Energy Consumption Estimation for Reliable Wireless Sensor Networks in Smart Homes

N. Satheesh[1],P. Santhosh Kumar Patra[2]
[1,2]Professor,St.Martin's Engineering College,Dhulapally,Secunderabad-500100

Abstract

Wireless interactions with sensors play a vital position in the evolving modern IoT environment. As the industry will now be able to carry out the second generation of IoT products, efforts are geared towards completely standardizing the Wireless Sensor Network (WSN) protocol suite and ensuring complete system IP compatibility. The WSN protocols are potential candidates for a highly usable implementation layer for the Internet of Things in terms of robust communications and conformity to the less verbose characteristics of WSNs in which sleep cycles are used in an attempt to maintain the overall power consumption of end nodes small. This article describes an ideal implementation of WSNs taking into consideration the usage of electromagnetic radiation, data link and physical layer, and energy use in smart homes. This research seeks to explore the need for simple connectivity between devices and servers in Smart Home environments, in an effort to establish an optimized state view of the network, and that this dimension of confusion while also trying to conform with the less verbous existence of restricted network context. A surface was specified for the study in which smart devices were distributed randomly to guarantee that the entire the devices conduct an efficient routing, entering the gateway via the formation of a WSN. In order to quantify the scale of the information and fill areas of the data link layer, various wireless networking systems were evaluated to evaluate the exact size that transports the physical material. This knowledge is used by increasing technologies to maximize channel utilization times, lengths, energy usage, and bandwidth specifications. This paper seeks to include an application-level keep-alive algorithm, which can be run separately, to serve as a feasible alternative to preserve a more up-to-date perception of safety-critical devices in WSNs than existing protocols deployed in today's Internet of Things operating systems provide.

Keywords: Smart Homes; WSNs; IoT , Energy Consumption, Channel Deployment, Protocol, Security.`

1. Introduction

The Internet of Things (IoT) is the colloquial term for the interconnection of objects or "things" to the existing Internet infrastructure. These devices, usually small embedded computational devices, will transform our concept of Internet connectivity. By equipping objects such as cars, laundry machines, in-door heating systems, and even our-selves with Internet capabilities, the way that we will interact with these objects and how these objects will interact with each other will change drastically. In this new era of

technology, it is expected that WSN will play a key role in the information exchange between embedded devices and the Internet. However, wireless communications are not without obstacles, and as we allow objects to become connected to the Internet, efforts must be taken to ensure reliable connection given any external impacts such as interference or absorption.

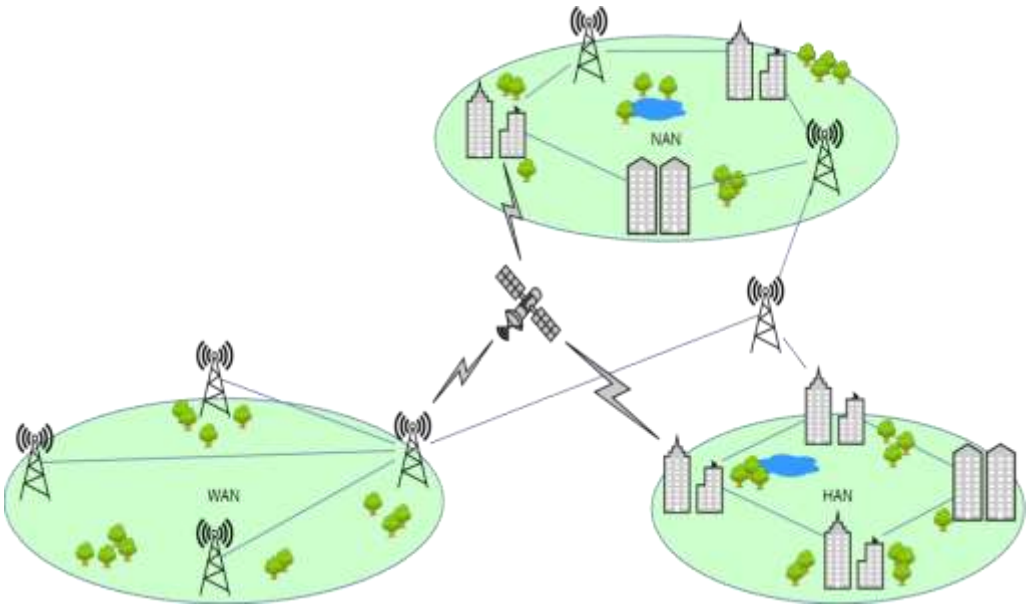

Figure 1.Model of Smart Communications in WSN

To form the smart grid, various integrated networks and subsystems need to be clustered together, offering features such as high rates of supply, health, performance, energy quality, and responsiveness to growth in demand. The modern smart electricity grids combine large-scale renewable energy to provide environmental protection, optimize output from generation to use through the cooperation of network systems, tracking, control, communications networks, sensors, and actuators (Refer figure 1).

