Paweł DYMORA, Mirosław MAZUREK

Politechnika Rzeszowska, Zakład Systemów Rozproszonych

A comparative study of self-adopting fault tolerant protocols in wireless sensor networks

Streszczenie. *Technologia bezprzewodowych sieci sensorowych pojawia się w wielu obszarach współczesnego życia. Ważną rolę w tej technologii odgrywają samoadaptacyjne protokoły poprzez które sieć reaguje na zachodzące w niej zmiany i uszkodzenia, dostosowuje się i efektywnie zarządza dostępnymi zasobami. W pracy przedstawiono analizę porównawczą istniejących rozwiązań w dziedzinie odpornych na uszkodzenia samoadaptacyjnych protokołów. Symulacje realizowano w środowisku OMNeT++. (**Badania porównawcze odpornych na uszkodzenia protokołów samoadaptacyjnych w sieciach sensorowych**).*

Abstract*. Wireless sensor network technology appears in many areas of today's life. An important role in wireless sensor network technology plays self-adopting protocols by which network responds to changes and faults, adapts and effectively manages the available resource. In this paper the comparative analysis of existing solutions in a field of wireless fault tolerant self-adopting protocols is presented. In the research simulation environment OMNeT++ was used.*

Słowa kluczowe: bezprzewodowe sieci sensorowe, odporność na uszkodzenia, samoadaptacyjne protokoły, OMNeT++.
Keywords: wireless sensor networks, fault tolerance, self-adopting protocols, OMNeT++.

doi:10.12915/pe.2014.01.40

Introduction

Owing to the scientific achievements in the field of miniaturization of electronic devices, and the development of wireless communication technologies we can observe the creation of a new type of computer networks, which are wireless sensor networks. These types of networks consist of a large number of small devices equipped with various types of sensors which can be used in many areas of life especially in the areas of critical infrastructures, responsible for warning of the occurrence of fires, tsunamis, landslides or floods is increasingly entering into our daily lives [1, 2, 7]. Possibilities of wireless sensor networks are enormous and their use is limited only by the imagination. In such a structure, there is usually directly defined path providing measurement data to the users. An important role in this class of networks plays self-adopting protocols by which network responds to changes and faults, adapts and effectively manages the available resources. Sensor network in most cases is left itself, the human intervention in network elements after its allocation in the difficult terrain is minimal, the network must be fault tolerant. Ensuring the maximal accessibility is particularly important in those places where any damage does not allow proper work of the whole system or makes the threat to humans. The degradation of the availability characteristics of the sensor network is mainly due to an increase in the number of their components, which at the same time very significantly increases the losses related to the unavailability of its resources. Therefore, to ensure continuous, uninterrupted availability of the resources of this class of systems that guarantee full functionality, it has become a priority for its design and operation [1, 2, 3].

This paper describes the most important feature of wireless sensor networks which is the ability to act independently without human intervention and obtain the highest level of fault tolerance. Fault tolerant self-reconfiguration protocols are interesting field of research and scientific work of scientists around the world. There is many existing protocols which were optimized for traditional wired computer networks but appearing of new technologies such as wireless communication technology and sensor networks made this adopted solution inefficient. Sensor network must respond to changes in topology, which can be caused by network nodes (sensors) failure, lack of energy in the node or electromagnetic interference which in general are new factors unlike for traditional technologies. Therefore, there is a need of optimization of these protocols or creation of a new class of solutions for wireless sensor network protocols. In this paper the comparative analysis of existing solutions in a field of wireless fault tolerant self-adopting protocols is presented. It is the first step towards the creation new optimal fault tolerant self-adopting protocol for wireless sensor networks.

Wireless sensor networks components

Architecture of wireless sensor networks is composed of the measuring nodes, data processing and communication elements that allow users to monitor and react to events and phenomena in a given environment. Thus, we can define four basic components: sensors allocated in a distributed system, internal network connecting the sensors (usually wireless), the central point of grouping information and a set of modules responsible for the processing and exploitation of data. Figure 1 shows the sample sensor network architecture diagram [1, 2, 7, 11].

