緊急情報の迅速かつ確実な転送のための
無線センサネットワークアーキテクチャの設計と評価

河井　哲也[†]　若宮　直紀[†]　村田　正幸[†]

[†] 大阪大学 大学院情報科学研究科　〒 565–0871 大阪府吹田市山田丘 1–5
E-mail: [†]{t-kawai,wakamiya,murata}@ist.osaka-u.ac.jp

あらまし　社会インフラとして用いられる無線センサネットワークでは，緊急情報を他の情報と差別化し優先して伝達する必要がある．本稿では，様々な緊急事態に柔軟に対応するために，動作する領域や時間の異なる複数のメカニズムを統合するセンサネットワーク設計の方法論を提示する．また，この方法論にもとづき新たに設計したセンサネットワークアーキテクチャを提案する．このアーキテクチャでは緊急情報は 3 つのクラスに分類され，緊急情報を優先させるために複数の単純で自己組織的かつ分散的なメカニズムが緊急事態の規模に応じて動作する．シミュレーションにより，このアーキテクチャは小規模および大規模な緊急事態下で緊急情報の到達率および遅延を向上させることを示した．

キーワード　センサネットワーク，緊急情報，迅速性，信頼性

Design and Evaluation of a Wireless Sensor Network Architecture for Fast and Reliable Transmission of Urgent Information

Tetsuya KAWAI[†], Naoki WAKAMIYA[†], and Masayuki MURATA[†]

[†] Graduate School of Information Science and Technology, Osaka University
1–5, Yamadaoka, Suita, Osaka 565–0871 Japan
E-mail: [†]{t-kawai,wakamiya,murata}@ist.osaka-u.ac.jp

Abstract　Wireless sensor networks used as a social infrastructure must be capable of differentiating and prioritizing transmission of urgent sensor information over other non-urgent information. In this paper, we show a network design methodology where several mechanisms which function in different spatial and temporal levels are integrated to adapt to an emergency situation in a self-organizing and distributed manner. We also present a novel and simple network architecture designed following the methodology. In this architecture, sensor information is classified into three traffic classes and each node activates one or more of several simple, self-organizing, and fully-distributed mechanisms in accordance with the scale of an emergency for fast and reliable transmission of urgent sensor information. Our simulation experiments showed that the architecture successfully improved the delivery ratio and delay of the urgent sensor information under both a small scale and large scale emergencies.

Key words　sensor networks, urgent information, fastness, reliability

1　Introduction

Wireless Sensor Network (WSN) technology is expected to play an essential role for our society in the near future. A WSN consists of a number of sensor nodes and a base station (BS). A node is equipped with a processing unit, a radio transceiver, and sensors. Nodes are deployed in a region to monitor and environmental information detected by sensors is collected to a BS through wireless communication among sensor nodes [1].

WSN technology will be used for a wide variety of applications, such as agricultural, health, environmental, and industrial purposes. Among them, a WSN used as a social infrastructure to make our life safe, secure, and comfortable is one of the most promising. This sort of WSNs is supposed to carry various types of information, such as temperature,

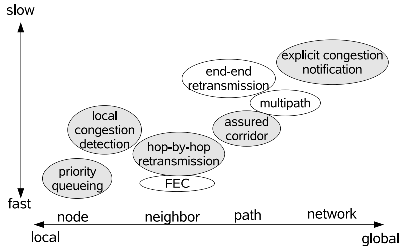

Fig. 1 Examples of control mechanisms.

humidity, fire alarm, intrusion warning, image, and sound. The urgent information, a fire alarm for example, has to be transmitted through a WSN with higher reliability and lower latency than other non-urgent information. Since the capacity of a wireless network is limited, a WSN must be capable of differentiating and prioritizing packets depending on their urgency and importance of embedded sensor information, which are defined by an application. Furthermore, in the event of a large emergency, such as an earthquake attack, a lot of nodes detect the emergency and send urgent information at the same time. A WSN should mitigate a serious congestion caused by this simultaneous emission of a lot of emergency packets, especially around a BS.

Our approach is unique in a sense that several simple mechanisms are incorporated above the network layer. It means that other existing mechanisms on the MAC or network layers can be incorporated with our architecture to improve the reliability and latency of urgent information transmission. Our architecture is fully decentralized. Each node activates one or more of the control mechanisms in accordance with locally observed conditions, and as a result, a series of appropriate controls take place from locally to globally adapting to the scale of an emergency ranging from a small event like a gas leakage to a catastrophic event such as an earthquake attack.

The rest of this paper is organized as follows. Section 2 and section 3 give the methodology for designing a network architecture for fast and reliable transmission of urgent sensor information and the details of the proposed network architecture respectively. The results of the simulation experiments are shown in Section 4. We conclude this paper in Section 5.

