Topology Experimentation in a Zigbee Wireless Sensor Network

Maria Dimou
TEI of Thessaly
Dept. of Informatics
Larissa, Greece
mariannadi8@gmail.com

Theofilos Kossyvakis
TEI of Thessaly
Dept. of Informatics
Larissa, Greece
theofiloskossivakis@gmail.com

Costas Chaikalis
TEI of Thessaly
Dept. of Informatics
Larissa, Greece
kchaikalis@teilar.gr

Konstantinos P. Tsoukatos
TEI of Thessaly
Dept. of Informatics
Larissa, Greece
ktsouk@teilar.gr

Charalampos Liolios
Public Power Corporation
Lamia, Greece
c.liolios@yahoo.gr

Vasileios Vlachos
TEI of Thessaly
Dept. of Informatics
Larissa, Greece
vsvlachos@teilar.gr

ABSTRACT
In this work, we consider a Zigbee wireless sensor network and study the effect of different network topologies on quality of service metrics such as throughput, end-to-end delay, and packet dropping. A campus building is selected as an experimentation testbed, where several end devices are placed, together with routers and a single coordinator. In this setup, the performance of Zigbee communication protocol was simulated using the OPNET Modeler simulation tool. Measurements of QoS metrics were obtained under different topologies, in order to quantify the complex effects of topology control on aggregate load, throughput, delay, and packet dropping. The results suggest that an increase in the number of routers in the network leads to a significant increase in network load and end-to-end delay, but at the same time offers higher throughput and minimum number of dropped packets.

General Terms
Performance, Design.

Keywords
Wireless sensor networks, ZigBee, Simulation, 5G, OPNET.

1. INTRODUCTION
Wireless sensor networks (WSNs) and 5th generation (5G) systems are predicted to dominate everyday life [1]. Advances in micro electromechanical systems, and low – power integrated digital electronics have enabled the development of wireless sensor networks [2]. These comprise a large number of small battery powered sensor nodes which form a network and after being deployed to the environment they are capable of monitoring environmental conditions such as humidity, temperature, pressure, noise, vibration, etc.

Sensor nodes can be used for continuous sensing, event detection, event ID, location sensing and local control of actuators [3]. Each sensor node typically consists of four sub-units namely the sensor itself, data acquisition system, local microcontroller and radio communication block.

WSNs can be used in virtually any environment, even where wired connection is not possible, or the terrain inhospitable. Their field of applications are [3]: military (monitoring forces, battlefield surveillance, targeting, nuclear biological and chemical attack detection), environment (forest fire detection, flood detection), health (tele-monitoring of human physical data, drug administration, tracking and monitoring doctors and patients in a hospital), home (home automation, smart environment) and other commercial applications (environmental control in office buildings, interactive museums, detecting and monitoring car thefts, managing inventory control).

A WSN has a number of exclusive characteristics when compared with conventional wireless networks, such as limited bandwidth, limited computation capability of individual nodes and limited energy supply [2]. Their small size prohibits the use of long lasting batteries, restricts their bandwidth and transmission ranges, and demands low power processors [3], [4].

In order for these problems to be addressed, many protocols that take into consideration the specific characteristics of the sensors and the applications requirements have been proposed. These can be classified into data centric (Spin, Grab), hierarchical (leach, teen) and location based (Gear, TTDD) [6].

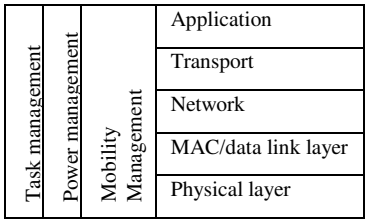

Figure 1: Sensor network protocol stack

PCI '16, November 10-12, 2016, Patras, Greece

DOI: http://dx.doi.org/10.1145/3003733.3003772

The protocol stack of a typical WSN is shown in Figure 1. This combines power and routing awareness, integrates data with networking protocols, communicates in a power-efficient manner through the wireless medium and promotes cooperation among sensor nodes [3].

The architecture of a sensor network typically consists of multiple pervasive sensor nodes, sink, public networks, manager nodes and end user. They communicate with each other through wireless connection in order to form a network, collect, disseminate and analyze data coming from the environment [3].

2. Zigbee Standard

Zigbee is a standard for Low Rate Wireless Personal Area Networks with main features its flexibility, low data rate, low cost and very low power consumption [1]. It is expected to support applications such as remote monitoring, home control and industrial automation [10].