Intelligent system energy use in data transmission/retransmission activities is a complicated problem to contend with as humans, systems, resources, and issues collide in real-time. Recent technology developments include tools that have the potential to collect, store, and transmit knowledge from the world to an information retrieval network.

The purpose of this thesis is to examine and review the currently emerging protocols and technologies together with the generally assumed uses of IoT in smart home environments and propose a method for addressing the unknown state problem, where embedded devices may be asleep for a long duration of time in order to prolong their battery life, but which introduces the uncertainty to whether the device is asleep, or if by any other means unable to communicate, such as due to device or link failure. And the optimization of energy usage must be taken into consideration when transferring data from the devices to the network gateway, the wireless infrastructure, and the protocols to be implemented. To evaluate the most effective technologies, we evaluated frame size, transmitting capacity, receiver responsiveness, range,

operating FRQ, transmitting rate, and the no. of maximum nodes that a WSN will eventually calculate when the channel is used in information transmission.

2. Related Works

Works on fault tolerance and fault detection in WSNs have previously been carried out by, among others [6] [7]. A common denominator for these previous works is that they try to find algorithms that are both fault-tolerant as well as energy-efficient, as fault tolerance cannot come at a high energy cost since long operation time by battery-operated nodes are of great concern. High redundancy, with the option of powering down the redundant nodes, has been suggested [8] [9], but which would inadvertently lead to the higher installation cost and increased complexity of the network. Moreover, evaluation and efforts on fault tolerance mechanisms for WSN standards IEEE 802.15.4 and ZigBee have been presented

Many approaches to achieving both energy efficiency and data consistency have been suggested. The Alep protocol indicated in [12], is an adaptive, lazy, and energy-efficient protocol that relies on aggregating data and delaying deliveries to reach energy efficiency.

IEEE 802.15.1 is a requirement for local area wireless networks. This optimizes electricity usage, owing to its short-range distribution area. This works in the frequency range of 2.4 GHz ISM, which has up to 79 outlets. For a length of 625 us, it utilizes slotted time outlets. Based on modulation schemes, the transmission speeds can differ and can hit range. 802.15.1 facilitates the construction of peer-to-peer or star topology networks. It has 32-bit data security from the CRC and can cover lengths of up to 10 meters. [6][7]

WSNs can provide "cells" through data collection and delivery inside IoT, allowing smart, context-conscious applications to be created. Such systems are the true enablers of IoT, in terms of lifespan, energy usage, low cost, and communication, by exchanging increasing forms of power sources and retaining resource control over long periods. Additionally, developments in electric power storage technologies have moved the flexibility of sensors to new heights.

The technical sophistication of advanced communication technologies, the growing amount of base stations needed for high data speeds, and electromagnetic emissions fuel the rise in total network energy usage. As energy costs increase, it is evident that the trade-off between radio output and energy conservation will become increasingly significant for WSNs, which are near future.

3. Proposed Methodology

There exist a number of different approaches to developing software for WSN devices. This chapter explains the standard method of using operating system programming to build software for constrained devices in the IoT field. This approach has become the norm when programming for sensor nodes, as the usage of a base operating system, dramatically reduces the need to duplicate functionality and simplifies the porting of software across different hardware platforms. Moreover, energy-efficiency, when communicating as well as compatibility between nodes can be increased as the underlying architecture of

the operating system can be shared across different types of nodes (refer figure 2). Also, in effort to speed up development and testing, the fundamental approach to programming with the operating system, which will be used when constructing and testing the algorithm in the subsequent chapter, is explained in this chapter together with how virtual topologies can be used for native devices to simulate high-depth networks. Further, it is explained how network data can be analyzed for both the native port and hardware nodes using a packet analyzer. To conclude the chapter, a clear presentation of the different device types that will be used when constructing the algorithm is also given. (refer algorithm 1)

