, Purulia, West Bengal

Date: 08.07.2020
Place: Purulia

ACKNOWLEDGEMENT

This project would not have taken shape without the guidance provided by Dr. A. R. Sardar, Assistance Professor of Computer Science and Engineering, project guide of the project. We profusely thank him for giving his support, encouragement and assistance to complete the project on time.

We would also like to thank our Head of Department Dr. Prasun Halder for his guidance and keen interest in our project.

We would also like to profusely express our gratitude to him for being a wonderful source of guidance for this project. We are grateful to him for lending his precious time and the patient listening they gave us every time we needed in spite of their busy schedule.

Last but not the least, above all we wish to express our heartfelt gratitude to our parents, without their support, blessings and motivation, we would not have been able to undertake this project in the first place.

Subhajit Mahata
Ankur Barick
Saikat Pal
Bikramjit Dutta

ABSTRACT

There are so many network designs and IoT models(devices) are available but all of these are not secured as well as energy efficient at the same time. The future of our next generation depends on the justifiable work we do today. Apart from these which are energy efficient, they are not fully optimized. However, in this project work we are targeting to make a network design which is concerned about IoT as well as its components in terms of energy efficiency and security. There have been a lot of research paper and research work on this topic we are aiming to make IOT device more fast, secure and energy efficient. Here we use some additional factors for performance evaluation that is "Trust Factor". Here trust factor of a node is decided by how efficiently a node send a data packet to the the destination node with minimum amount of energy. TRUST is a factor which is determined by a mathematical function which increases gradually but decreases rapidly.

This will help us to optimize the energy and also helps us to minimize the energy consumption. Then we are able to send more amount of data packets without losing a huge amount of energy.

The next factor which we focused is the "energy remaining of a node". When a node is sending some data packets they lose some energy, so we have to select only those nodes which have maximum energy as compared to the other nodes. Here we choose both best and second-best path because if a node continuously sends data packets they lose energy every time and after some time the node will be dead. To avoid the situation, we use second best path for energy efficient network design.

The next factor is LQI (Link Quality Indicator). This indicates the life span of an IOT device. The device which has more LQI factor then it has a long-term life span. It detects the quality effectiveness of a device.

The hop count refers to the number of intermediate devices between source and destination. A large number of hops in a network implies lower real time performance. So, we are targeting to decrease the number of hop count as much as possible. Shortest path may be the possible solution to reduce hop counts but it is not always realistic with respect to energy efficiency and security. So our objective is to communicate through some optimized paths which are energy efficient, trusted and also efficient with respect to hop counts.

We are going to use AODV (Adhoc On-demand Distance vector) routing protocol for making the path selection of nodes which makes the network real time efficient. It operates on two phases: route discovery and route maintenance. Route maintenance means if a node breaks down then it will share its data to the neighboring nodes. In AODV protocol the source node will not carry the complete path,

which is not seen in other routing protocol. Here each node only knows its previous nodes and the node next to it. Each node maintains route cache.

In the route discovery process there are mainly three factors: RREQs (route requests), RREPs (route replies) and RERRs (Route errors).

This RREQ has five parameters: source node id, destination node id, recent sequence number, broadcast id, hop count.

To send information from a source to a destination is the most important tasks to be carried out in a large scale and dynamic IoT environment. The routing protocols such as ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) are designed to find just the shortest path without any consideration of the energy consumption of a node. Thus, a node may be repeated many times while finding the shortest path, that decrease the life span of a node and the network becomes dead leads to the partitioning of the network. Excessive RREQ leads to the battery run out and hence we have to the limit the transmission of RREQ packets.

INTRODUCTION

We still have devices to do things before IoT [1] exists. The Internet of Things (IoT) is a platform where electronic devices are connected to the internet, so they can interact with each other and transmit data to the others. This reducing the human intervention in a machine cycle. This machine is continuously in touch with each other and adapt to their needs and modify how they function. IoT allows network connection between smart gadgets at all times, everywhere, and about everything. Wireless Sensor Networks (WSNs) [2,3] play a vital role in increasing the omnipresence of networks with smart devices that are cost effective and easy to deploy.

There are two types of wireless sensor networks: Unstructured and structured. Unstructured have a dense collection of nodes, ad-hoc deployment, it has a lot of difficulty in network maintenance. Structured have a few scarcely distributed nodes, pre-planned deployment and lower network maintenance.

Sensor applications is the local storage of data. It has permission to access the hardware and is able to interact with the operating system directly. Node Application has a specific tasks and functions of the middleware to build up and maintain the network. The IoT device faces a lot of architectural issues like energy efficiency, network topology, failure in long range communication, increases in traffic decreases the life span of a device.

AODV [4] is the reactive routing protocol. It is an extension of DSR (Dynamic source routing). In case of DSR, the data packet carries the entire route. So, as the network size grow length of path also increase and route path also increased. As a result, data packet's header also increases. For this reason, bandwidth is not utilized efficiently as most of the bandwidth is used for sending the route path. In DSR, node can have multiple route for same destination.

For this AODV is very frequently used routing protocol as it is totally depending on On-demand route acquisition system. These routes are created when it is needed, so it is called on-demand routing. It is a broadcast route discovery mechanism having RREQ (Route request packets) broadcasting to find a route and RREP(route reply packet) is used to set up forward path. It is used for sending data packets and when the data packets received then it send some acknowledgements in reply (route reply).AODV has dynamic establishment of route table entries. Nodes lie on active path only maintain routing information. It has a clear maintenance of timer-based states and for that reason a routing table entry is expired if not used recently.

In AODV, every node maintains two counters: one is sequence number and another is broadcast_id: which is increase whenever the source issues a anew RREQ. Then source broadcast RREQ data packet

for searching route <source_addr, source_sequence#, broadcast_id,dest_addr,dest_sequence#,hop count>.

After that when the destination receives the packets then it replies using RREP unicasting <source_addr, dest_addr,dest_sequence#, hop_count,lifetime>. RREP contains the current sequence number, hop count=0, full lifetime.

If the intermediate nodes found any duplicate nodes then it discards it and send RREP, if it has active route with higher sequence number.