Zigbee is built on the IEEE 802.15.4 standard and specifies the MAC and physical layers. Physical layer supports three radio bands: 2.4 GHz band (Worldwide – 250 Kbps) with 16 channels, 915 MHz band (Americas – 40Kbps) with 10 channels and 868 MHz band (Europe – 20Kbps) with a single channel.

MAC layer controls the access to the radio channel using the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) mechanism. Zigbee's transmission range varies from 1 to 100 m and it can support up to 65536 nodes [12]. Its overall specifications compared with the other wireless transmission protocols are presented in [13].

2.1 Network Components

Each Zigbee network is composed of the following types of nodes [11]:

- Coordinator

ZigBee networks always have a single coordinator device. It is responsible for forming the network, handing out addresses and managing the other functions that define the network.

- Router

A router is a full-featured ZigBee node. It can join existing networks, send, receive and route information. Routers are typically plugged into an electrical outlet because they must be turned on all the time.

- End device

End devices are essentially stripped-down versions of a router. They can join networks and send and receive information. Furthermore, since they do not act as messengers between any other devices, they can use less expensive hardware and can power themselves down intermittently, saving energy by going temporarily into a nonresponsive sleep mode. End devices always need a router or the coordinator to be their parent device.

2.2 Data Layers

Zigbee standard consists of application, network, MAC and physical layers, the use of which offers extremely low cost, easy-to-implement, reliable data transfer, short range operation, very low power consumption and appropriate levels of security [1], [14].

2.3 Topologies

IEEE 802.15.4 supports three topologies, as shown in Figure 2.

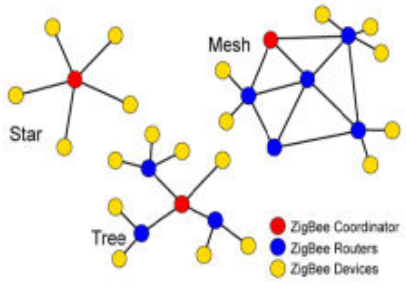

Figure 2: Zigbee topologies

2.3.1 Star Topology

This is a topology where the coordinator is surrounded by a group of either devices or routers directly connected to it. This topology may not be feasible if end devices are located too far to establish direct communication with the coordinator device. In such cases, hierarchical topologies with intermediate relay nodes are needed.

2.3.2 Tree Topology

In a Tree network, a coordinator initializes the network and is the top (root) of the tree. The coordinator can now have either routers or end devices connected to it. Every router node can have many child nodes attached to it. Child nodes do not connect to end devices; they connect to routers who have the ability to relay messages to their destination. The tree topology allows different levels of hierarchy, where the coordinator is at the highest level, and the end devices lie at the leaves. In order for information to reach other nodes in the same network, each source message is continually relayed to a node higher up in the tree, until it can be passed back down to its destination node. Since there is only one potential path between each source-destination pair, this type of topology is also sensitive to path failures. If a router fails, then all of that router's children are cut off from communicating with the rest of the network [15].

2.3.3 Mesh Topology

Mesh topology is the most flexible and robust topology of the three. Robustness is due to the availability of multiple candidate paths that a message can use to travel from source to destination. If a particular router fails, then ZigBee's self-healing mechanism will allow the network to find a suitable alternate path, and route messages along this path [15].

3. SIMULATION MODEL

Metrics such as load, throughput, end to end delay and packets dropped are collectively referred to as a systems quality of service (QoS). There is a substantial need for a realistic simulator that can accurately reflect network performance, so as to provide all the necessary information for the network's actual deployment. For this reason, the OPNET Modeler tool was chosen to conduct the simulation.

3.1 Simulation Scenarios

Simulation experiments were carried out to evaluate various alternatives for wireless sensor network deployment. As an experimentation test bed we selected a particular building sized in 100 m x 70 m, presented in Figure 3. In all scenarios, we placed 37 end devices, routers and a single coordinator all considered

fixed and immobile. Zigbee was chosen as the communication protocol while total simulation duration was set to 10 hours. The purpose of the simulation is to evaluate the QoS offered by the network.

Figure 3: Simulation test bed

3.1.1 1st Scenario

The first scenario consists of 37 end devices divided into 2 clusters depending on their distance from the coordinator. Messages travel from end-devices to routers, and finally to the coordinator, as shown in Table 1.