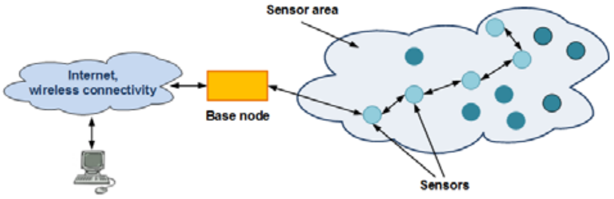

Fig. 1. Sensor network architecture model [1]

As a sensor network node we understand a sensor with integrated controller responsible for the data processing and sending collected information to a central network point via the internal network - usually wireless. Processing units – sensors, have a separate processor, local memory and I/O module. Because sensors do not have a shared memory, they communicate with each other, creating a distributed communication network. The nodes of the given site of action, sends (directly or indirectly) collected and partially modified information to the parent node. Wireless sensor network may consist of a large number of sensors, densely deployed in a given area. When using a fixed logical topology, programmable before physical deployment, we should manually deploy the individual nodes to maintain adequate distance between them. Such situations are rare and used with a small amount of sensors. In most cases, the deployment of network nodes by dropping sensors from a plane over the desired area is used. Also because of individual sensors failure it makes difficult to manually configure logical topology. For this reason, the logical topology of sensor network is constantly changing, and thus its management is a demanding task. The routing protocols deal with that automatically without human intervention. Protocols configure the logical network topology and adapt to the changing number of sensors or a failure in communication between them. The most important design criterion for sensor networks is to determine the high level of reliability (fault tolerance). Due to the nature of the operations, wireless sensor networks are used in difficult and unpredictable environments, where some of the nodes may be damaged, or may be environment interferences or simply a lack of energy which will result in blocking the node action. Destruction of single nodes or groups of nodes in wireless sensor network cannot effect on carrying out the tasks, which involves using a factor that determines the ability to meet desired functions in the network. Such a factor is the fault tolerance, the amount of potential losses in the number of nodes that do not damage the correct and reliable operation of the entire network. Wireless sensor reliability is determined based on the Poisson distribution, equation (1).

$$R_k(t) = \exp(-\lambda_k \cdot t) \tag{1}$$

Is defined as the probability of failure of the sensor node over the time where λ_k is a coefficient of *k* nodes failure at the time *t* [1, 3, 4, 5, 6].

Fault tolerant self-adopting algorithms

A very high self-organization and coordination between all the sensors is required in order to realize all the potential benefits from the use of wireless sensor networks. Routing protocols play a major role here in creating a wireless multihop network that can be self-organized, self-reconfigured and fault tolerant. Sensor networks due to the specific application require specific routing algorithms that are very different from those used in computer wireless networks. Routing protocols for wireless sensor networks can be classified according to three main common features: creation of the transmission path, network structure type and the communication initiator. Categorization according to the formation of the transmission path is divided into protocols: proactive routing protocols, reactive routing protocols and hybrid routing protocols. Classification by the network structure: flat network structure, also known as a unitary structure, hierarchical network and direct network. Another categorization according to the communication initiator: protocols initiated by the source and the protocols initiated by the destination [1, 2, 7, 10, 11].

One of the most important protocols in flat self-reconfigured sensor networks is AODV protocol (*Ad-hoc On-demand Distance Vector*). This protocol is a reactive protocol. Rapidly discovers routes and does not force the network nodes to keep information about inactive sensors. The second protocol is SPIN (*Sensor Protocol for Information via Negotiation*) – it is a reactive routing protocol that extends the classical flooding and gossip about the elements that allow to overcome the defects in these algorithms. In order to improve overlap and implosion SPIN introduces a negotiation. Another important protocol is DSR (*Dynamic Source Routing*). It is a reactive protocol. The main difference compared to the AODV protocol is a way of storing data about the route. AODV in the routing tables store information about the following hops, DSR stores full details of the route from the source to the destination. Other popular protocols: Directed Diffusion, Energy Aware Routing protocol [1, 7, 10, 11].