LITERATURE SURVEY

Internet of Things (IoT) has been attracting much interest of many researchers in the last few years. IoT creates a worldwide network of interconnected devices that should be uniquely addressable. Many routing protocols are available for Wireless Sensor Networks (WSNs) and some classifications are flat, location-based and hierarchical/cluster categories [5].

Hierarchical architecture consists of heterogeneous nodes viz. cluster-head and non-head nodes which have different roles or functionalities. To improve energy consumption and QoS for a set of IoT applications [6] (for example multimedia-based fire station [7]), routing protocols based on clustering can be an alternative. Nodes of the cluster architecture transmit with sensor-to-sensor and with the cluster-head which is responsible for communicating outside the cluster i.e. sensor-to-Base Station. Nodes like cluster-head can have cameras and extra batteries [8]. Residual energy, link quality and location [9] these are the key features based on which cluster-head is elected and there are many algorithms for that. But these algorithms require time for cluster formation, generating additional complexity and delay, which are unstable for many IoT applications.

Collection Tree Protocol (CTP) [10] is widely used in WSNs. This architecture totally based on collecting trees where sensor nodes share the same specific destination node or BS. CTP and Multihop LQI [11] are some existing solutions. A tree of multiple hops is constructed dynamically for routing messages and data, then a traffic pattern of many-to-one is created naturally. As the applications of this feature are dynamic in nature, it prohibits their general use in IoT. Such kind of applications are smart parking and environmental monitoring. However, routing solutions should consider different types of traffic pattern such as one-to-many, many-to-one and many-to-many.

LABILE is another protocol which is based on lexical structures and link quality evaluation. LABILE is one of the protocols for WSNs/IoT that does not evaluate the number of hops metric. LABILE is also called Link Quality-Based Lexical Routing [12]. Routing algorithm proposed by LABILE evaluates end-to-end link quality [13], by classifying the possible values of LQI [14] into good or bad. For link classification a threshold value is determined, then the lowest values of LQI are considered bad which are below the threshold value. These links are more capable of packet loss. These types of bad links are counted, recorded and reported with the help of an additional field in RREQ and RREP messages, during the route discovery process. These are the *Weak Links*. However, the main objective of LABILE is to select routes with good link qualities. This type of behavior leads to

exhaustive use of good link quality routes which causes the premature death of the nodes associated with that specific route. This happens because there is no mechanism which considers an alternative route in this situation. During route selection process, therefore, LABILE does not consider energy-efficiency factor and load balancing mechanisms. Thus, LABILE does not meet the expected result for multipath WSN/IoT scenarios [15].

The EEURP (Energy Efficient Unicast Routing Protocol) [16] proposes a cost function to select routes based on the average energy consumption in the end-to-end path, hop count and the minimum energy level. The additional fields for RREQ and RREP messages report the lowest energy level along a route and the total amount of residual energy of a path. The minimum energy of a path shows if there is a hop with a critical level of energy. The route discovery mechanism takes into account that only the destination node answers the RREQ messages, i.e., the intermediate nodes that have an available route to the destination do not reply by using a RREP message. This approach is required to calculate the energy level of the entire route, although it creates an extra signalling overhead, leading to an additional expenditure of energy and congestion in the WSNs. The main drawback of EEURP is that it does not include a mechanism to estimate the link quality level. EEURP is focused only on the network lifetime and does not consider QoS support for IoT applications.

Routing protocols for WSNs can be classified into three categories: flat, location-based and hierarchical/cluster categories. The flat structure is the most common among all and can be considered a suitable solution for many IoT applications, such as smart homes and offices, healthcare [17], and many smart city services [18]. Still most of the devices and services have very less tolerance of packet losses.
A routing protocol depend upon on three possible routing procedures. The routing protocols are as follows: simple routing, based on Round-Robin, and weighted-Round Robin.

In simple routing models, each and every network node select only one single node to route each packet node but, in the Round, -Robin routing, each source node has to choose two or more nodes to route each packet using an equilibrium in load balance. This process has no order for delivery of nodes from source to destination. But we cannot use this method in many IoT devices due to its non-feasibility.

The weighted Round-Robin routing technique gives load balance mechanism that assigns a weight to each routing node that is proportional to its metric values. However, the protocol uses remaining energy as routing metric, it does not give any solutions for the problem of energy hole [19]. Although, the estimation of the quality of link used in the experiments does not represent the end-to-end link quality during the process of route selection.

Wireless ad-hoc networks are broadly used in various types of applications such as vehicle-to-vehicle (V2V) networks. Here, each node can send messages to only those nodes in the wireless communication range. Messages are forwarded to destination nodes by wireless node-to-node communication in AODV routing protocols. It is very difficult to reduce the electric energy

consumption of nodes to deliver messages because nodes work by using the electric battery. A reliable unicast communication protocol named ESU (Energy-Saving Unicast routing) protocol where an energy-efficient route from a source node to a destination node is actively found by selecting nodes which engross smaller electric energy. In the evaluation, we can see that electric energy consumption of nodes can be reduced in the ESU protocol contrast to other protocols.

AODV algorithm widely used because of its well-defined structure and low complexity. In AODV, on-demand routes can be discovered, which decrease the overhead of a node, by using pairs of Route Request (RREQ) and Route Reply (RREP) messages. Generally, the route selection is based on the number of hops (hop count), which is not completely energy efficient.

A short path, in terms of hop count, can be more vulnerable to packet loss, because of both noise and interference that affect the link quality. Due to lack of energy-efficiency mechanism energy holes and an uneven distribution of scarce network resources are created. Apart from this AODV only stores one possible route for a given destination node. This means that if a single route fails or is unavailable, a new route must be discovered, which need more time and increases the delay or failure rate of data delivery.

A routing protocol depending on Routing by Energy and Link quality (REL) [20] widely used in IoT applications. To increase dependability and energy-efficiency, REL choose routes on the basis of a suggested end-to-end link quality estimator mechanism, residual energy and hop count. Moreover, REL introduces an event-driven mechanism to provide load balancing and avoid the impulsive energy deployment of nodes/networks and by performing this, REL also avoids the premature death of nodes/networks. Performance assessment were carried out using simulation and testbed experiments to show the influence and advantages of REL in small and large-scale networks. To increase the system's reliability and assure QoS support for IoT applications, REL basically uses the link quality of wireless links and residual energy during the routing selection process. This routing protocol consists of two main operation which are Link Quality Estimation and Path Selection & Load Balancing. The results show that REL increases the network life span and quality of services availability. It also gives an even distribution of deficient network resources and decrease the packet loss rate, as compared with the performance of commonly used protocols.

