



OPTIMIZATION OF LIFETIME IN WIRELESS MONITORING NETWORKS

Yuliia Kovalova ¹⁾, Tetyana Babenko ²⁾, Oleksandr Oksiuk ²⁾, Larysa Myrutenko ²⁾

¹⁾ National TU Dnipro Polytechnic, pr. Dmytra Yavornytskoho, 19, Dnipro, Ukraine, 49000, kovalovajp@gmail.com

²⁾ Taras Shevchenko Kyiv National University, Bogdana Gavrylishina Str., 24, Kyiv, Ukraine, 04116, babenkot@ua.fm, oksiu@ukr.net, myrutenko.lara@gmail.com

Paper history:

Received 21 February 2019

Received in revised form 20 February 2020

Accepted 24 February 2020

Available online 14 June 2020

Keywords:

wireless monitoring networks;
energy efficiency;
network lifetime;
ZigBee networks.

Abstract: Wireless network finds application in communal facilities monitoring and management systems. One of the basic requirements for the construction of a wireless monitoring network with autonomous power supply is the guaranteed network lifetime. Up-to-date challenges in the field of wireless monitoring networks are creation of universal hardware platforms that allow for usage of widespread proprietary transceivers of different manufacturers aiming at creating network topologies raising energy efficiency and lifetime of WMN. The article describes a model of a wireless network allowing evaluation of its lifetime by energy parameters and dynamic reconfigurations induced by external influence.

On the basis of the represented test results one may conclude that energy consumption is defined by the level of the application stack of the protocol ZigBee and doesn't depend on PHY and MAC layers of the protocol 802.15.4. Considering energy consumption of the data transmission process, potential increase in the lifetime of the devices and network as a whole is mostly controlled by the sizes of useful messages.

*Copyright © Research Institute for Intelligent Computer Systems, 2020.
All rights reserved.*

1. INTRODUCTION

Wireless networks for communal facilities monitoring and management systems are among the basic internet technologies on the basis of which a Smart City concept can be developed.

Energy consumption wireless monitoring network (WMN) is a distributed self-configured wireless network consisting of intelligent data acquisition and transmission devices. Each device is equipped with a microcontroller, a transceiver, a battery and it is connected to a meter or sensor through a corresponding interface.

Up-to-date challenges in the field of wireless monitoring networks are creation of universal hardware platforms that allow for usage of widespread proprietary transceivers of different manufacturers aiming at creating network topologies raising energy efficiency and lifetime (standalone downtime) of WMN [1-4]. One of the problems hindering the increase in energy efficiency of WMN is the problem of irregular energy consumption of network nodes. The problem is complex and includes not only network topological peculiarities

but also the realization of security threats at the program level of the used protocol stacks.

The main task for the monitoring networks built on the basis of the ZigBee technology with autonomous power supply is provision of the guaranteed network lifetime during the calibration period of metering devices making up the network.

The simplest possible methods to increase standalone downtime of WMN are the reduction of energy consumption of hardware, optimization of network topology and an increase in the battery capacity.

Wireless network lifetime is directly connected with its energy efficiency. Energy efficiency is often used to specify standards, algorithms and protocols and achievement thereof is one of the basic tasks of technical projects. In other words, longer standalone downtime of WMN in case of full transfer of registered data provides higher energy efficiency. For this reason network lifetime additionally requires service quality assurance that the network should comply with.

ZigBee / 802.15.4 technology was developed to minimize power consumption of devices supporting

the standard. For this purpose the activity of the devices should be minimized so that they could stay in a low-power mode (sleep mode). Consequently a device should 'wake up' (be active) to transfer (or receive) data during a short period of time. The main task is to maximize the battery lifetime of the field devices of wireless energy monitoring system and consequently optimize the lifetime of the network.

During encapsulation of the top-layer packets low-layer packets are supplied with 33 bytes of service information. And the data of application layer in the packet makes up 100 bytes. For this reason the size of the transferred data packets (for instance daily load/consumption curve) and its frequency to a great extent define system lifetime.

It should be taken into consideration when developing a model that would allow wireless sensor network battery lifetime forecasting. To forecast battery lifetime in practical implementation of the network 802.15.4 / ZigBee one should define activity cycles by data transmission as well as the current generated from the battery during different dynamic operation especially during transceiver (main power consumer in devices) activation operations [5, 6].