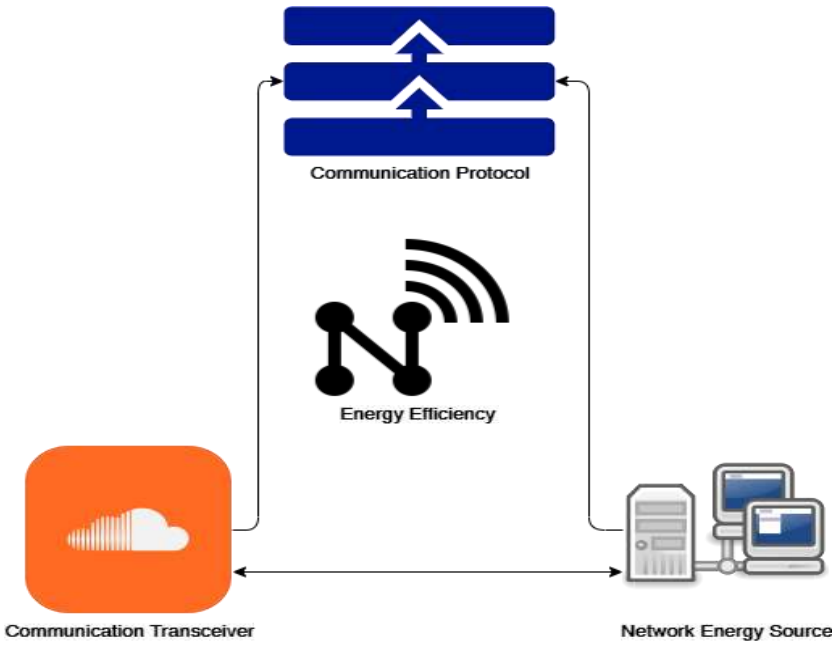

Figure 2.A design of Energy Efficiency Wireless Sensors

3.1. Issues of Medium Access

When operating on the same radio frequency, the installation of wireless devices in the home poses a big problem when they have to wait to reach the network, since they have to control the channel to be capable to transmit data without collisions. To avoid disturbance, the gap b/w the gateway and the distant nodes is minimized by conducting multi-site networks that use fewer resources in information transfer, because the communication will be sent to the closest node. Based on the equipment you are able to utilize various radio channels to reduce contact interruption, the amount of radio channels depends on the system being implemented in the sensor network. To resolve the issue, the optimization of the energy resources in knowledge transmission was suggested by evaluating the lower power usage taking into account the capacity losses in the free room. To reduce the costs of transmitting and retransmitting data, it must be taken into consideration that there is a bandwidth constraint that offers each node and the degree of operation provided by the communications.

3.2 Network Exposure

The wireless networking network comprises of a limited range of sensors with radio interfaces, the same ones used for data acquisition and transmission. The sensors are uniformly dispersed, ensuring complete coverage of the region where they were installed. In order to reduce the transmitting power of all nodes and to allow more excellent coverage of a zone, a node which ensures wireless connectivity to any other nodes could be upgraded into a parent node, and it can receive information of several nodes around the coverage area and rebroadcast to another node so that the data can be transported at the lowest power cost and may be retransmitted to another node.

3.3. Data Generation

Data generation relies on the sampling period optimized in the device so that to enter the network gateway, and there could be several sensors collecting information and transmitting it to their neighbor node. Similarly, the sensors that are in contact bridge with other sensors should have information processed for communicating and must have adequate memory to catch and retransmit the data as well as to transfer the produced data.[1]

3.4 Analyzing Data

Since the virtual TAP interfaces simulate a real network interface, it is possible to use packet analyzers such as Wire shark to analyze the network flow in real-time. In order for Wireshark to be able to parse packets correctly sent over TAP interfaces by RIOT's native nodes, a Wireshark dissector is required1. Analyzing data from real nodes requires a sniffer, which is a node that is able to forward all packets received to another interface. Usually, a serial interface such as USB, which would be connected to a desktop computer where the packets can be analyzed with, e.g., Wireshark. Sniffer software is an essential part of analyzing real network traffic, and software for Sniffer s is included within the Operating Systems Contiki and RIOT. The Sniffer could be put anywhere in the network, but it will only be able to forward packets that it is physically able to receive, making direct communications from far-away nodes invisible to the snifter. Multiple Sniffer s could be used in order to fully cover an extensive 802.15.4 network in order to analyze all packets indicated in figure 3.