Software Requirements Specifications (SRS)

1. Introduction

1.1 Purpose

The purpose of this document is to provide the software requirement specification report for the

Energy Efficient Probabilistic Routing Algorithm for efficient transmission of Data Packets.

1.2 Intended Audience and Reading Suggestions

This project is the college level project and is implementing under the guidance of college professors.
This project is useful for increasing trust value and efficiency of an IoT device for transmission of data.

1.3 Scope

The IoT devices and all wireless sensors networks are smarter than any device but still it has a lot of disadvantages. It is easy for hackers to hack a network, so we have to make network design more secure. It has comparatively low speed of communications so there is a scope to enhance the speed of communication. The wireless devices can be distracted by various elements so we have to be aware about this and should try to make it more reliable and practical. The devices which have a long range of communication they are very costly, so we have a scope to make IoT projects in a large scale which will be cost efficient. The life span of nodes is not so high so there will be a future scope to make it more effective throughout a long span of time. The last but not the least, energy efficiency, there is a huge scope to make IoT devices more energy efficient in the future and to make it optimized. In the future we can see that people are fond of wireless devices which makes their life easier and more comfortable. It avoids lot of wiring and can accommodate new devices at any time. Flexible to go through physical partitions and can be accessed through a centralized monitor.
Wireless sensors networks possess the potential for many applications. The advancement of technology allows the creation of WSN's, but the hardware and software both have a huge scope before WSNs are practical, secure, cost-efficient.

1.4 Definitions, Acronyms and Abbreviations

Term	Definition
OMNET ++ [21]	Extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators.
Castalia [22]	A simulator for Wireless Sensor Networks (WSN), Body Area Networks and Wireless networking
LQI	Link Quality Indicator
AODV	**Ad-hoc On-demand Distance Vector**, a loop-free routing protocol for ad-hoc networks. It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviors such as node mobility, link failures and packet losses.
PDR	Packet Delivery Ratio
Router	Networking device that forwards data packets between computer networks
IP	Internet Protocol
QoS	Quality of Service
REL	Routing by Energy and Link quality

2. General Description

2.1 Product Perspective

Trust Based Energy Efficient and Secured Probabilistic Routing Algorithm provides the most efficient way for transmission of data packets in a selective way by avoiding multicasting.

- **OMNeT++:** OMNeT++ (Objective Modular Network Testbed in C++) is a modular, component-based C++ simulation library and framework, primarily for building network simulator. OMNeT++ can be used for free for non-commercial simulations like at academic institutions and for teaching. OMNEST is an extended version of OMNeT++ for commercial use cases.
- OMNeT++ itself is a simulation framework without models for network protocols like IP or HTTP. The main computer network simulation models are available in several external frameworks. The most commonly used one is INET which offers a variety of models for all kind of network protocols and technologies like for IPv6, BGP etc. INET also offers a set of mobility models to simulate the node movement in simulations. The INET models are licensed under the LGPL or GPL.

- **Castalia:** Castalia is a simulator for Wireless Sensor Networks (WSN), Body Area Networks and generally networks of low-power embedded devices. It is based on the OMNeT++ platform and used by researchers and developers to test their distributed algorithms and/or protocols in a realistic wireless channel and radio model, with a realistic node behaviour especially relating to access of the radio. Castalia uses the lognormal shadowing model as one of the ways to model average path loss, which has been shown to explain empirical data in WSN. It also models temporal variation of path loss in an effort to capture fading phenomena in changing environments (i.e., the nodes or parts of the environment are moving). Castalia's temporal variation modeling is designed to be fitted to measured data instead of making specific assumptions on the creation of fast fading. Other features of Castalia include: physical process modeling, sensing device bias and noise, node clock drift, and several MAC and routing protocols implemented.
- Castalia was developed at the National ICT Australia starting in 2006. Since 2007 it is public as an open source project under the Academic Public License. The current release version is 3.3.

2.2 Product Functions

Trust Based Energy Efficient and Secured Probabilistic Routing Algorithm performs the following functions:

- Make the networking model more efficient and secured.
- Reduce the Traffic in a Complex Networking System
- Reduce the hop count of a node
- Avoid Multicasting and Broadcasting and send data packets to only selective nodes which achieves better PDR (Packet Delivery Ratio)

2.3 Operating Environment

- Platform: C++ (GCC-14), Python 3.6

Operating System: Windows/Linux/Mac

- Database: Not used.
- Client/Server: Not used

2.4 Assumptions and Dependencies

- Castalia should be installed.
- OMNeT++ should be installed.
- Install Ubuntu 12.04.5-LTS 64 bit
- Install CtpCastalia-beta-1.1

The algorithm is designed in C++14 and Python 3.6 environment thus C++ and Python should be installed in order to run the Algorithm. The algorithm requires a secured structure and networking system for which we use OMNeT++.

The accuracy of the result is dependent on the following factors:

- ❖ PDR with respect to number of nodes
- ❖ PDR vs no. of malicious nodes
- ❖ No. of nodes dies with respect to time
- ❖ Remaining energy of each node after time T

3. Specific Requirements

3.1 External Interface Requirements

3.1.1 User Interfaces

- Command Line Interface.

3.1.2 Hardware Interfaces

- Processor equivalent to or greater than Pentium Dual Core.

3.1.3 Software Interface

Software	Description
C++14	The system is designed in C++14 environment.
Python 3.6	The system is designed in a Python3.7 environment.
OMNeT++	Extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators.
Castalia	**Castalia** is a simulator for Wireless Sensor

	Networks (WSN), Body Area Networks (BAN) and generally networks of low-power embedded devices.

3.1.4 Communications Interfaces

- Command Line Interface is used for communication purpose.

DESIGN PHASE

The primary goal of the project is to make an algorithm which can increase efficiency of an IoT Device, reduce multicasting and send data packets only to specific nodes and increase trust value of a device.

