Iwona GROBELNA, Agnieszka WĘGRZYN
UNIWERSYTET ZIELONOGÓRSKI, INSTYTUT INFORMATYKI I ELEKTRONIKI

Usage of Wireless Sensor Networks in Safety Control Systems

Mgr inż. Iwona GROBELNA

Ukończyła studia na Wydziale Elektrotechniki, Informatyki i Telekomunikacji Uniwersytetu Zielonogórskiego. Absolwentka Zintegrowanych Studiów Zagranicznych Uniwersytetu Zielonogórskiego i Fachhochschule Giessen-Friedberg (Niemcy). Tematem pracy magisterskiej było zarządzanie danymi w bezprzewodowych sieciach sensorowych. Obecnie jest studentką studiów doktoranckich.

e-mail:I.Grobelna@weit.uz.zgora.pl

Dr inż. Agnieszka WĘGRZYN

Adiunkt w Instytucie Informatyki i Elektroniki Uniwersytetu Zielonogórskiego. Zainteresowania naukowe obejmują: modelowanie i weryfikację układów sterowania opisanych sieciami Petriego, formalne metody specyfikacji algorytmów sterowania, bazy danych oraz aplikacje internetowe.

e-mail:A.Wegrzyn@iie.uz.zgora.pl

Abstract

Wireless Sensor Networks can be used in safety of control systems. An example of such a system can be a distributed control system, which involves also reconfigurable logic controllers RLC based on FPGA structures, local databases and application with superior database. System based of three layers enables its flexible scalability. The proposed system can be used in industry (e.g. for controlling of production processes), but also in today's life (e.g. for buildings monitoring).

Streszczenie

Bezprzewodowe sieci sensorowe mogą znaleźć zastosowanie jako zabezpieczenie systemów sterowania. Przykładem takiego systemu może być system rozproszonego sterowania, w skład którego wchodzą także rekonfigurowalne bezpieczne sterowniki logiczne RLC na bazie elementów FPGA, lokalne bazy danych oraz aplikacja programowa z nadrzędną bazą danych. Trójwarstwowość systemu umożliwia łatwą jego skalowalność. Zaproponowany system może być wykorzystany w przemyśle (np. przy nadzorowaniu procesu produkcji), jak również w życiu codziennym (np. do monitoringu budynków).

Keywords: Wireless Sensor Networks, distributed control systems, safety systems.

Słowa kluczowe: bezprzewodowe sieci sensorowe, rozproszone systemy sterowania, systemy o podwyższonym bezpieczeństwie.

1. Introduction

In the paper, an distributed control system is presented [1], focusing especially on Wireless Sensor Network (WSN) as its part. The system consists of three layers. The first layer is an application with main (superior) database. The second layer are local databases. The third layer consists of two independent sets – reconfigurable logic controllers (RLC) and sensor nodes. Schema of the distributed control system is presented in Fig. 1.

The first layer is an application available via Wide Area Network. It allows user to choose an appropriate control program. Application modifies data in superior database. On the second layer there are local databases that store information about planned control programs. Using mechanisms available in DBMS, they communicate with superior database and particular RLC controllers.

As the third layer there are RLCs and sensor nodes. RLCs are based on FPGA structures, and they can be reconfigured. Sensor nodes build together a Wireless Sensor Network. They sense the surrounding world and in case of observing some abnormal situations (invalid values) they send appropriate information to the local database using wireless communication. As the result the appropriate logic controllers are reconfigured, what either solves the problem completely or at least prevents the problem from getting more serious. Using at the same time control processes visualization editor, described in details in [2], cooperating with local database it is possible to control normal work of the system. The visualization editor is a comfortable connector between user and physical components. Additionally, it could be possible to monitor on-the-fly dangerous situations basing on particular sensors readings.