Figure 4: 1st simulation scenario

Table 1. 1st scenario routing table

Destination	Name	Settings
Router 1	Lect 1A, Lect 1B, Lect 2A, Lect 2B, A1 A, A1 B, A1 C, WC 3, WC 4 Off 1, Off 2, Off 3, Off 4, Off 5, Off 6, Off 7, Door, Hall 1,Hall 2, Hall 3	Default settings
Router 2	Lect 3A, Lect 3B, Lect 4A, Lect 4B, Lab 1A, Lab 1B, Lab 2A, Lab 2B, A2 A, A2 B, A2 C, A2 D, WC 1, WC 2, Hall 4, Hall 5	Default settings
Coordinator	Router 1, Router 2	Default settings

3.1.2 2nd Scenario

This scenario increases the number of routers to four dividing this time our network into four clusters according to the routers number. The topology of the network is shown in Figure 5 while routing is presented in Table 3.

Figure 5: 2nd Scenario

Table 2. 2nd scenario routing table

Destination	Name	Settings
Router 1	Off 1, Off 2, Off 3, Off 4, 0ff 5, Off 6, Off 7, Hall 2, Hall 3	Default settings
Router 2	Lab 1A, Lab 1B, Lab 2A, Lab 2B, A2 A, A2 B, A2 C, A2 D, WC 1, WC 2, Hall 4, Hall 5	Default settings
Router 3	A1 A, A1 B, A1 C, WC 3, WC 4, Door, Hall 1, Hall 6	Default settings
Router 4	Lect 1A, Lect 1B, Lect 2A, Lect 2B, Lect 3A, Lect 3B, Lect 4A, Lect 4B	Default settings
Coordinator	Router 1, Router 2, Router 3, Router 4	Default settings

3.1.3 3rd Scenario

In this scenario, the network gets again divided into two clusters but we add two cluster heads that collect the information provided by each cluster and forward it to the routers and through them to the coordinator (Table 3).

Figure 6: 3rd Scenario

Table 3. 3rd scenario routing table

Destination	Destination	Name
Router 1	Cluster Head 1 – Hall 3	Lect 1A, Lect 1B, Lect 2A, Lect 2B, A1 A, A1 B, A1 C, WC 3, WC 4 Off 1, Off 2, Off 3, Off 4, Off 5, Off 6, Off 7, Door, Hall 1, Hall 2, Hall 6
Router 2	Cluster Head 2 – Hall 5	Lect 3A, Lect 3B, Lect 4A, Lect 4B, Lab 1A, Lab 1B, Lab 2A, Lab 2B, A2 A, A2 B, A2 C, A2 D, WC 1, WC 2, Hall 4
Coordinator		Router 1, Router 2

3.1.4 4th Scenario

Scenario 4 divides our network into four clusters, with a cluster head in each one. The number of routers remains two.

Figure 7: 4th Scenario

Table 4. 4th scenario routing table

Destination	Destination	Name
Router 1	Cluster Head 1 – Hall 3	Lect 1A, Lect 1B, Lect 2A, Lect 2B, Off 1, Off 2, Door, Hall 2
Router 1	Cluster Head 3 - Hall 6	A1 A, A1 B, A1 C, Off 3, Off 4, Off 5, Off 6, Off 7, WC 3, WC 4, Hall 1
Router 2	Cluster Head 2 – Hall 5	A2 A, A2 B, A2 C, A2 D, WC 1, WC 2
Router 2	Cluster Head 4 - Hall 4	Lect 3A, Lect 3B, Lect 4A, Lect 4B, Lab 1A, Lab 1B, Lab 2A, Lab 2B
Coordinator		Router 1, Router 2

3.1.5 5th Scenario

The 5th scenario works as the previous one, the only difference being in the number of routers that is now increased to four.

Figure 8: 5th Scenario

Table 5. 5th scenario routing table

Destination	Destination	Name
Router 1	Cluster Head 1 – Hall 3	Lect 1A, Lect 1B, Lect 2A, Lect 2B, Off 1, Off 2, Door, Hall 2
Router 2	Cluster Head 2 – Hall 5	A2 A, A2 B, A2 C, A2 D, WC 1, WC 2
Router 3	Cluster Head 3 - Hall 6	A1 A, A1 B, A1 C, Off 3, Off 4, Off 5, Off 6, Off 7, WC 3, WC 4, Hall 1
Router 4	Cluster Head 4 - Hall 4	Lect 3A, Lect 3B, Lect 4A, Lect 4B, Lab 1A, Lab 1B, Lab 2A, Lab 2B
Coordinator		Router 1, Router 2, Router 3, Router 4

3.1.6 6th Scenario

In this last scenario we eliminated totally the presence of the routers in our network. The network remains divided into four clusters, with a cluster head in each one that routes the information directly to the coordinator.