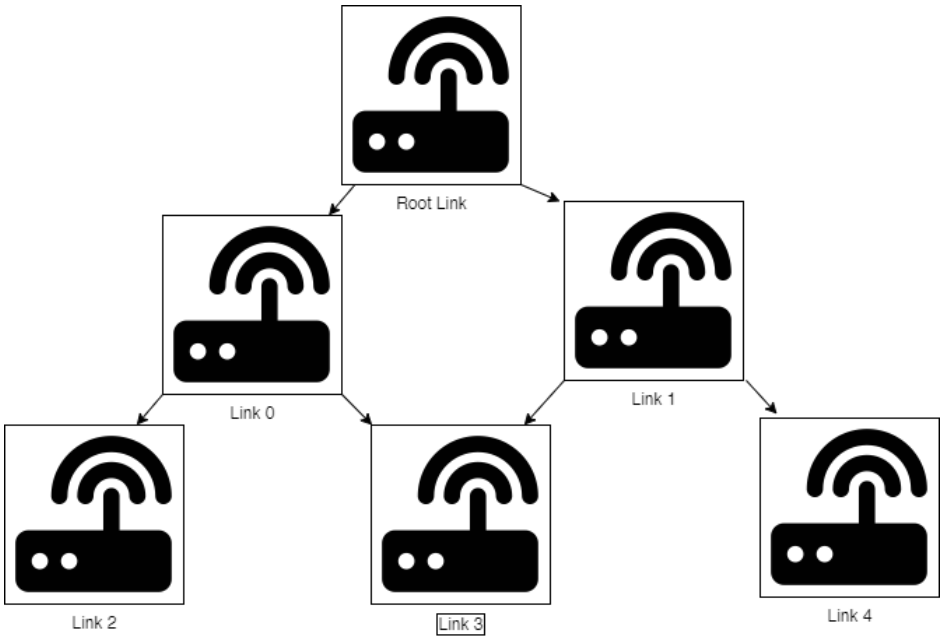

Figure 3. A virtual topology with a customizable link loss rate.

4. Design of the proposed method

As mentioned, the only way to make sure that a node is still functioning correctly is for that node to communicate on the network actively. In the absence of communications from the node, the node will be in an unknown state from the viewpoint of the border router as to whether the node is functional and communicative, or faulty, or in any other way unable to communicate. By using keep-alive messages with associated timers, it is possible to limit the time in which the node is in this unknown state. Timers could be set arbitrarily, and when such a timer runs out, the node could be either assumed non-functional or further actions could be taken to verify its current state in the network. As wireless communications are prone to message loss, it is essential to consider that timers might run out due to delays or interference in the network, which could either be intermittently present or of a more permanent nature.

As for the decision unit (figure 4 and 5), any missed time deadline should be treated as a potential malfunction of the node in question; however, further investigation by the server should be taken to ensure that the node in question is not available, to avoid a potential false positive. Further studies could include an arbitrary number of rounds of keep-alive traffic, during which intermittent delays and interference will have time to recede. One crucial aspect is how an increase in message exchange will affect the overall performance of the network, as a smart home WSN might include many different types of sensors and actuating nodes, which will all share the network with the safety-critical nodes. An aspect such as the power usage of the nodes, the overall throughput, and delays in the network needs to be considered not only for the safety-critical part of the network but for the network as a whole.