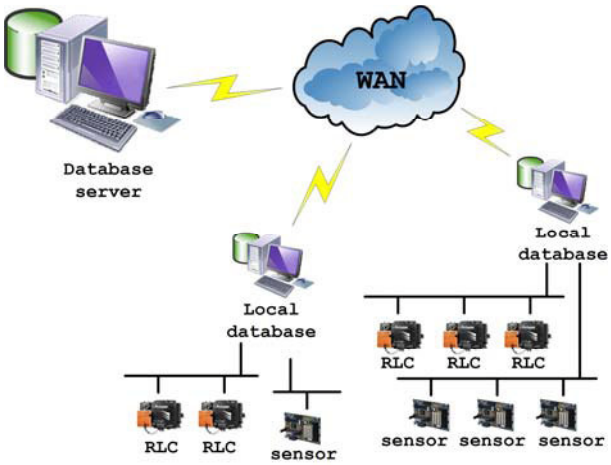

Fig. 1. Schema of the distributed control system
Rys. 1. Schemat rozproszonego systemu sterowania

The proposed distributed control system can be used as high reliability system with an immediate response to any alarm situation. In the paper the usage of Wireless Sensor Networks as safety mechanism in the sample distributed control system is discussed.

2. Wireless Sensor Networks

Wireless Sensor Networks were considered in [6] as one of the technologies that will have enormous influence on the future and will change the world. Nowadays, they are becoming a popular general available technology. They can be used in industrial, business, healthcare [11] and military systems, as well as in monitoring of environmental phenomena [8, 12] or emergency and disaster scenarios [3, 9, 10, 13]. They consist of tiny low-power wireless devices (called also *sensor nodes* or *motes*), which in turn are built of sensing unit, processing unit, power unit and transceiver [4]. A construction of sensor network component is presented in Fig. 2. Sensing unit includes different sensors that sense the vicinity and produce electrical response to some changes in the physical environment.

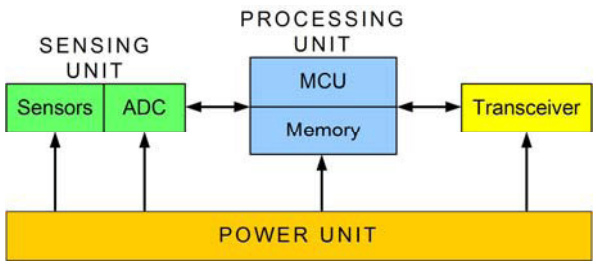

Fig. 2. Construction of sensor network component.
Rys. 2. Budowa węzła bezprzewodowej sieci sensorowej.

Processing unit can include a microcontroller, microprocessor or even a field-programmable gate array (FPGA) [7]. Using sensor nodes with FPGA-based processing unit it is possible to reprogram or to reconfigure the device during system deployment and to adapt it to changing requirements. The disadvantage is that they consume much more energy than motes with other type of processing unit. Power unit can include rechargeable or non-rechargeable batteries, in many cases energy source is a pair of AA batteries. Size of power supply often influences size of a sensor network component.

The communication can be realized in different ways, like by using optical communication (laser), infrared, ultra-sound communication for underwater applications or radio-frequency (RF). Each of the possibilities has another advantages and disadvantages und choosing an appropriate communication method depends on the particular usage scenario. More information can be found in [7].

Motes can sense the surrounding world, store measured values in the local memory or send it to the specified receiver using wireless communication protocols. Measured values (for example temperature, chemical presence, weight, light, position, vibration or sound) may indicate some abnormal state, if they exceed the previously defined values.

Wireless Sensor Networks have an enormous advantage in comparison with "Wired Sensor Networks". They can be namely embedded in the physical environment without any additional infrastructure. It is very comfortable especially in situations when wiring would be too costly, could not reach the specified points or would limit system flexibility [5], like by building a system working over a large area or in case of extending an already running system.

There exists a scenario for gathering information from all motes in one place – it is a sink-based solution. Sink is a place where the Wireless Sensor Network connects with an external file system or an external database [14].