WMN is a peer-to-peer distributed system whereat every node can exchange data with any of the neighboring one. On the basis thereof there are three basic types of network nodes: an end-user device, a router and a coordinator.

a) An end-user device collects data from meters and sensors and transfers it to the network. As a rule, most of the time it is in the power-down mode, when main power consumers – transceivers – are off.

b) A router relays data coming from end-user devices to the polling point (coordinator).

c) A coordinator (gateway) receives data from the whole network and transfers it to the top-level application through a wire or wireless interface. As a rule a coordinator has a constant power source and unlike other nodes is not restricted in power supply.

The breakdown is used to design centralized monitoring and management systems whereat a coordinator either processes information coming from the whole network itself or transfers it to the device having more resources (for instance, system server) [5].

Main standard that networks are based on being of practical and commercial importance is IEEE 802.15.4 [6, 17]. It describes physical and layer levels of the OSI model [7, 9]. Higher levels come complete in ZigBee specifications [8, 10].

ZigBee specifications regulate such protocol stack, where top-layer protocols use services provided by underlying protocols. Standard IEEE 802.15.4. is used as two low-level protocols (physical layer PHY and MAC layer). MAC-layer in

ZigBee networks realizes CSMA-CA (listening of carrier frequency and elimination of collisions), network layer (NWK) routes messages and APS layer (application support) provides application layer interface. In the context of energy efficiency MAC and NWK layers are of the highest interest.

Sensor network concept involves all nodes using independent power supply. As each network element implements a set of tasks an outage thereof could mean the following: in case the set of tasks realized by the node is not critical it could mean a worse network performance; in case the node is a key system element routing data-flow, an outage and a route change failure thereof could mean the outage of the whole network.

Service quality (QoS) defines if a network can provide required data transmission services under specific conditions.

Unlike classical networks wireless monitoring networks provide not only data transmission services but also data collection and processing. Thus, service quality of the wireless sensor networks and their parameters differ from the classical concept [13, 14].

Quality of service of wireless sensor networks is specified by the following parameters: network delay, network capacity, network losses, network lifetime, specific area coverage and topology variation tolerance [13].

As WMNs are generally autonomous there comes a point when the network is not able to perform its tasks. Time from the start of the network performance to the mentioned point is called lifetime or network standalone downtime (network lifetime).

Temporary worsening of service quality comprises loss of registered data of the invalid node over some time. Thus, the network stops performing its function upon final drop of the service quality.

When solving practical tasks referring autonomous WMN there are two main tasks referring lifetime:

a) Estimation of the assumed network lifetime upon given hardware parameters and operation algorithms

b) Increase of the lifetime applying some methods and algorithms.

2. THE LIFETIME OF WMN

Extension of network lifetime is the general purpose of research on wireless networks as network node is usually constrained by the power capacity that defines its lifetime.

Energy density of a node is defined by the ratio of the total consumed energy to the initial reference energy of the battery. Higher density is achieved by lower ration of the energy used by node operation in a network to its initial energy.

According to the model, total energy consumed includes energy spent for transmitting and receiving of packets, sleep mode and exploration.

Considering numerous models describing relationship of energy consumption with working modes of 802.15.4/ZigBee devices at MAC and NWK specification layers development of realistic model for forecasting lifetime and transmission lags in IEEE 802.15.4 sensor nets, taking into account possible external network influence, are of the specific practical interest.

Thus, energy consumption of nodes to define their lifetime and consequently network lifetime is the key issue in analytical model development.

In the same model of network lifetime forecasting one should take into consideration energy consumption of field devices taking into account sleep-, monitoring-, controlling- and retransmitting modes of field devices due to network disturbances.

Energy losses are classified considering characteristics of wireless communication. The authors [7, 8, 14-16] admit that the most significant losses are suffered by monitoring of networking and retransmission. Active transceiver consumes the same energy volume regardless transmission taking place or not. Collisions happen when many frames are transmitted at the same time. All conflicting packets are retransmitted which results in higher energy consumption and network load.

Another reason for energy losses is monitoring of networking, namely receiving packets destined for other nodes.

To improve networking they apply an addressing scheme that uses transmitting of control packets which results in additional energy losses [9, 19-21].

To save energy MAC protocol should use the minimal possible quantity of control packets.

Main energy losses of fixed networks with ‘meshed’ configuration are caused by data transmitting mode. At the same time energy losses for the first two modes are permanent fixed indices not critical for the network lifetime.

Wireless network of data collection node is considered being operational until it reads sensors and transfers the data to the network without any error. When designing and installing a network, it is important to estimate an approximate lifetime of each node before the change of batteries is required. It is important to understand the factors influencing its standalone downtime.