In a hierarchical sensor networks, we can distinguish the following self-reconfiguration protocols: OLSR (*Optimized Link State Routing Protocol*), LEACH (*Low-Energy Adaptive Clustering Hierarchy*), Teen (*Threshold-sensitive Energy Efficient Sensor Network Protocol*) and APTEEN (*Adaptive Periodic Threshold-sensitive Energy Efficient Sensor Network Protocol*). The most commonly used in this class are OLSR and LEACH algorithms. OLSR is a reactive routing protocol. This protocol creates points responsible for control packets flow on the network which is associated with a significant reduction in the load across the sensor network. Such points are called Multipoint Relays. LEACH protocol divides the sensors into clusters, and then selects the base node that collects data from sensor nodes that belong to the same sensor field. These data are aggregated and sent to the base station [1, 7, 9, 11].

Simulation results of wireless sensor network fault tolerance self-adopting protocols

This chapter presents the results of research and the various simulation runs of the selected fault tolerant self-adopting protocols used in wireless sensor network as also in the MANET networks (*Mobile Ad-hoc Network*). In the test simulation scenarios were implemented illustrating the wireless sensor network reconfiguration capabilities in case of failures and ability to provide operations. The key parameter is the number of sensors and the number of failures in the network. The last simulation component is fault tolerant self-adopting protocol responsible for automatic network routing. In this paper the AODV, DSR, SPIN, OLSR and LEACH algorithms were tested. These protocols have implementations in several programming languages. Their implementations are consistent with specifications such as the ZigBee implementation. To build a sensor network node we use modules implemented in the INET framework of the OMNeT++ (*Objective Modular Network Test-bed in C++*). Tested sensor network is covered with 100, 256, 512 and 1024 nodes, where the allocation was carried out with pre-calculated position, or randomly. For the tests with created simulations a special script was prepared, where the most important parameters were configured as follows: the signal frequency is 2,4 GHz, the signal strength 8mW, 10mW maximum signal strength, base noise 110 dBm, receiver sensitivity -85 dBm, number of a communication channel is 11 (capacity 250 kb/s), battery capacity of 2,5 A, voltage 1,5 V and power consumption while sending 9,4 mA, power consumption while receiving is 1,38 mA, power consumption in standby mode 0,06 mA. First simulation scenario, reflects a motion of a programmed robot (mobile sensor) in the edge of the sensor field where sensor is moving at a speed of 5 meters per second. Data are sent wirelessly through the dynamic route established with the use of the sensors evenly distributed in the area are received by the master sensor, located in the middle of the sensor field. The second implemented scenario shows the communication between two mobile nodes. These nodes move within the sensor field with different speeds and in different directions, sending information between themselves [1].

In order to study the properties of fault tolerant routing protocols to adequately respond to changes in the network topology we focused on the main wireless sensor network characteristics like the minimal and maximal number of hops, the ratio of the amount of all data sent to the all control packets for a sensor field and packet loss.

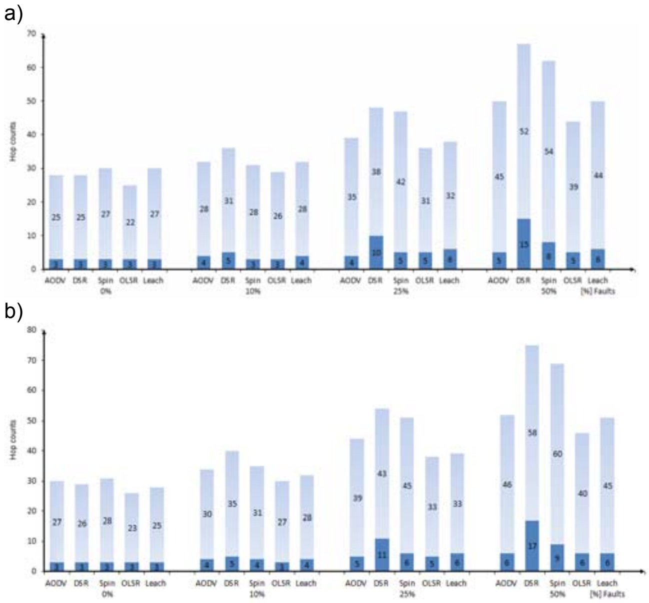

Fig. 2. Scenario 1 - minimal and maximal hops count for a sensor field of 1024 nodes with: a) regular allocation; b) random allocation