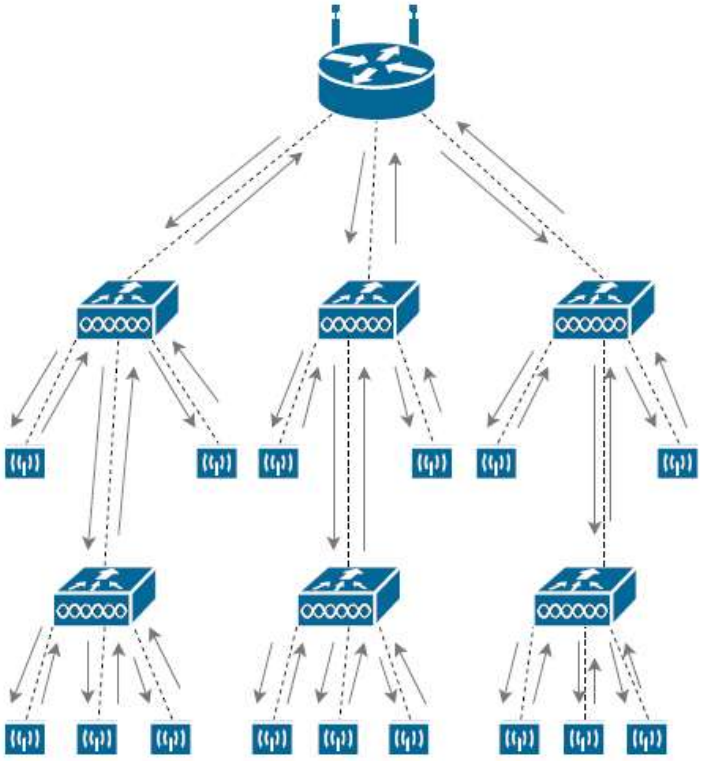

Figure 4. The message flow of WSN

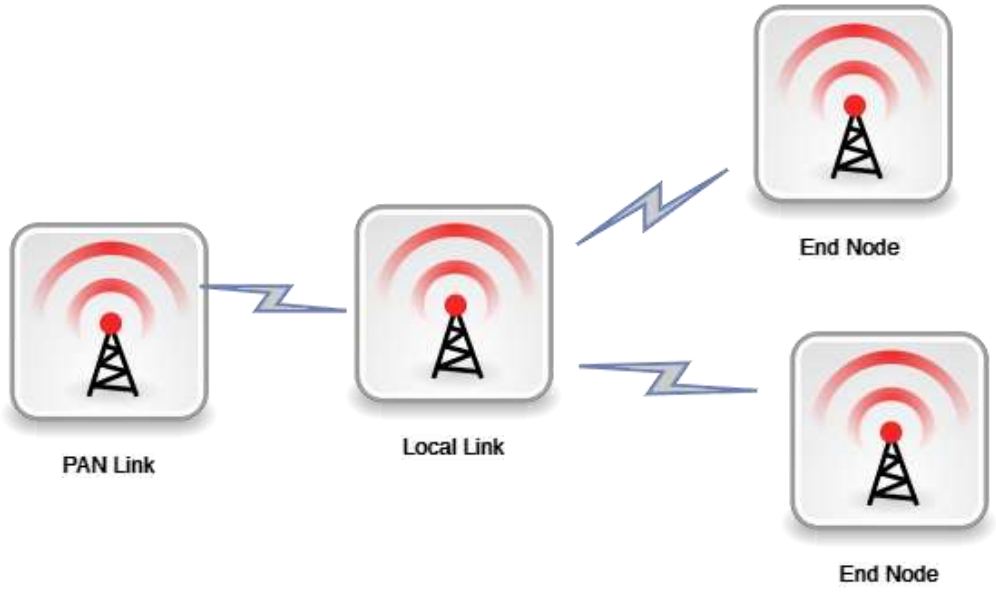

Figure 5. The simulated topology of PANcoordinator

4.1.Algorithm of Optimal Scheduling for WSN in Smart Home

Step 1:

Input:

Nd = Total Nodes

DN_s = Node Distances

D_{xy} = Location Gateway

Max_j = Max No. of Jumps

C_{Node} = No. of Clusters

NXT_{hop} = Vector of Coordinates

BT= Bandwidth

$Frame_T$ = Frame Size

CH_c = Channel Power

Step 2:

For i = 1:N

X_i = Random (1, 2)

Y_i= Random (2, 3)

$Node_{xy} = (X_i, Y_i)$

End For

Step 3:

Compute $DN_{i,j}$

Compute L= *length* (X_s)

Step 4:

While $DN_s < Max_j$ && $NXT_{hop} < DN_s$ **Do**

Delaunay (X_s,Y_s)

For k = 1:N

Travel Cost, Route Path = Dijkstra(G_{xy},X_s,Y_s,,k,Node+1)

If Costs < DN_s && Network Paths > 2

Node€ Network Size

End If

End For

Step 5:

Goto Step 3

Step 6:

For i_i = 1:$Node_{max}$

$C_c=(ST/T)+C_c$

End For

5. Result and Discussion

The simulated topology used for the simulation of the algorithm consisted of the PAN coordinator, from which the algorithm was initiated, a local coordinator, which relayed the keep-alive messages to and from the end nodes. Two end nodes included in the keep-alive algorithm were added to the topology. With this, three links with a statically configured link loss were set up to allow for communications between devices. The links were configured so that the two end nodes would have the local coordinator as their parent, and any message exchange between the PAN coordinator and the end nodes would, therefore, be routed through the regional coordinator as visually in figure 6.