It is known that energy demand of some network elements depends on the following factors that should be considered by WMN simulation [16]:

a) Hardware characteristics (battery-, microcontroller- and transceiver capacity).

b) Data acquisition and communications frequencies.

c) PHY and MAC protocols defining first of all network access control mechanisms.

d) Logical network topology defining volume of information passing through every element (considering retransmission).

e) Used routing protocol bringing additional maintenance traffic to the network.

DATD (data acquisition and transmission device) is used for reading of meter and sensor indices and transmission thereof to the network.

Its main feature is an ability to support flashlight modes (by sensor actuation) and retranslation (ability for end-to-end transmission of the data, incoming from other devices).

When an event model (flashlight transmission) or a scheduled transmission model is used it usually works according to the cyclic circuit represented in Fig. 1.

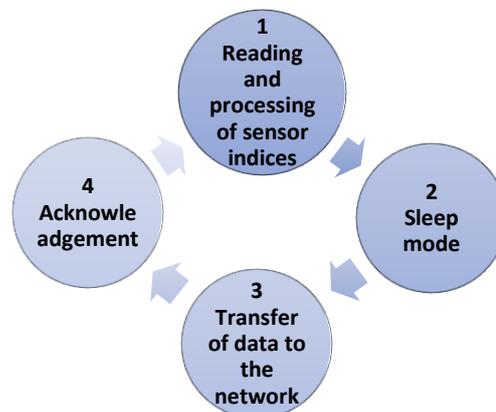


Figure 1 – DATD operation cycle

Considering the fact that the process of reading sensor indices, being one of the key parameters defining DATD lifetime, depends exclusively on the technical characteristics of the used microcontroller, its contribution to the future energy consumption is predictable.

Energy consumption caused by transmit-to-receipt and acknowledgement of data is more critical as for the lifetime as it will be mentioned further.

In practice each transmission through a wireless line is associated with possible losses either by transmission of a frame with a useful load or by acknowledgement.

As a result, the device has to initiate one or several retransmissions delaying the switch to the sleep mode.

3. ENERGY CONSUMPTION TEST

To test DATD energy consumption one could apply a test stand construction scheme comprising usage of the digital oscilloscope UNIPRO V-121. Fig. 2 represents the scheme of measurement of the energy consumption parameters of field devices ‘Sigma ZB’ equipped with the transceivers DIGI and REXENSE in the standard operation mode.

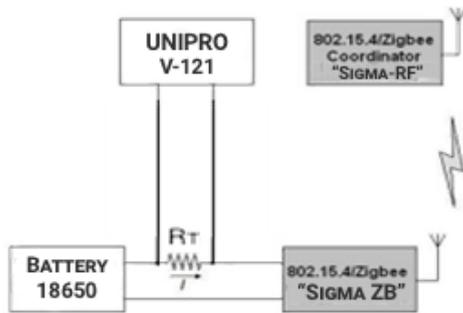


Figure 2 – Scheme of measurement of energy consumption of field devices ‘Sigma ZB’

Based on the Nyquist-Shannon (Kotelnikov) theorem oscilloscope sampling frequency should be two times higher than max frequency of the captured signal.

As min monitoring time slot makes up 200 ms the max sampling frequency should equal 50 kHz.

Test measurement of battery discharging rate is represented below in Fig. 3.

The diagrams above refer to the measurement of energy consumption of the DATD ‘Sigma ZB’ with the installed module XBee rev.b of 1 mW. Considering expected dependence of energy consumption of field devices on the size of transmitted data frames, parameters of different operational modes of network devices, equipped with transceivers DIGI (S1and S2) and REXENSE (REX3D), were measured.

The test was conducted in the medium SCTM-Dialog with the fixation of parameters of transmitted and received packets.