As first the minimal and maximal number of hops in the path from a source node to destination node was studied. This parameter is one of the most important coefficients because the smaller the number of nodes on the packets route, the faster data arrives, and less nodes energy resources are consumed. In figures 2a and 2b we can see that all five examined protocols in the scenario 1 with the full network efficiency and in a few cases of a node faults appearance. With the growing number of node failures in the sensor network, the number of hops increases. For a network consisting of 100 sensor nodes regularly allocated, the difference between the maximal and the minimal number of hops is reduced considerably in the event of a greater percentage of node failures.

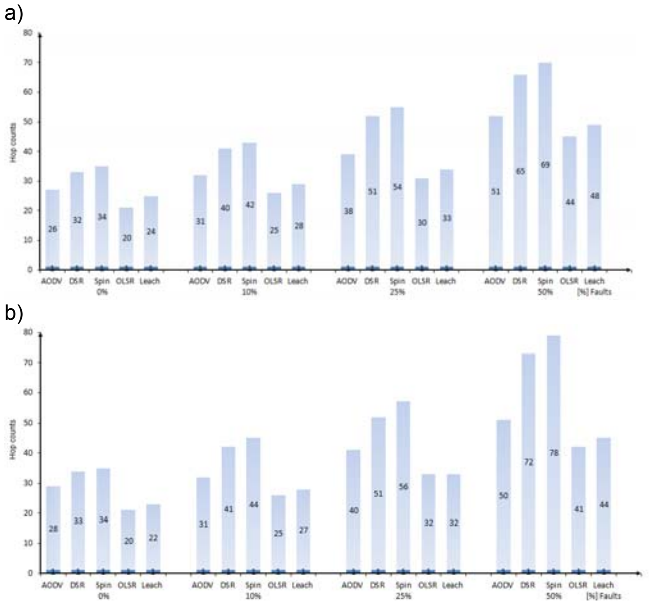

Fig. 3. Scenario 2 - minimal and maximal hops count for a sensor field of 1024 nodes with: a) regular allocation; b) random allocation

For the remaining amount of the sensors in the network, these values remain practically unchanged, only a maximal number of hops is rising. In the network consisting of 1024 sensor nodes, the obtained results are higher by about 100% than in the case of 100 nodes (Fig. 2). Between results obtained for different amount of nodes there was a difference about 20%. Almost in all cases the largest increase in the hops number occurs in the DSR protocol. Protocol OLSR has the least amount of hops. Protocol AODV has a similar minimal hops value as OLSR. Also LEACH protocol has acceptable values. In the case of random distribution (Fig. 2b) of the sensors can be seen an increase in the minimal hops value in correlation to the percentage of node failures. Protocols in the network distributed randomly over such a large area have problems with the correct assignment of optimal routes. For protocol OLSR and LEACH situation looks much better then in case of SPIN and DSR protocols, as the number of nodes in the network increases the situation improves, but hops number are higher than in the case of uniform distribution. The second scenario presents the communication between two mobile nodes in the sensor field. In all cases (Fig. 3a and 3b), the minimum hops count for all protocols, and all scenarios with the different nodes number is always equal to 1 - because moving nodes always pass so close that communication takes place directly between them.