Overview of OMNeT++

The OMNeT++ discrete event simulation environment has been publicly available since 1997. It has been created with the simulation of communication networks, multiprocessors and other distributed systems in mind as application area, but instead of building a specialized simulator, OMNeT++ was designed to be as general as possible. Since then, the idea has proven to work, and OMNeT++ has been used in numerous domains from queuing network simulations to wireless and ad-hoc network simulations, from business process simulation to peer-to-peer network, optical switch and storage area network simulations. This paper presents an overview of the OMNeT++ framework, recent challenges brought about by the growing amount and complexity of third-party simulation models, and the solutions we introduce in the next major revision of the simulation framework.

OMNeT++ was designed from the beginning to support network simulation on a large scale. This objective lead to the following main design requirements:

- To enable large-scale simulation, simulation models need to be hierarchical, and built from reusable components as much as possible.
- The simulation software should facilitate visualizing and debugging of simulation models in order to reduce debugging time, which traditionally takes up a large percentage of simulation projects. (The same feature set is also useful for educational use of the software.)
- The simulation software itself should be modular, customizable and should allow embedding simulations into larger applications such as network planning software. (Embedding brings additional requirements about the memory management, restartability, etc. of the simulation).
- Data interfaces should be open: it should be possible to generate and process input and output files with commonly available software tools.
- Should provide an Integrated Development Environment that largely facilitates model development

Overview of Castalia 3.2

Castalia is a simulator for Wireless Sensor Networks (WSN), Body Area Networks (BAN) and generally networks of low-power embedded devices. It is based on the OMNeT++ platform and can be used by researchers and developers who want to test their distributed algorithms and/or protocols in realistic wireless channel and radio models, with a realistic node behavior especially relating to access of the radio. Castalia can also be used to evaluate different platform characteristics for specific applications, since it is highly parametric, and can simulate a wide range of platforms. The main features of Castalia are:

- Advanced channel model based on empirically measured data.
- Model defines a map of path loss, not simply connections between nodes
- Complex model for temporal variation of path loss
- Fully supports mobility of the nodes
- Interference is handled as received signal strength, not as separate feature
- Advanced radio model based on real radios for low-power communication.
- Probability of reception based on SINR, packet size, modulation type. PSK FSK supported, custom modulation allowed by defining SNR-BER curve
- Multiple TX power levels with individual node variations allowed
- States with different power consumption and delays switching between them
- Realistic modelling of RSSI and carrier sensing
- Extended sensing modelling provisions
- Highly flexible physical process model.
- Sensing device noise, bias, and power consumption.
- Node clock drift
- MAC and routing protocols available.
- Designed for adaptation and expansion.

Concerning the last bullet, Castalia was designed right from the beginning so that the users can easily implement/import their algorithms and protocols into Castalia while making use of the features the simulator is providing. Proper modularization and a configurable, automated build procedure help towards this end. The modularity, reliability, and speed of Castalia is partly enabled by OMNeT++, an excellent framework to build event-driven simulators [OMNeT++ link].

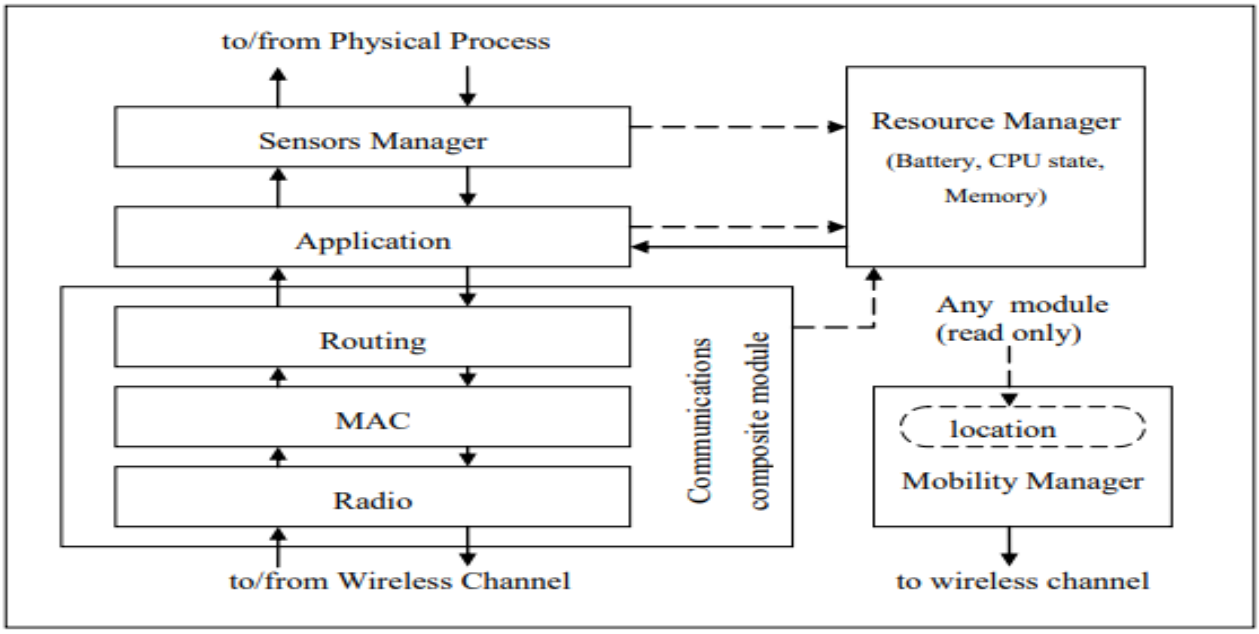


Fig: The node composite module

Castalia is not sensor-platform specific. Castalia is meant to provide a generic reliable and realistic framework for the first order validation of an algorithm before moving to implementation on a specific sensor platform. Castalia is not useful if one would like to test code compiled for a specific sensor node platform.