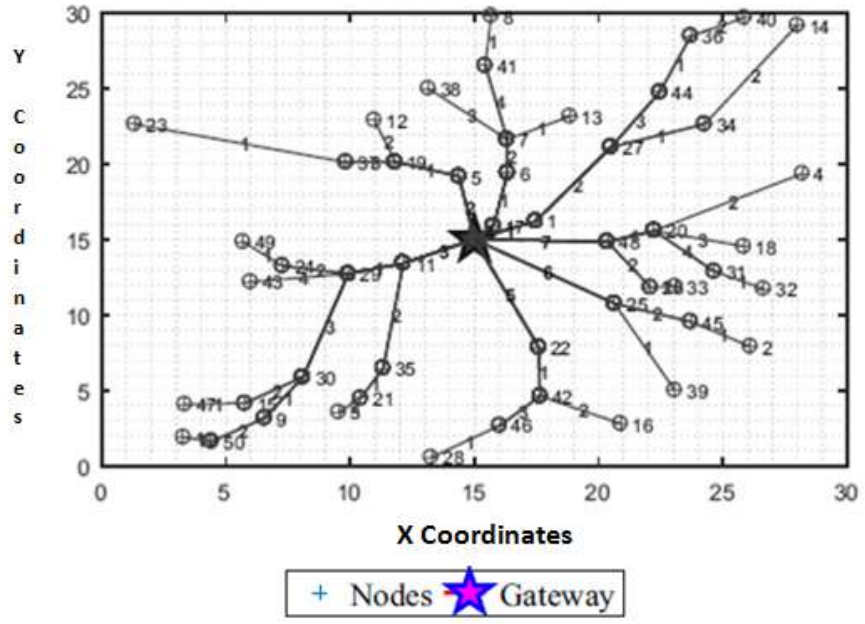

Figure 6. The optimum no. of sensor nodes in the wireless network

Figure 7 shows how the system uses the Electromagnetic Spectrum (ES) more time in a mesh shaped with ten nodes and thirty bytes of details. A domain consumption period of less than one means the domain may be reused.

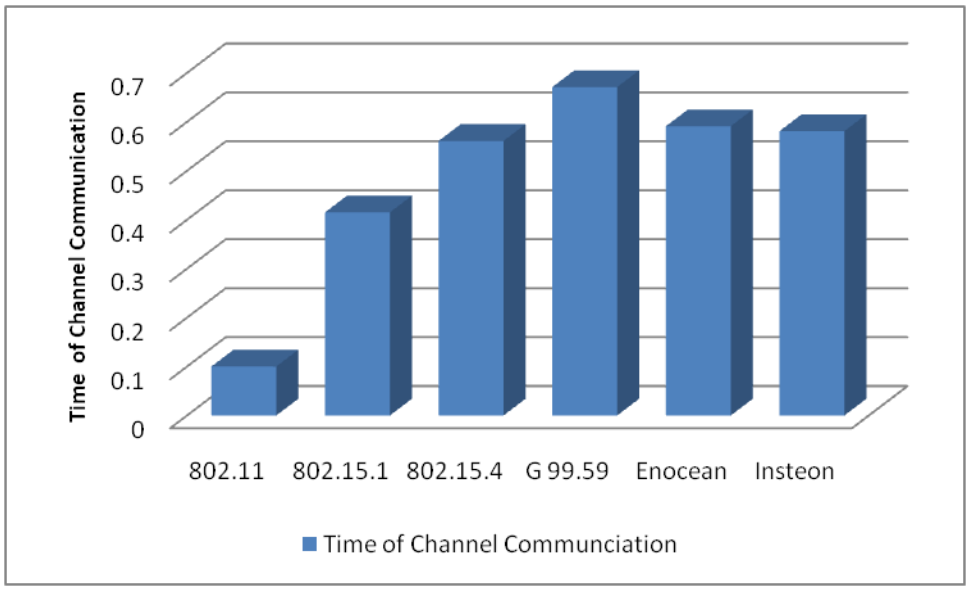

Figure7. Network with 10 nodes Vs. 30 bytes

Figure 8 shows how technology improves the usage of electromagnetic radiation by growing node numbers.

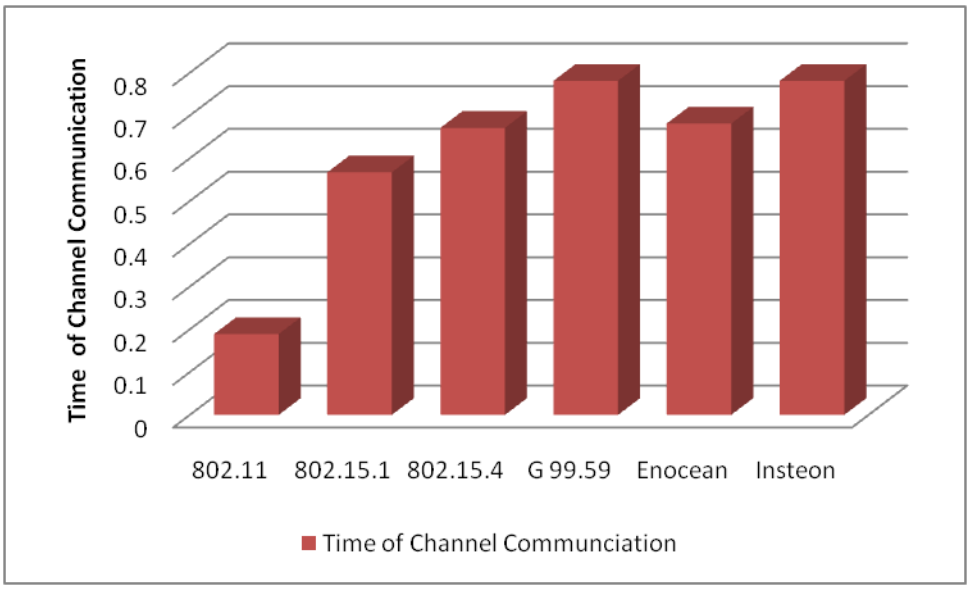

Figure 8. Network with 20 nodes Vs. 30 bytes

Figure 9 illustrates how IEEE technologies are more efficient in the use of the ES and have a large capacity for transmitting lots of information. A channel consumption period higher than one suggests that two or more channels are required for the communications.