3. Usage of Wireless Sensor Networks in distributed control system

Wireless Sensor Networks can be placed in the third layer of distributed control system. The system requires high reliability so the design process for particular usage scenario must be performed very carefully. Authors of [4] report some categorisation methods of sensor network applications. Using the traditional categorisation that defines eight types of applications, the proposed solution fits into the *Industry & Business* group and *Smart Home / Office / Classroom* group.

In the distributed control system an *Event detection* pattern specified in [14] for interaction between sources and sinks can be used. Sensor network components are sources and local database is a sink. Sensor nodes communicate with the sink only when they detect the occurrence of a specified event. This pattern allows to save valuable energy and does not cause communication overhead.

A sensor node measures synchronously the attribute (like temperature or light). Time intervals between measurements depend on particular attribute type and particular usage scenario. If the measured value is in the range of allowed values, a mote does not do anything, it neither transmits it to the sink nor stores it in the local memory. But in the situation when the value exceeds the previously defined allowed values, the mote transmits it to the sink and additionally stores it in the local memory (i.e. Flash memory). Such a behaviour allows to save the energy and does not cause much communication traffic. It is better to communicate only in abnormal situations than to transmit each time some data as the total amount of transmitted data in the sensor network can be enormous and communication dominates the energy budget of a sensor node. On-mote values storing, which indicate some abnormal state, does not consume much energy and can be treated as an additional backup place with information. In case when the database will be corrupted, all history information in it would be lost. However, there would still be a possibility to restore the information basing on data kept in the local memory of the sensor network components.

Sensor nodes have restricted energy and computing power. However, this usage scenario enables a mote to run for a long period of time. In the simply mode (detecting alarm event basing on one measured attribute from any of the motes) there will be no complex operations (the only one is the comparison of two values) and communication will be limited to minimum (only abnormal situations). Energy constraints may also be overcome, because in some of the situations it will be possible to change or recharge the battery – points where motes are placed are well known to the user and are often accessible. If there will be some inaccessible or dangerous places, special self-rechargeable batteries scavenging energy from the environment can be used [15]. Potential energy sources can be for example solar cells for indoors and outdoors use, vibrations, wind or air flow, naturally occurring temperature gradients.

If some anomalies will be detected, sensor node sends a warning to the local database. The information is then stored in the local database and in the main (superior) database. As a response, the local database sends data to the appropriate reconfigurable logical controller RLC (as a bit stream file) to reprogram it. The immediate reaction is supposed to stop the dangerous process and save people, animals or machines from being injured or corrupted. All alarm situations and performed operations can be presented to the user by visualization editor. Detected events can be marked on the screen by red colour and additionally make the computer produce some sound as they deserve special attention. The schema of communication inside the distributed control system is presented in Fig. 3.

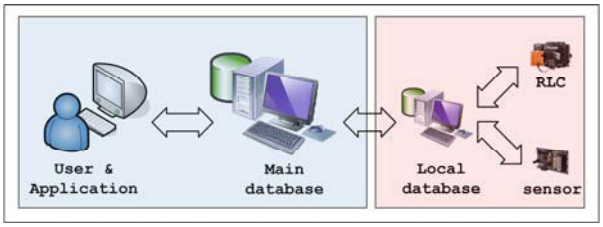

Fig. 3. Schema of communication inside the distributed control system.
Rys. 3. Schemat komunikacji w rozproszonym systemie sterowania

There is also a possibility to detect more complex anomalies basing on different attributes values, i.e. temperature, light and sound for detecting explosions. If all sensors necessary to recognize some abnormal situations are placed on one sensor network component then the processing unit evaluates the situation basing on sensors readings (operations like adding, subtracting, multiplying and dividing of numbers have to be performed). However the amount of different sensors on one mote is limited and in some cases sensors have to be placed in different remote places. Then distributed data processing can be performed and sensor nodes have to cooperate with each other to decide whether something abnormal has happened or not. By specifying the mathematical formula(s) for detecting an event Wireless Sensor Network designer has the possibility to specify the weight (importance) of particular attributes and the sensitiveness of the whole safety system.