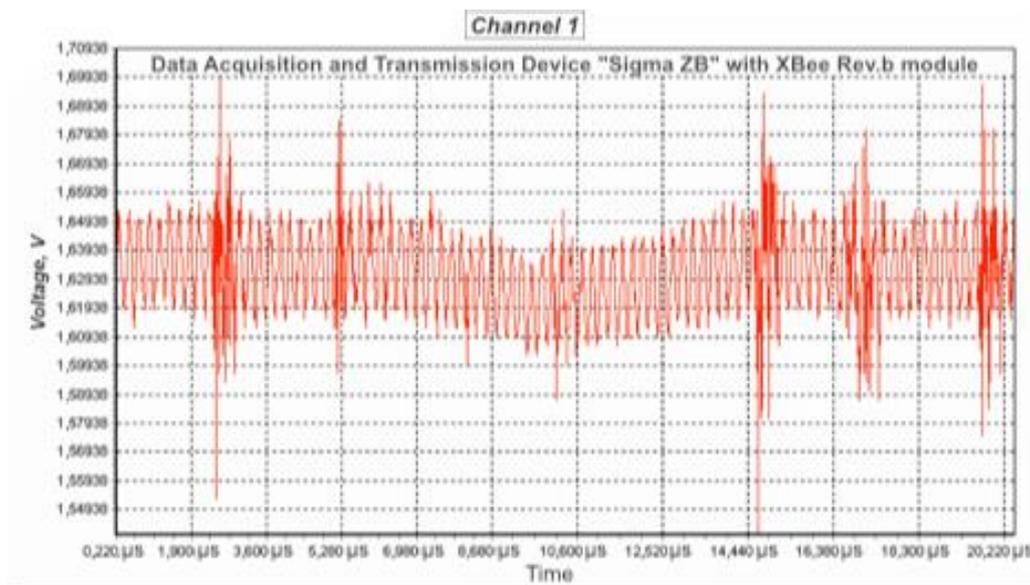


Figure 3 – Measurement of the resistor (shunt) voltage

Based on the known indices of the effective standard deviation of the signal amplitude and resistance of the shunt resistor, effective average current consumption indices of the devices ‘Sigma ZB’ were calculated as follows:

- by the network time synchronization mode and packet size of 56 bite (Table 1),
- by the field device address detection mode and packet size of 34 bites (Table 2),
- by the network addressing mode and packet size of 62 bites (Table 3).

Test value

Module type	Capacity, mW	Standard deviation, mV	Average effective current, mA
XBee rev.b	1,0	2,51	4,14
XBee S2	4,0	25,31	41,77
REX3D	6,0	15,47	25,52

Table 1. Test values

Module type	Capacity, mW	Standard deviation, mV	Average effective current, mA
XBee rev.b	1,0	5,22	8,62
XBee S2	4.0	45,24	74,66
REX3D	6,0	30,14	49,73

Table 1. Test values

Module type	Capacity, mW	Standard deviation, mV	Average effective current, mA
XBee rev.b	1,0	3,44	5,68
XBee S2	4.0	33,89	55,92
REX3D	6,0	20,66	34,09

According to the represented test results one may conclude that energy consumption of a field device depends not much on the capacity of a transceiver as other authors claim, it is defined by hardware interface of a transceiver with microcontroller installed on the field device to provide user functions.

4. CONCLUSION

On the basis of the represented test results one may conclude that energy consumption is defined by the level of the application stack of the protocol ZigBee and does not depend on PHY and MAC layers of the protocol 802.15.4. Due to energy consumption of the data transmission process, potential increase in the lifetime of the devices and network as a whole depends mostly on the control of the sizes of useful messages. Consequently, the crucial task would be the optimization of energy consumption of field devices of self-powered wireless networks in user applications allowing usage of transceivers from different manufacturers in mass data acquisition and transmission devices to design wireless monitoring networks.

5. REFERENCES

- [1] D. J. Malan, M. Welsh, M. D. Smith, "Implementing public-key infrastructure for sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 4, article 22, 23 p., August 2008.
- [2] T. Gao, D. Greenspan, M. Welsh, "Improving patient monitoring and tracking in emergency response," 2005, [Online]. Available at: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.117.1956>
- [3] M. Neugebauer, J. Plonnigs, K. Kabitzsch, "A new beacon order adaptation algorithm for IEEE 802.15.4 networks," *Proceedings of the 2nd European Workshop on Wireless Sensor Networks (EWSN'2005)*, Jan 31–Feb 2, 2005, pp. 302-311.
- [4] X. Ji, H. Zha, "Sensor positioning in wireless ad-hoc sensor networks using multidimensional scaling," *Proceedings of the 23th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'2004)*, Hong Kong, March 2004, pp. 2652–2661.
- [5] N.I. Naumenko, Yu.V. Stasev, A.A. Kuznetsov, "Methods of synthesis of signals with prescribed properties," *Cybernetics and Systems Analysis*, vol. 43, issue 3, pp. 321-326, May 2007.
- [6] IEEE 802.15.4d-2009 standard, Institute of Electrical and Electronics Engineers, 2009, [Online]. Available at: https://standards.ieee.org/standard/802_15_4d-2009.html.
- [7] Y. Semenov, Wireless networks ZigBee and IEEE 802.15.4, [Online]. Available at: <http://book.itep.ru/4/41/zigbee.htm>.
- [8] H. Kwon, H. Seo, S. Kim, B. G. Lee "Generalized CSMA/CA for OFDMA systems: protocol design, throughput analysis, and implementation issues," *Journal of Wireless Communications*, vol. 8, no. 8, pp. 4176–4187, 2009.
- [9] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, "SPINS: security for sensor networks," *Proceedings of the International Conference on Mobile Computing and Networking*, Italy, 2001, pp. 189-199.
- [10] Wei Ye, J. Heidemann and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 3, pp. 493-506, June 2004.
- [11] Y. Wang, X. Liu, J. Yin, "Requirements of quality of service in wireless sensor network," *Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies*, Washington, DC, USA. 2006, pp. 116.