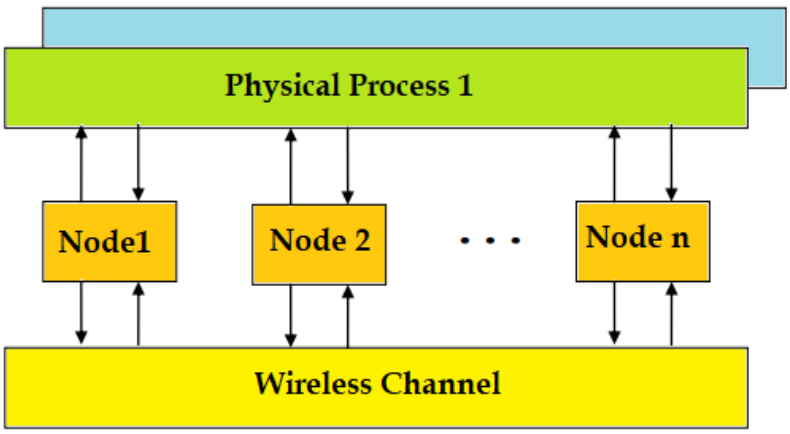


Fig: Modules and their connections in Castal

Proposed Algorithm

PATH FINDING ALGORITHM

1. Let LQIth = LQI threshold value
2. Let REth = RE threshold value
3. Let TRUSTth= TRUST threshold value
4. PossiblePath emty Array
5. For All path Psd
6. If Minimum(LQI)>=LQIth and Minimum(RE)>=REth and Minimum(TRUST)>=TRUSTth
7. Cost(i)=W1*Minimum(LQI)+W2*Minimum(RE)+W3*Minimum(TRUST)
8. Add Psd in PossiblePath
9. End If

9. End For

10. For PossiblePath i and j
11. If |hopCount(ith path)- hopCount(ith path) |<=D
12. Send Data to Minimum Cost Path(ith path,jth path)
13. Else
14. Let Next Minimum Cost Path Kth path
15. If Energy(kth path) - Energy(kth path) >=mde
16. Send Data to Kth Path
17. End If
18. End If
19. End For

1.The proposed EESPR algorithm controls the request packet forwarding process in order to reduce the packet loss and network congestion in the context of AODV protocol.

2.The proposed algorithm is based on four main components, namely,

i)Trust factor: The trust factor of a node is decided by how efficiently a node sends a data packet to the destination node using minimum amount of energy. This will help us to optimize the energy and also helps us to minimize the energy consumption. It is determined by a mathematical function which increases gradually but decreases rapidly.

ii)Energy of a node: When a node sends data packets, it loses some energy, so we select only those nodes which have maximum energy when compared to the other nodes. Here we choose both the best and second-best paths because if a node continuously sends data packets, it loses energy every time and will gradually become dead. In order to overcome this situation, we use the second-best path for energy efficient network design.

iii) LQI (Link Quality Indicator): This indicates the lifespan of an IoT device. A device with more LQI factor will have longer life span. It denotes the quality effectiveness of a device.

iv)Hop Count: It refers to the number of intermediate devices between source and destination.A large number of hops in a network implies lower real time performance. So, we target on minimizing the number of hops as much as possible.

3.AODV is a reactive routing algorithm and is totally dependent on On-Demand routing system, ie., routes are created only when needed.

4. It is a broadcast route discovery mechanism having RREQ(Route request packets) broadcasting to find a route and RREP(route reply packet) is used to set up the forward path.

5. Initially, a source node that has data packets to transmit forwards the RREQ packets to its neighbour nodes by composing their trust factor, residual energy and hop count.

6.The forwarded node that receives a RREQ packet calculates the forwarding probability using its residual energy and trust factor, hop count and then forwards it to all their neighbor nodes till the data packets reach the destination node.

7.Here every node maintains two counters: sequence number and broadcast_id: which increases whenever the source issues a a new RREQ. Then source broadcast RREQ data packet for searching route <source_addr, source_sequence#, broadcast_id,dest_addr,dest_sequence#,hop count>.

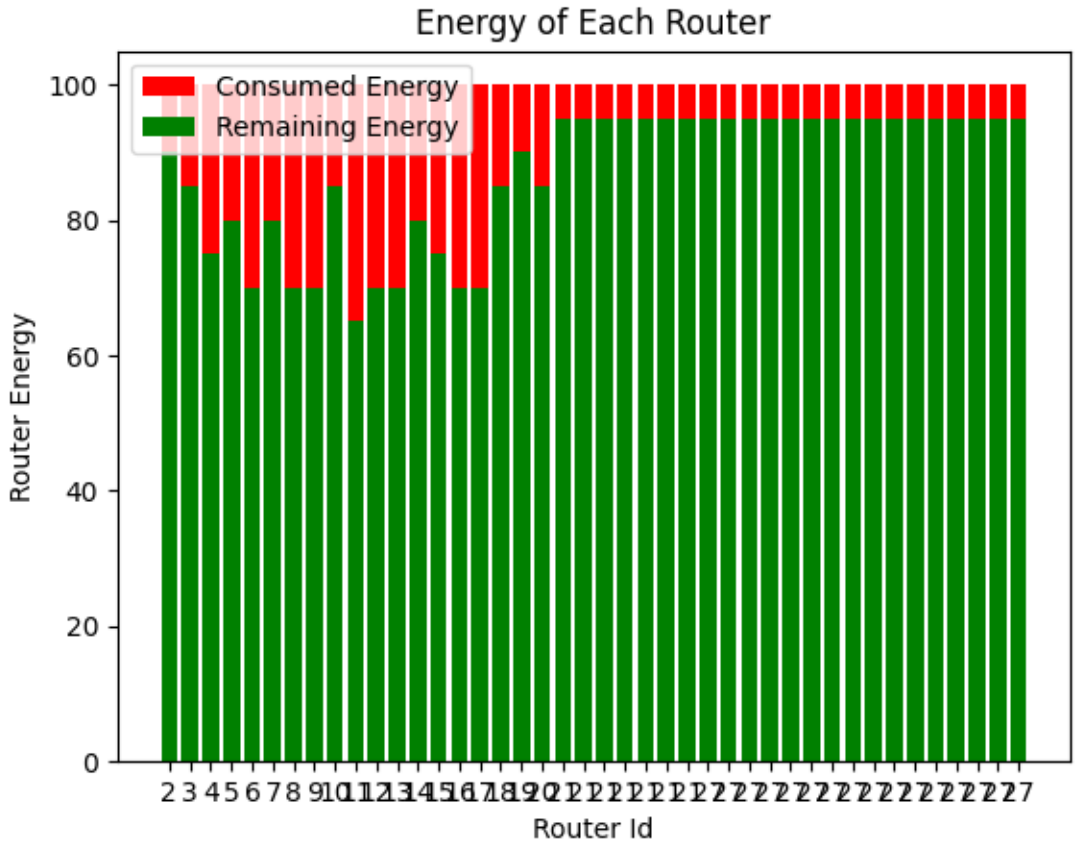
8. After that when the destination receives the packets then it replies using RREP unicasting <source_addr, dest_addr,dest_sequence#, hop_count,lifetime>. RREP contains the current sequence number, hop count=0, full lifetime.