Figure 9: 6th Scenario

Table 6. 6th scenario routing table

Destination	Destination	Name
Coordinator	Cluster Head 1 – Hall 3	Lect 1A, Lect 1B, Lect 2A, Lect 2B, Off 1, Off 2, Door, Hall 2
Coordinator	Cluster Head 2 – Hall 5	A2 A, A2 B, A2 C, A2 D, WC 1, WC 2
Coordinator	Cluster Head 3 - Hall 6	A1 A, A1 B, A1 C, Off 3, Off 4, Off 5, Off 6, Off 7 , WC 3, WC 4, Hall 1
Coordinator	Cluster Head 4 - Hall 4	Lect 3A, Lect 3B, Lect 4A, Lect 4B, Lab 1A, Lab 1B, Lab 2A, Lab 2B

4. RESULTS AND DISCUSSION

In order to estimate the potential QoS that can be offered by the network above, we measured the following parameters: Load, Throughput, End-to-end Delay and Packets Dropped.

4.1 Load

Network load refers to the traffic burden on the network and directly affects its performance. Lower load gives faster and more reliable data transmission. As shown in Figure 10, the most suitable solution in our case study with respect to load is the one with no routers and 4 cluster heads. We see that an increase in the number of routers coincides with an increase in the total load of the network.

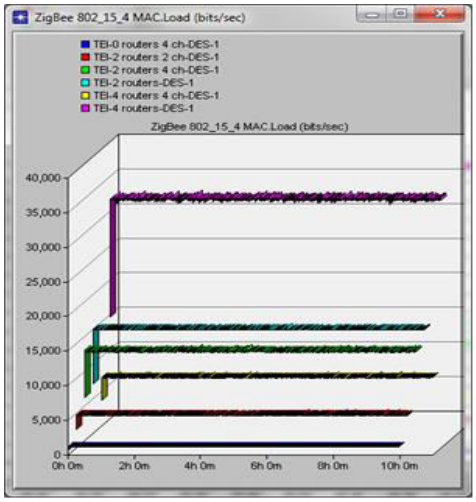

Figure 10: Load vs number of packets

4.2 Throughput

Throughput is the total amount of data received correctly at the intended destination within a specified time limit. Throughput usually depends on many network design aspects, such as topology control, routing policies, scheduling, energy and power control, etc. Figure 11 shows aggregate throughput against the number of nodes for all six scenarios simulated. It can be clearly seen that, contrary to the previous load measurements, a decrease in the number of routers results in a decrease in the data delivered successfully from source to destination, i.e., inferior performance.

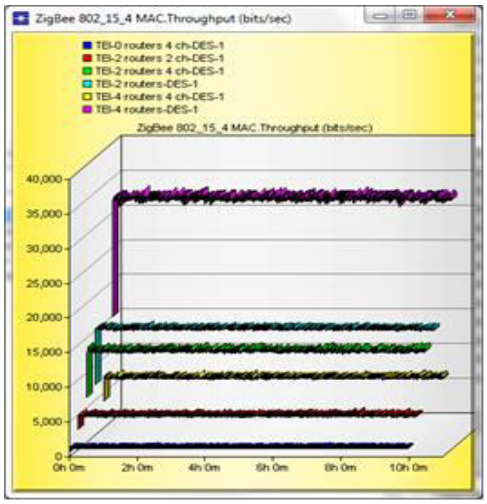

Figure 11: Throughput vs number of packets

4.3 End-to-end Delay

End-to-end delay refers to the delay of a packet in the network, and is measured as the time it takes for a packet to get from its source node to the intended destination. Figure 12 shows the overall end-to-end delay measured for each one of the described scenarios. It is clear that the 6th scenario is the one with the least end-to-end delay in our network, while the other scenarios seem to be barely acceptable, and the 2nd scenario yields unacceptable delay.

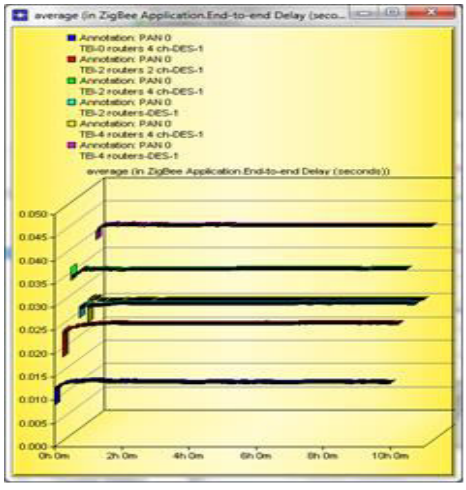

Figure 12: End to End Delay vs number of packets

4.4 Packets Dropped

Packets dropped refer to the amount of data lost while traveling through the network. Information loss is a very significant factor for performance and a key indicator of network QoS. As presented in Figure 13, the 2nd configuration seems to be the best choice for preventing significant packet loss in the network, while the other scenarios share almost the same amount of packets dropped and hence offer the same level of QoS.