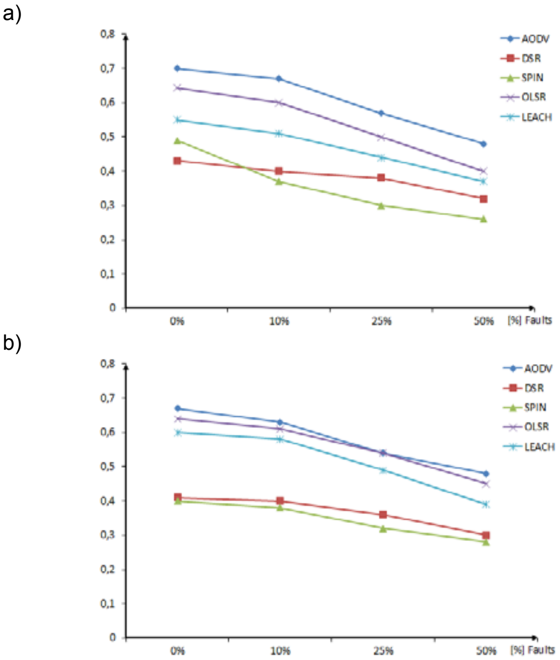

Fig. 4. Scenario 1 - The ratio of the amount of all data sent to the all control packets for a sensor field of 512 nodes with: a) regular allocation; b) random allocation

All other results in all cases for all protocols has generally deteriorated. The values of all protocols in case of random allocation has raised. Also protocols OLSR and LEACH presents the best results whereas SPIN and DSR protocols have higher maximal hops count for a sensor field from 100 to 1024 nodes amount and regular or random allocation pattern. As far we state that proactive hierarchical protocols gain better value of this parameter mainly because of its clustering and regionalization.

An important aspect of the simulation is to study the transmission parameters, which is based on counting packets sent by source node and comparing them to the number of packets that arrived to the destination node. There were counted data of transmission control packets and data packets themselves - which made possible to calculate the ratio of the amount of data sent to the control packets and packets accuracy percent. In addition, the delays on a packets route were measured. In the scenario 1 (Fig. 4a and 4b) - the ratio of the all data packets to the amount of auxiliary protocols packets for the mesh from 100 to 1024 nodes for protocols OLSR and AODV are negligible, while DSR and SPIN protocols significantly differs from the other. The increase in network traffic of control packets is due to the increasing ratio of nodes failure in the network. Using the random distribution (Fig. 4b) at once we can see a change in the ratio of sent data packets to the control packets. For protocols AODV, SPIN and DSR the decline is larger than in the uniformly distributed network topology. But for LEACH and OLSR there is a danger increase. For 100 randomly distributed nodes and the network failure about 50% AODV protocol send control data more than 80% of the overall traffic. By using a larger number of randomly distributed sensors the network traffic relations are improving, but still decrease is greater than using a uniform grid for nodes allocation.

In the scenario 2 (Fig. 5a and 5b) – generally the main trend as in the scenario 1 is also present. All protocols generally has improve their results. Only in the regular allocation the LEACH algorithm has worse characteristics in all testing cases rather than in scenario 1.

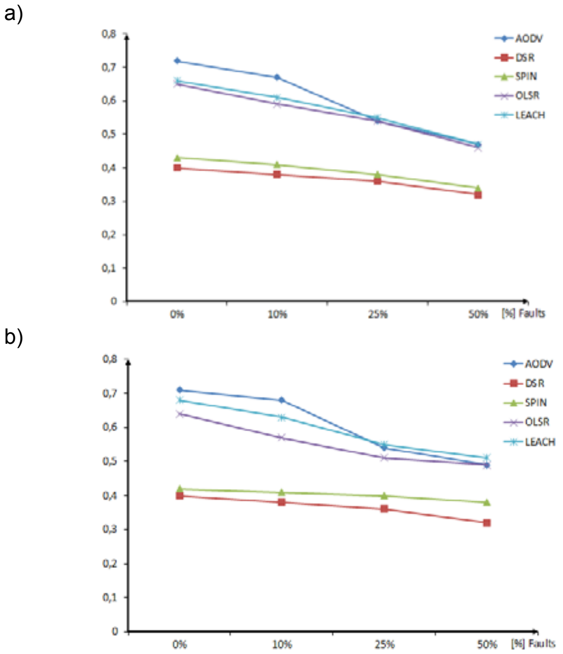

Fig. 5. Scenario 2 - The ratio of the amount of all data sent to the all control packets for a sensor field of 512 nodes with: a) regular allocation; b) random allocation

We can state that the ratio of data packets sent to the control packets in this scenario has improved. Protocols OLSR, SPIN and DSR gained the most when there is not too many damaged nodes. As for effectiveness in the packages delivery, it can be easily seen the improvement compared to the previous scenario.