In another situation, measurements of one attribute from different remote places are required to raise an alarm. As an example, a storage reservoir controlling water level in the further part of the river with a dam can be taken. On the storage reservoir banks there can be placed umpteen sensor network components equipped with humidity sensors which detect water level but are insensitive to increased humidity caused by rain. Couple of sensor nodes can become wet due to unpredictable animals movements or waves caused by strong winds. However these accidents should not influent the system functionality. If the amount of motes that detected the event exceeds the previously defined number (i.e. 75% of all sensor networks components) what indicates that water level has indeed increased, appropriate alarm message is sent to the lo-

cal database and as the result reconfigurable logic controllers controlling the dam will be reprogrammed. Consequently some volume of water will flow from the storage reservoir into the further part of the river decreasing water level in the reservoir. In this situation sensor nodes have to cooperate with each other and the common data should be processed.

4. Ensuring of reliability and robustness in Wireless Sensor Network

Security in Wireless Sensor Network is an important issue that has to be taken into account especially in real-time control systems. The system has to provide high reliability and be robust to potential threats. Messages are sent only in abnormal situations which do not happen often, but they are critical to the system and may change system behaviour. This is why they have to be delivered immediately.

First of all physical security of sensor network components should be ensured. In some usage scenarios sensor nodes are placed in safe and supervised points. In other scenarios they should be placed in hidden and hard accessible points so that they are invisible for a casual human being. This will make difficult for a potential attacker to destruct or hijack sensor network components.

Attackers may use different techniques to manipulate system functionality. One of them is eavesdropping where an attacker intercepts messages and analyzes them. Geographical distribution of sensor nodes simplifies it. Retransmitting intercepted messages any time later may cause false alarm. Dangerous situation is also a disruption. Semantic disruption involves injecting messages or corrupting sent data. This may lead to very dangerous situations when information about detected event will be delivered to the sink in corrupted form (shortened, lengthened or with changed bits). The message will not be correctly analyzed in database and none of further operations will be performed what may lead to physical destruction of machines or injury of people. Similar consequences may also have physical disruption when attacker directly manipulates the environment in the vicinity of sensor node. It may cause either false alarm and unreasonable reprogramming of reconfigurable logic controllers or not reported abnormal situation.

More information about security in Wireless Sensor Networks can be found in [16].

5. Conclusions

Wireless Sensor Networks are well-suited to be a safety support in real-time control systems. In the paper, a proposal of using WSN in distributed control system together with reconfigurable logic controllers. Sensor network components are placed in fundamental important points for recognizing dangerous situations. If something incorrect (abnormal) happens, sensor nodes detect it and send information to the local database and as the result appropriate RLC controllers will be reprogrammed what will change system behaviour.

Sensor nodes have limited resources but in the proposed solution it is not a big problem. Wireless communication, that is very energy-consuming, is performed only in case of detected events which are supposed to happen hardly ever. However, communication in Wireless Sensor Networks is not always one-hop communication when a node sends a message directly to the sink (local database). In scenarios, where motes are scattered over an large area, multi-hop communication has to be performed what means that multiple sensor nodes have to take part in transmitting of information. In usage scenarios with umpteen sensor nodes and events, based on multiple sensors readings motes, have to cooperate with each other. In both situations, they have to listen at regular time intervals, whether some other nodes have broadcasted any messages. It is also important that the Wireless Sensor Network is self-organizing what means that in case of any node's failure it will not influence system functionality and it will be still possible to transport the message to the sink using another way. Sensor network components may be powered by self-rechargeable batteries scavenging energy from the environment, what will lengthen their lifetime. If this kind of energy source is unavailable the problem can be solved by introducing an additional message type including mote's energy level sent regularly to the local database, e.g. every week.

An important aspect is to secure the sensor nodes and communication between them to ensure high reliability and system robustness. Attacker may change the system behaviour by directly manipulating sensor network devices or the environment in the closest vicinity of them. This may lead either to false unreasonable alarms or to unnoticed abnormal situations. Both cases are dangerous to the system and may cause serious damages, casualties or even a catastrophe.