2 Design Methodology

In this paper, we consider a WSN deployed in a building or a house to monitor and control a living and working environment. A WSN consists of one BS and a number of immobile sensor nodes. The BS corresponds to a gateway server or a home server with power supply and sends sensor information to a monitoring station of a security company or an administration center if necessary. Sensor nodes are operated on a battery and equipped with a variety of sensors. Although the mechanisms proposed here work above the network layer and do not depend on any specific MAC or routing protocols, we assume a contention-based MAC protocol and a multihop routing protocol.

Each node observes the environment and reports obtained sensor information to the BS at regular intervals, which is defined by an application's requirement. A way that sensor information is transmitted to the BS depends on a routing mechanism or a data gathering mechanism employed. There have been a lot of excellent works on data gathering schemes which can be applied in normal situations, for example, [2]. Once an emergency occurs, an appropriate series of actions take place to deliver urgent information to the BS. For the sake of scalability, there is no centralized control in our architecture and decisions are made by a node itself. Those nodes which are not involved in the emergency keep their normal operation.

In summary, our design objectives of a WSN architecture for transmission of urgent sensor information, are:

- *High reliability and low latency.* The reliability and latency of transmission of urgent information are the most important issues. We consider that energy efficiency can be sacrificed to some extent for transmission of urgent information.
- *Self-organizing and localized behavior.* The type and scale of an emergency and the number of simultaneous emergency events are unpredictable and dynamically change as time passes. A centralized architecture is infeasible for this dynamically changing condistions. Therefore, we need an architecture which is fully-distributed, self-organizing, and adaptive. A globally-organized behavior of a WSN against detected emergencies emerges as a consequence of localized reactions of each sensor node.
- *Simplicity.* Since a node has limited computational capacity and a small amount of memory, mechanisms to support fast and reliable transmission of urgent information must be simple enough.

To satisfy the above requirements, a sensor node should have several simple control mechanisms (see Fig. 1), which work in different spatial and temporal levels, instead of applying a single and complex mechanism to all types and scale of emergency. One or more mechanisms are activated in response to the local conditions and emergency-dependent control emerges from local to the whole.

Since the capacity of a WSN is limited, it is not possible to transmit all emergency packets with high reliability and low latency. Therefore, it is necessary to classify sensor information into several classes in accordance with the required QoS in terms of delay and reliability.

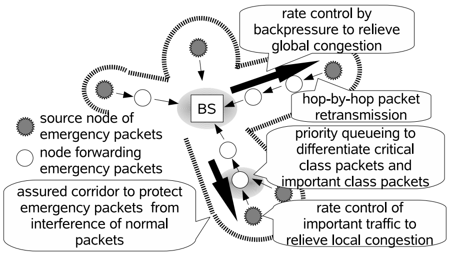
rate control by backpressure to relieve global congestion
BS
hop-by-hop packet retransmission
source node of emergency packets
node forwarding emergency packets
priority queueing to differentiate critical class packets and important class packets
assured corridor to protect emergency packets from interference of normal packets
rate control of important traffic to relieve local congestion

Fig. 2 The mechanisms leveraged in UMIUSI.

3 Proposal of Architecture

We construct UMIUSI (aUtonomous Mechanisms Integrated for Urgent Sensor Information) architecture for transmission of urgent sensor information in a WSN following the design policy stated in the previous section. First, we consider three classes of sensor information as one normal class and two emergency classes and prioritize emergency class information over normal class information.

- *Normal Class.* Any non-urgent information belongs to this class. Normal class information is gathered to the BS at regular intervals of t_{norm}. An application can tolerate delay and loss of normal class information under emergency conditions. Packets of this class are called normal packets.
- *Important Class.* This class is for urgent information, but an application can tolerate loss and delay of important class information to some extent. Packets belonging to this class, called important packets, can be delayed or dropped depending on the level of congestion in an emergency. The interval of emission of important packets $t_{\mathrm{imp}} < t_{\mathrm{norm}}$ is determined by an application, but could be regulated to be larger than t_{norm} to mitigate congestion.
- *Critical Class.* This class is for the most urgent and important information which requires highly reliable and fast transmission to the BS. Critical packets are emitted by a node detecting an emergency at fixed regular intervals of $t_{\mathrm{cri}} < t_{\mathrm{norm}}$, which is determined by an application. The total amount of critical class traffic should not exceed the network capacity to guarantee a high delivery ratio and low delay of the required level. Therefore, the number of sensor nodes for critical information should be limited at the deployment, or some of them should be categorized into the important class.

As stated in the previous section, mechanisms leveraged in UMIUSI must be simple and work independently of other schemes and protocols. In addition, a WSN should adapt to dynamically changing emergency situations by adopting control mechanisms working in different time and topological levels, from fast and local to slow and global. From these points of view, we incorporate following five mechanisms into UMIUSI (shaded circles in Fig. 1).