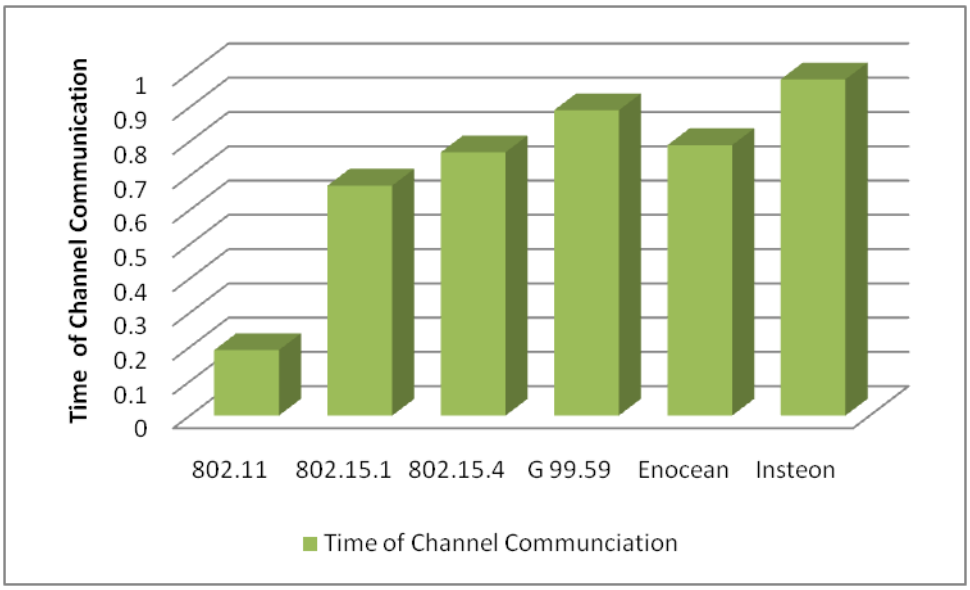

Figure 9. Network with 30 nodes Vs. 60 bytes

5.1 False Positives

The rate of false positives can be calculated, given the number of messages per rounded the static link loss per link as visualized in Figure 10. It shows that given the criteria that the algorithm would be operating in a home environment with a range of 10 to 100 safety-critical nodes present, the rate of false positives quickly becomes intolerable as more links are introduced in the network with the given static link loss of 0.01, 0.02, and 0.05. To combat this, multiple rounds can be executed before a failure is allowed to be acted on, as to limit the number of false positives. Figure 10 shows that the algorithm is vulnerable to scaling, as it only takes one link failure for the whole round to fail. Another angle of attack to minimize the number of false positives is by using subgroups, where the algorithm would run independently for a limited subset of the total amount of safety-critical nodes. In such a case, the rate of failure could be reduced, at the total cost of a few extra messages