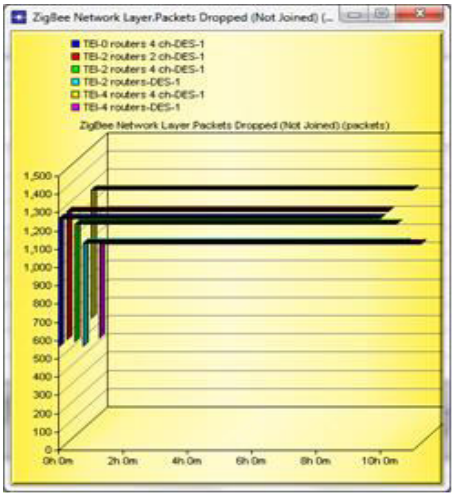

Figure 13: Packets Dropped vs number of packets transmitted

5. CONCLUSIONS

This paper presented an overview on wireless sensor networks that use the IEEE 802.15.4 (Zigbee) protocol and examined the effect of different network topologies on QoS metrics. The results were obtained by simulating and evaluating different WSN topologies using the OPNET Modeler 14.0 simulator.

In order to identify the most suitable solution, we simulated six different scenarios, adding or removing each time significant components of the network. We used a total of 37 nodes, different number of routers each time and a single coordinator. All network nodes were identical and all settings were set to default.

Simulation results show that an increase in the number of routers in the network yields a significant increase in the network load and end-to-end delay, while at the same time offering the maximum throughput and the minimum number of packets dropped.

Future work may examine energy efficient techniques, with emphasis on protocols that will maximize network duty cycle.

6. REFERENCES

[1] Mihajlov B., Bogdanoski M., "Overview and analysis of the performance of Zigbee – Based Wireless Sensor Networks", International Journal of Computer Applications, Vol. 29, September 2011.

[2] Sohrabi, K. "Protocols for self-organization of a wireless sensor network", IEEE Personal Communications 7 (5), pp. 16 – 27, 2000.

[3] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. "A survey on sensor network", IEEE Communications Magazine, 2002.

[4] Park S., Savvidis A., Srivastava M.B., "Simulating Networks of Wireless Sensors", Proceedings of the 2001 Winter Simulation Conference.

[5] Dishongh T.J., McGrath M., "Wireless Sensor Networks for Healthcare Applications", Boston, 2010.

[6] Seah W., Tan Y. K., "Sustainable Wireless Sensor Networks", 2005.

[7] Sinha A. and Chandrakasan A. "Dynamic Power Management in Wireless Sensor Networks", IEEE Design Test Comp., 2001.

[8] Merrett G.V, Al-Hashimi B. M., White N.M., Harris N.R. Resource aware sensor nodes in wireless sensor networks, Journal of Physics, Vol.15, no.1, pp.137 – 142, 2005.

[9] Lattanzi E, Regini E., Acquaviva A., and Bogliolo A., "Energetic sustainability of routing algorithms for energy-harvesting wireless sensor networks", Computer Communications, Vol.30, No.14-15, pp.2976-2986, 2007.

[10] Ding G., Sahinoglu Z., Bhargava B., Orlik P., Zhang Z., "Reliable Broadcast in ZigBee Networks", ", IEEE Transactions on Mobile Computing, Vol. 5, No 11, November 2006.

[11] Faludi R., "Building Wireless Sensor Networks", First Edition, O Reilly, 2011.

[12] Huang M.-C., Huang, J.-C., Jong G.J., "The Wireless Sensor Network for Home-Care System Using ZigBee".

[13] Lee J.-S., Su Y-W., and Shen C.C. "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi", the 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON) Nov. 5-8, 2007, Taipei, Taiwan.

[14] Kinney P., "ZigBee Technology: Wireless Control that Simply Works" Communications Design Conference October 2003.

[15] Leung S., Gomez W., Kim J.J., "Zigbee mesh network simulation using OPNET, and study of routing selection", ENSC 427: Communication Networks, Spring 2009.