6. References

[1] Węgrzyn A.: Application of databases for management of distributed control systems, Discrete-Event System Design 2006, A Proceedings volume from the IFAC Workshop, DESDes'06, Rydzyna (Polska), Adamski M., Gomes L., Węgrzyn M., Łabiak G. (Eds.), 26-28.09.2006, Zielona Góra University Press, Zielona Góra, 2006, 263-268.

[2] Węgrzyn A., Jóźwiak I.: Visualization of control processes by means of Petri nets and database, Proceedings of SPIE, Vol.6347, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2006, Romaniuk R.S. (Ed.), 2006, 63472P1-8.

[3] ALERT System, http://www.alertsystems.org (last viewed: 2008-01-06)

[4] Khemapech I., Duncan I., Miller A.: A Survey of Wireless Sensor Networks Technology, Proceedings of the 6th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting, PGNET, Merabti M.,Pereira R., (Eds.), EPSRC, Liverpool, UK, 2005, 26-31.

[5] Karl H., Willig A.: A short survey of wireless sensor networks, Technical Report TKN-03-018, Telecommunication Networks Group, Technische Universität Berlin, 2003.

[6] Technology Review, Ten Emerging Technologies That Will Change the World, www.technologyreview.com, 2003.

[7] Vieira M.A.M, Coehlo C.N. Jr., da Silva D.C. Jr., da Mata J.M.: Survey on Wireless Sensor Network Devices, Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation, ETFA '03, Vol.1, 2003, 537-544.

[8] Mainwaring A., Polastre J., Szewczyk R., Culler D., Anderson J.: Wireless Sensor Networks for Habitat Monitoring, Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications. WSNA'02, ACM Press, New York, 2002, 88-97.

[9] Mehta P., Chander D., Shahim M.., Tejaswi K., Merchant S.N., Desai U.B.: Distributed Detection Strategies for Landslide Prediction using Wireless Sensor Network, Proceedings of the IEEE Global Information Infrastructure Symposium, GIIS 2007, 2007, 195-198.

[10] Werner-Allen G., Lorincz K., Johnson J., Lees J., Welsh M.: Fidelity and Yield in a Volcano Monitoring Sensor Network, Proceedings of the 7th USENIX Symposium on Operating Systems Design and Implementation, OSDI'06, 2006, 381-396.

[11] Patel S., Lorincz K., Hughes R., Huggins N., Growdon J.H., Welsh M., Bonato P.: Analysis of Feature Space for Monitoring Persons with Parkinson's Disease With Application to a Wireless Wearable Sensor System, Proceedings of the 29th IEEE EMBS Annual International Conference, Lyon, France, 2007.

[12] Juang P., Oki H., Wang Y., Martonosi M., Peh L., Rubenstein D.: Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet, Proceedings of the Tenth International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS'02, 2002, 96-107.

[13] Hartung C., Holbrook S., Han R., Seielstad C.: FireWxNet: A Multi-Tiered Portable Wireless System for Monitoring Weather Conditions in Wildland Fire Environments, MobiSys'06, 2006.

[14] Karl H., Willig A.: Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons Ltd., 2005.

[15] Roundy S., Steingart D., Fréchette L., Wright P.K., Rabaey J.M.: Power Sources for Wireless Sensor Networks, Proceedings of the First European Workshop on Wireless Sensor Networks, EWSN'04, Holger K., Willig A., Wolisz A. (Eds.), Lecture Notes in Computer Science, Vol. 2920, Springer, Berlin, Germany, 2004, 1-17.

[16] Anand M., Cronin C., Sherr M., Blaze M., Ives Z., Lee I.: Sensor Network Security: More Interesting Than You Think, Proceedings of the 1st USENIX Workshop on Hot Topics in Security, HotSec 2006, 2006, 25–30.

Tytuł: Wykorzystanie bezprzewodowych sieci sensorowych w systemach sterowania o podwyższonym bezpieczeństwie.

Artykuł recenzowany