Conclusion

Previous studies concerning the design and operation of sensor networks especially wireless sensor networks in terms of their availability and reliability, focus on determining the set of alternatives, unrelated physical information transmission path. Using the dynamic routing techniques, defines the current route for the information transport between sensors in the event of any node failure to the selected nodes or communication channels. This assumes that the priority will be to maintain the coherence of the system However, this approach to the problem of providing continuous availability is not without drawbacks because it does not reflect the capabilities of modern communication technology, in particular with regard to the use of multi-channel transmission. Secondly - the use of reconfiguration on a physical level for systems with large size usually does not produce the expected results, it is expensive and difficult to upgrade and providing only communication system coherence in many cases is insufficient. It is also necessary to retain its functional characteristics [3, 4, 6].

The study presented in this paper shows that fault tolerance self-adopting protocols in sensor networks based on clustering and using hierarchy are better than the others what is a good base for future research and development of new protocols. Improving the availability and reliability of a distributed system consenting of many independent sensor nodes can be achieved by the decomposition of the sensor network connecting the region with minimal communication between them and the combined direct connections to transmit information streams with the highest intensity. This is the main research direction for further development of wireless sensor networks in order to ensure the quality of service (QoS) by improving and creating new fault tolerant algorithms for self- adopting sensor networks.

Research carried out on the equipment purchased in the project No POPW.01.03.00-18-012/09 from the Structural Funds, The Development of Eastern Poland Operational Programme co-financed by the European Union, the European Regional Development Fund.

REFERENCES

[1] Dymora P., Mazurek M., Płonka P., Simulation of reconfiguration problems in sensor networks using OMNeT++ software, *Annales UMCS Informatica*, 2013, in printing

[2] Dymora P., Mazurek M., Nieroda S., Sensor network infrastructure for intelligent building monitoring and management system, *Annales UMCS Informatica*, 2012

[3] Hajder M., Dymora P., A novel approach to fault tolerant multichannel networks designing problems, *Annales UMCS Informatica*, 2011

[4] Byczkowska-Lipińska L., Filipiak-Karasińska A., Dymora P., Method of coverage improvement in wireless regional networks, *ECUMIC*, 2008

[5] Hajder M., Filipaik-Karasińska A., Dymora P., The effective coverage in wireless regional networks, *Poznan University of Technology Academic Journals – PWT*, 2007

[6] Krivoi S., Hajder M., Dymora P., Methods For Determining The Fault Tolerance Degree, *ECUMIC*, 2006

[7] Sohraby K., Minoli D., Znati T., Wireless Sensor Networks: Technology, protocols, and applications, *Wiley & Sons*, 2007.

[8] Szymanski B. K., Chen G. Sensor Network Component Based Simulator, *Handbook of Dynamic System Modeling*, 2007

[9] Weingärtner E., H. vom Lehn, Wehrle K., A performance comparison of recent network Simulator, *IEEE International Conference on Communications*, 2009

[10] Raghavendra C., Sivalingam K., Znati Eds T., Wireless Sensor Networks, *Kluwer Academic*, 2004

[11] Varga A., Using the OMNeT++ discrete event simulation system in education, *IEEE Transactions on Education*, 1999

***Authors**: dr inż. Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Rozproszonych, ul. Żwirki I Wigury 2, 35-959 Rzeszów, E-mail: PDymora@prz.edu.pl; dr inż. Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Rozproszonych, ul. Żwirki i Wigury 2, 35-959 Rzeszów, E-mail: MMazurek@prz.edu.pl.*