9.Thus using this EESPR algorithm, we send the data packets from source to destination without multicasting and also with minimal energy loss and consumption.

10.In addition, the EESPR algorithm controls the flooding of RREQ packets in an opportunistic way, so reduces the overhead in the routing process, and finds the energy-efficient routing path more efficiently compared to the other protocols.

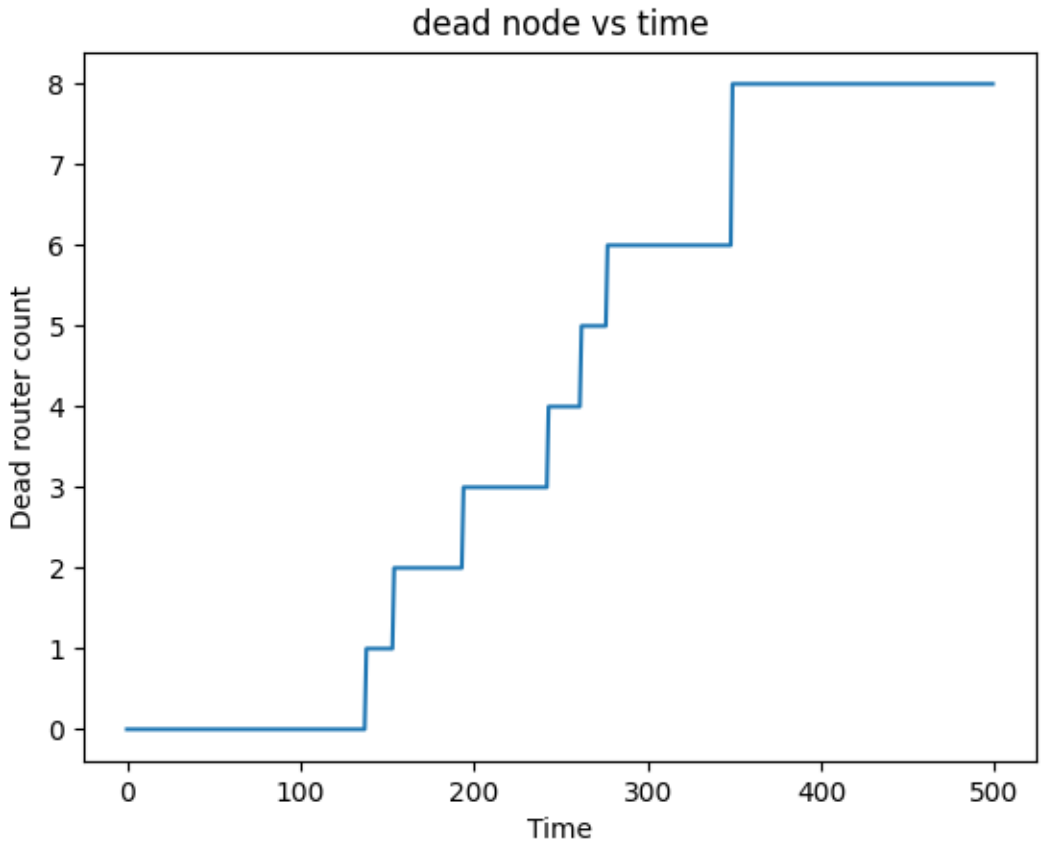
RESLUTS ANALYSIS AND DISCUSSION

Figure 1: Consumed Energy vs Remaining Energy



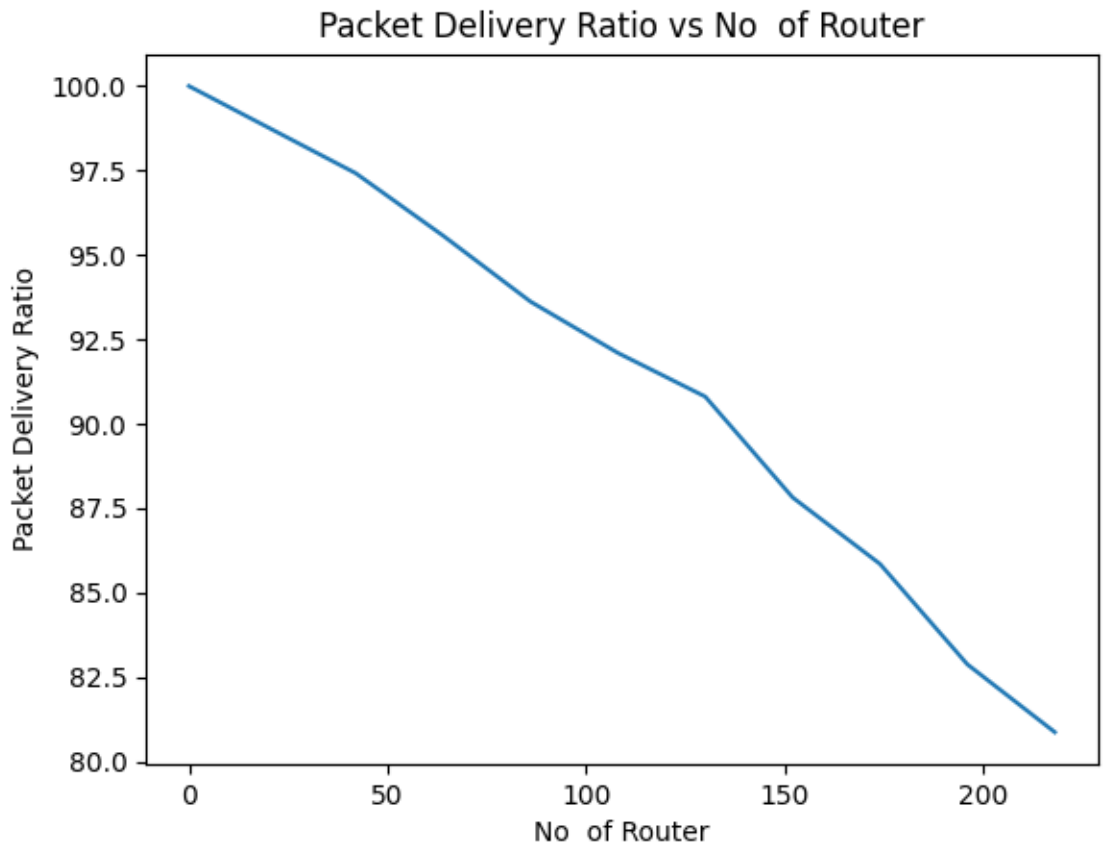
In this project we evaluate the performance of our Routing Algorithm as compared to typical AODV and EEPR algorithm. This graph shows a relationship between Consumed Energy and Remaining Energy in a Networking model with many nodes. In terms of Energy Efficiency our Algorithm is more efficient as compared to other previous Algorithms because in AODV, we send data packets to every node and hence a huge amount of energy needed but, in our algorithm, we send data packets only to the selected nodes based on some factors. That's why we use minimum amount of energy which is a important factor for IoT Devices.