- [12] C. Ramassamy, H. Fouchal, P. Hunel, "Impact of application layers over wireless sensor networks," *Proceedings of the 12th International Conference on Innovative Internet Community Systems (I2CS'2012)*, Trondheim, Norway, June 13-15, 2012 pp. 130-141.
- [13] M. Karpinski, V. Chyzh, S. Balaban, J. Gancarczyk, P. Falat, "Increasing the level of information security in wireless sensor networks by improving their geometric models," *Proceedings of the International 18th Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM'2018*, 2018, vol. 18, pp. 469-476.
- [14] ZigBee Alliance, ZigBee Specification, 2008, [Online]. Available at: https://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/s2011/kjb79_ajm232/pmeter/ZigBee%20Specification.pdf.
- [15] C. Perkins, *Ad hoc On-Demand Distance Vector (AODV)*, C.E. Belding-Royer, RFC 356, July 2003, 37 p.
- [16] J. Balen, D. Zagar, G. Martinovic, "Quality of service in wireless sensor networks: a survey and related patents," *Journal of Recent Patents on Computer Science*, vol. 4, pp. 188–202, 2011.
- [17] ZigBee Alliance, ZigBee specification overview, 2012, [Online]. Available: <http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf>.
- [18] Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4-2003, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), New York, IEEE Press. October 1, 2003, 679 p.
- [19] P. Lin, C. Qiao, X. Wang, "Medium access control with a dynamic duty cycle for sensor networks," *Proceedings of the Wireless Communications and Networking Conference (WCNC'2004)*, Atlanta, GA, USA, March 2004, pp. 1534–1539.
- [20] B. Bougard, F. Catthoor, D.C. Daly, A. Chandrakasan, W. Dehaene, "Energy efficiency of the IEEE 802.15.4 standard in dense wireless microsensor networks: modeling and improvement perspectives," *Proceedings of Design, Automation and Test in Europe (DATE)*, Munich, Germany, March 2005, vol. 1, pp. 196-201.
- [21] A.A. Kuznetsov, Smirnov, A.A., D.A. Danilenko, A. Berezovsky. "The statistical

analysis of a network traffic for the intrusion detection and prevention systems," *Telecommunications and Radio Engineering*, vol. 74, issue 1, pp. 61-78, 2015. DOI: 10.1615/TelecomRadEng.v74.i1.60.



Yuliia Kovalova, Assistant of the Department of Information Security and Telecommunications at The Dnipro Polytechnic University (since 2017). 2009 graduated from the National Mining University (Ukraine), specialty "Management of Information Security" and received a master's degree.

2010-2017 – postgraduate education in the field of information technologies. Areas of scientific interests: IT, Cybersecurity, wireless technologies.



Tetyana Babenko, Dr.Sc. Professor, Professor of the Cybersecurity and Information Protection Department at Taras Shevchenko National University of Kyiv. The main areas of scientific research are intelligent decision support systems in the field of cyber security of assets, problems of synthesis of intel-

lectual models for assessing the security of cybernetic systems, intelligent models of cyber incidents classification.



Oleksandr Oksiuk, Dr.Sc. Professor, Head of Cybersecurity and Information Protection department at Taras Shevchenko National University of Kyiv. The main areas of scientific research are fundamental and applied scientific research related to

development of intelligent systems, logical-linguistic modeling in cyberspace, and the theory and practice of developing automated systems and conducting expert assessments, models, and methods for building an integrated information security system in the context of developing threats.



Larysa Myrutenko, Assistant professor of Cybersecurity and Information Protection Department at Taras Shevchenko National University of Kyiv. In 2017 received a scientific degree of the candidate of engineering sciences in Information Technologies. The

main areas of scientific research are systems of technical information protection, Cybersecurity.