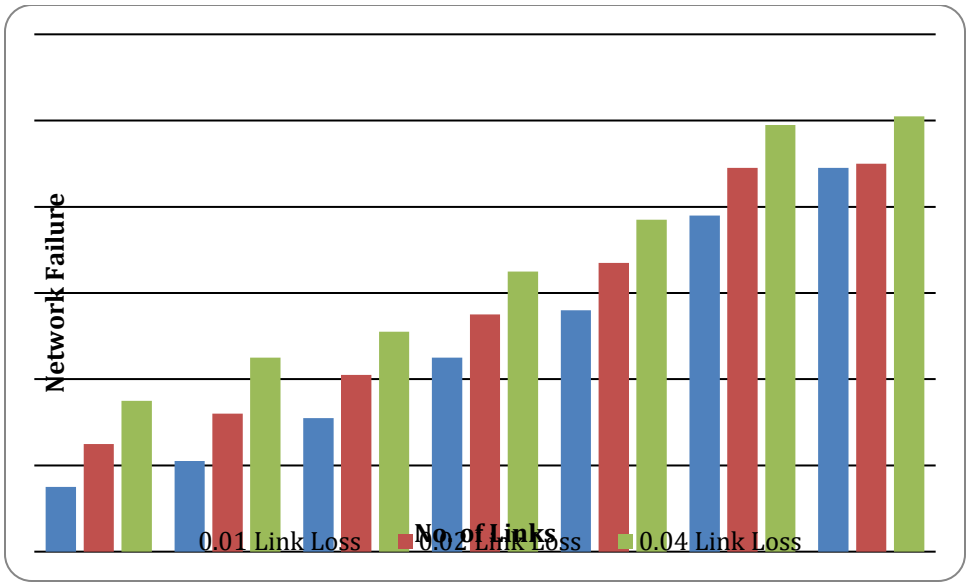

Figure 10. Probability of failed round

6. Conclusions

This paper has presented the issue of keeping a continuously consistent view within WSNs while still trying to adhere to the minimalist and low energy principles of WSN. Conclusions can be drawn from the results of the simulation as to how the algorithm would perform in a real network environment. Other than confirming the functionality and proper implementation of the algorithm, an actual network setup or a more advanced simulation is required in order to analyze the algorithm in a dynamic environment. As such, there are a number of concerns that could not be addressed due to the nature of running simulated nodes in a simulated network environment. The thesis proposes an algorithm that makes use of a round-robin approach where end nodes are relaying a keep-alive message to other end nodes, in order to minimize the number of messages required to keep a continuously consistent view of safety-critical nodes and links. Moreover, authentication was left out in the algorithm that was implemented. As authenticity is of deep concern in order to verify the correctness of received keep-alive messages, it is of high importance that either the algorithm itself can provide the necessary authentication, or that underlying layers are able to offer it. Both wireless technologies tested have the lowest transmitting capacity for Omni-directional wireless coverage of 10 meters. Optimization tests display IEEE 802.15.4 as the most effective norm in the usage of the ES, enabling access to 255 host building networks and being the system that better manages energy usage.

7. References

1. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," vol. 47, pp. 445–487, 2005.
2. M. Vega, F. Santamaria, and E. Rivas, "Modeling for home electric energy management_: A review," *Renew. Sustain. Energy Rev.*, vol. 52, pp. 948–959, 2015.
3. J. Ekanayake and K. Liyanage, *Smart Grid Technology and Applications*, First edit. New Delhi, 2012.
4. D. Nunes, P. Zhang, and J. Silva, "A survey on Human-in-the-Loop applications towards an Internet of All," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 1–1, 2015.
5. P. Guo, X. Liu, J. Cao, and S. Tang, "Lossless In-network Processing and Its Routing Design in Wireless Sensor Networks," *IEEE Trans. Wirel. Commun.*, vol. X, no. X, pp. 1–1, 2017.
6. A.-S. Porret, T. Melly, C. C. Enz, and E. A. Vittoz, "A low-power low-voltage transceiver architecture suitable for wireless distributed sensors network," *2000 IEEE Int. Symp. Circuits Syst. Emerg. Technol. 21st Century. Proc. (IEEE Cat No.00CH36353)*, vol. 1, no. 1, pp. 56–59, 2000.
7. F. Araújo, L. Rodrigues, On the Monitoring Period for Fault-Tolerant Sensor Networks, in: C. Maziero, J. Gabriel Silva, A. Andrade, F. de Assis Silva (Eds.), Dependable Computing, Vol. 3747 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2005, pp. 174–190.
8. H. Liu, A. Nayak, I. Stojmenovic, Fault-Tolerant Algorithms/Protocols in Wireless Sensor Networks, in: S. C. Misra, I.Woungang, S. Misra (Eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, Springer London, 2009, pp. 261–291.
9. K. Sha,W. Shi, On the e_ects of consistency in data operations in wireless sensor networks, in: Parallel and Distributed Systems, 2006. ICPADS 2006. 12th International Conference on, Vol. 1, 2006,
10. S. Rost, H. Balakrishnan, Memento: A Health Monitoring System for Wireless Sensor Networks, in: Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on, Vol. 2, 2006, pp. 575–584.
11. S. Rost, H. Balakrishnan, Memento: A Health Monitoring System for Wireless Sensor Networks, in: Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on, Vol. 2, 2006, pp. 575–584.
12. G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC 4944 (Proposed Standard), updated by RFCs 6282, 6775 (Sep. 2007).
13. O. Hahm, E. Baccelli, H. Petersen, M. Wählisch, T. Schmidt, Simply RIOT: Teaching and Experimental Research in the Internet of Things, in: 13th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN 2014), ACM, Berlin, Germany, 2014.
14. P. Suriyachai, U. Roedig, A. Scott, A Survey of MAC Protocols for Mission-Critical Applications in Wireless Sensor Networks, Communications Surveys Tutorials, IEEE 14 (2) (2012) 240–264.