Figure 2: Dead node vs Time plot



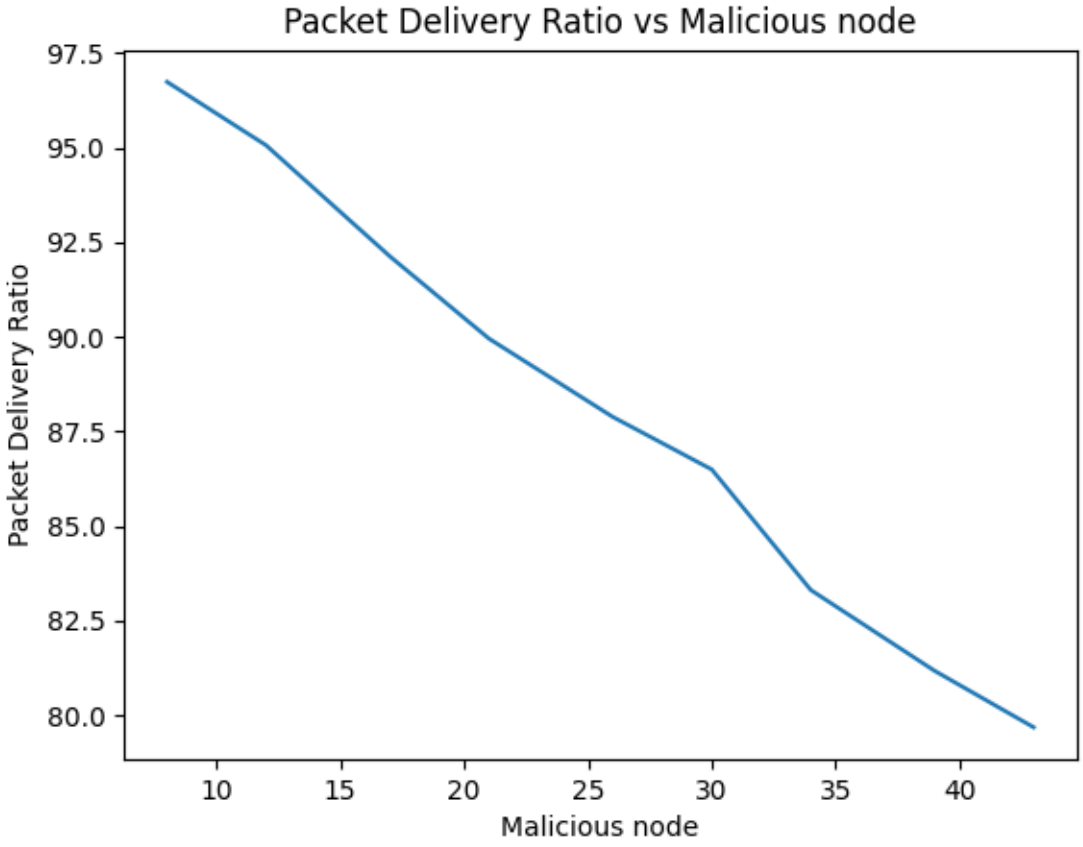
This graph depicts the relationship between dead nodes with respect to time. Basically, in AODV protocol after sometime the nodes become dead (with zero energy left) because the send data packets to each node and losses a huge amount of energy. But in our modified Algorithm, a single router sends data packets and transmit data with a single router (one to one) with minimum energy. So, the life span of a node increases and a node can transmit data for long time, it will bring a plus factor in IoT Devices.

Figure 3: Packet Delivery Ratio vs No. of Router



This graph shows the performance in comparison with PDR (Packet Delivery Ratio) with respect to number of routers. Here, our algorithm is less efficient than compared to typical AODV and EEPR algorithm because we send data packets to only one router and hence probability of successful receiving of data packets is less here. But in AODV, we send data packets to each and every router despite of any factors so the ratio is high for successful transmission of data and hence increasing packet delivery ratio also.

Figure 4: Packet Delivery Ratio vs Malicious Nodes



This is a graph plot between malicious nodes and Packet Delivery Ratio. In typical algorithms like AODV if Number of malicious nodes increases in a network then the Packet Delivery Ratio will decrease. But, our algorithm has an additional factor which is “TRUST FACTOR”. If a node sends data packet to a selective node based on the factors we considered previously, and it found to be malicious then its trust value will decrease and hence they will not send data to that particular node. That means if the Trust Value become less than threshold value, then the node will not send data to that node. This will save a lot of energy.

CONCLUSION AND FUTURE SCOPES

1)The primary objective of this project is to transfer data packets in an energy-efficient, secure manner and we implemented it using our modified algorithm considering the important aspects of nodes such as their Trust Value, Energy Remaining, LQI and hop count.

2)The proposed EESPR algorithm has longer network lifetime but the limitation is that the routing set up delay is slightly
increased.

3)The IoT devices and all wireless sensors networks are smarter than any device but still it has a few disadvantages.

4)The variables trust factors, LQI and energy of the node that are used in this algorithm are taken as constants, but there is always a scope to optimize the output of the algorithm by modifying the variable values.

5)We designed the project using OMNeT++ thus trying to make it more secure than the other protocols but there might be a loophole, for hackers to hack a network, so there is scope to make the network design much more secure.

6)It has comparatively low speed of communications so there is a scope to enhance the speed of communication.

7)The wireless devices can be distracted by various elements so we have to be aware about this and should try to make it more
reliable and practical.

8)The devices which have a long range of communication are very costly, so there is a scope to make IoT projects in a large scale
which will be cost efficient.

9)The life span of nodes is increased considerably in this project and there will be a future scope to make it more effective throughout a long span of time.

REFERENCES

1. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. Comput. Netw. 2010, 54, 2787–2805.
2. Akyildiz, I.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. Comput. Netw. 2002, 38, 393–422.
3. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. Comput. Netw. 2008, 52, 2292-2330
4. Perkins, C.; Belding-Royer, E.; Das, S. Ad hoc on Demand Distance Vector (AODV) Routing (RFC 3561). Available online: http://www.ietf.org/rfc/rfc3561.txt (accessed on 30 January 2013).
5. Ehsan, S.; Hamdaoui, B. A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. IEEE Commun. Surv. Tutor. 2012, 14, 265–278.
6. Becker, M.; Gupta, A.; Marot, M.; Singh, H. Improving Clustering Techniques in Wireless Sensor Networks Using Thinning Process. In Proceedings of the International Conference on Performance Evaluation of Computer and Communication Systems: Milestones and Future Challenges, Lisbon, Portugal, December 2011; pp. 203–214.
7. Ros´ario, D.; Costa, R.M.; Paraense, H.; Machado, K.; Cerqueira, E.; Braun, T. A Smart Multi-Hop Hierarchical Routing Protocol for Efficient Video Communication over Wireless Multimedia Sensor Network. In Proceedings of the 2nd IEEE International Workshop on Smart Communication Protocols and Algorithms, Ottawa, Canada, 10–15 June 2012.
8. Ros´ario, D.; Machado, K.; Abel´em, A.; Monteiro, D.; Cerqueira, E. Recent Advances and Challenges in Wireless Multimedia Sensor Networks; Mobile Multimedia—User and Technology Perspectives; InTech: New York, NY, USA, 2012; pp. 74–96.
9. Diallo, C.; Marot, M.; Becker, M. A Distributed Link Quality Based D-Clustering Protocol for Dense ZigBee Sensor Networks. In Proceedings of the IFIP Wireless Days 2010, Venice, Italy, 20–22 October 2010; pp. 1–6.
10. Gnawali, O.; Fonseca, R.; Jamieson, K.; Moss, D.; Levis, P. Collection Tree Protocol. In Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, Berkeley, CA, USA, 4–6 November 2009; pp. 1–14.
11. Diallo, C.; Marot, M.; Becker, M. Link Quality and Local Load Balancing Routing Mechanisms in Wireless Sensor Networks. In Proceedings of the Sixth Advanced International Conference on Telecommunications (AICT), Barcelona, Spain, 9–15 May 2010; pp. 306–315.
12. Butt, M.; Javed, M.; Akbar, A.; Taj, Q.; Lim, C.; Kim, K. Labile: Link Quality-Based Lexical Routing Metric for Reactive Routing Protocols in IEEE 802.15.4 Networks. In Proceedings of the 5th International Conference on Future Information Technology (FutureTech), Busan, Korea, 21–23 May 2010; pp. 1–6.

13. Gomez, C.; Boix, A.; Paradells, J. Impact of LQI-based routing metrics on the performance of a one-to-one routing protocol for IEEE 802.15.4 multihop networks. EURASIP J. Wireless Commun. Netw. 2010, 2010, 1–20.
14. Renner, C.; Ernst, S.; Weyer, C.; Turau, V. Prediction Accuracy of Link-Quality Estimators. In Proceedings of the 8th European Conference on Wireless Sensor Networks, Bonn, Germany, 23–25 February 2011; pp. 1–16.
15. Radi, M.; Dezfouli, B.; Bakar, K.; Lee, M. Multipath routing in wireless sensor networks: Survey and research challenges. Sensors 2012, 12, 650–685.
16. Chung, Y. An energy-efficient unicast routing protocol for wireless sensor Networks. Tech. Int. J. Comput. Sci. Emerg. Tech. 2011, 2, 60–64.
17. Gao, T.; Greenspan, D.; Welsh, M.; Juang, R.; Alm, A. Vital Signs Monitoring and Patient Tracking over a Wireless Network. In Proceedings of the 27th Annual International Conference of the Engineering in Medicine and Biology Society, Osaka, Japan, 30 August–3 September 2006; pp. 102–105.
18. Sanchez, L.; Galache, J.; Gutierrez, V.; Hernandez, J.; Bernat, J.; Gluhak, A.; Garcia, T. SmartSantander: The Meeting Point between Future Internet Research and Experimentation and the Smart Cities. In Proceedings of the 2011 IEEE Future Network & Mobile Summit, Warsaw, Poland, 15–17 June 2011; pp. 1–8.
19. Ramos, H.S.; Oliveira, E.M.R.; Boukerche, A.; Loureiro, A.A. Characterization and Mitigation of the Energy Hole Problem of Many-to-One Communication in Wireless Sensor Networks. In Proceding of the IEEE International Conference on Computing, Networking and Communications, Okinawa, Japan, 5–7 December 2012.
20. Machado, K.; Ros´ario, D.; Nakamura, E.; Abel´em, A.; Cerqueira, E. Design of a Routing Protocol Using Remaining Energy and Link Quality Indicator (REL). In Proceedings of the 6th Latin America Networking Conference, Quito, Ecuador, 12–14 October 2011; pp. 33–39.
21. Varga, A. The OMNeT++ Discrete Event Simulation System. In Proceedings of the European Simulation Multiconference (ESM 2001), Prague, Czech Republic, 6–9 June 2001.
22. Boulis, A. Castalia, A Simulator for Wireless Sensor Networks and Body Area Networks, Version 2.2. User's Manual; NICTA: Canberra, Australia, 2009.