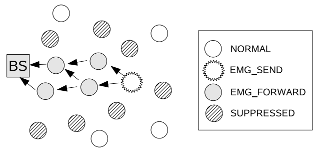

Fig. 3 An assured corridor.

3. 1 Assured corridor mechanism (ACM)

The main purpose of this mechanism is to avoid loss of emergency packets caused by collisions with normal packets. In addition, ACM contributes to avoiding delay caused by sleeping nodes.

An assured corridor consists of awake nodes, which is on the path from the source node to the BS, and surrounding silent nodes, which are in the range of the radio signals of awake nodes (Fig. 3). All nodes in a WSN follow the state transitions among four states: *NORMAL, EMG_SEND, EMG_FORWARD*, and *SUPPRESSED*. In normal operation, all nodes are in the *NORMAL* state and operate in accordance with a data gathering scheme. Once a node detects an emergency, it moves to the *EMG_SEND* state and begins to periodically emit packets labeled as a critical packet or important packet. On receiving an emergency packet for the first time, other node moves to either of the *SUPPRESSED* or *EMG_FORWARD* state. A node on the path to the BS moves to the *EMG_FORWARD* state, cancels its sleep schedule to keep awake, and immediately relays emergency packets it receives. A node which receives an emergency packet but is not on the path moves to the *SUPPRESSED* state. A node in the *SUPPRESSED* state completely stops sending normal packets or decreases the sending rate of normal packets. Details of ACM with simulation results can be found in [3].

3. 2 Retransmission

In order to recover a lost emergency packet and provide differentiated services, we introduce a prioritized scheduling algorithm of hop-by-hop retransmissions.

A node retransmits an emergency packet when it detects a loss. The hop-by-hop acknowledgement can be easily done by, for example, overhearing a packet sent by a next-hop node. If the overheard packet does not contain the information that the node sent, the packet is considered to be lost. An example of a retransmission schedule for the important and critical class is shown in Fig. 4.

3. 3 Priority queueing

Each node has a priority queue for emergency packets, with which important packets are served only when there is no critical packet queued. This means that fast transmission of critical packets is accomplished at the sacrifice of longer transmission delay of important packets.

Transmission of normal packets at a node in either the

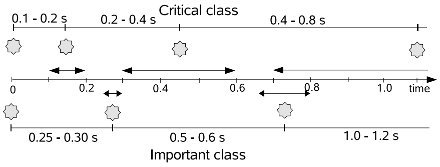

Fig. 4 An example schedule of retransmission of emergency packets. Double-headed arrows and stars show the possible duration for retransmission and averaged timings of packet emission respectively.

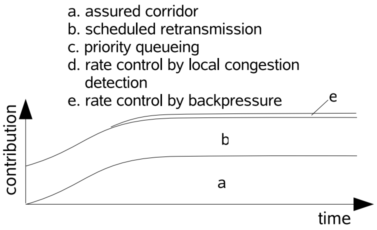

Fig. 5 The contribution of each mechanism for a small scale event.

EMG_SEND or *EMG_FORWARD* state is delayed until the node moves to the *NORMAL* state.

3.4 Rate control by local congestion detection

To mitigate congestion as fast as possible by local control, we introduce a rate control mechanism which is triggered by detection of local congestion. In order to keep the reporting rate of critical information at $1/t_{\mathrm{cri}}$, the rate control is applied only to important class traffic. In our simulation experiments, a node detects local congestion by not receiving any acknowledgement from any of its next-hop nodes, however, congestion detection can be done by other methods such as proposed in [4].

As a rate control algorithm, we employ a TCP-like AIMD (Additive Increase and Multiplicative Decrease) algorithm, such as that in [5], for its simplicity. When an *EMG_SEND* node confirms delivery of an important packet to its next-hop node, its emission rate is increased by decreasing the emission interval t_{imp} as

$$t_{\mathrm{imp}} \leftarrow \frac{t_{\mathrm{imp}}}{1+\alpha t_{\mathrm{imp}}}, \tag{1}$$

where α ($\alpha > 0$) is a constant. The upper bound of the emission rate is determined by the application. When a node detects congestion, its emission rate of important packets is decreased by multiplying the parameter β ($0 < \beta < 1$), which further corresponds to the following adjustment,

$$t_{\mathrm{imp}} \leftarrow t_{\mathrm{imp}}/\beta. \tag{2}$$

3.5 Rate control by backpressure

In an event of a larg emergency such as an earthquake, the rate control with local congestion detection cannot fully mitigate congestion around a node belonging to multiple paths and around the BS, where many emergency packets concentrate on. We adopt a mechanism in which a backpressure message is sent back to source nodes from a point of congestion by piggybacking on an emergency packet to regulates the emission rate of important packets.

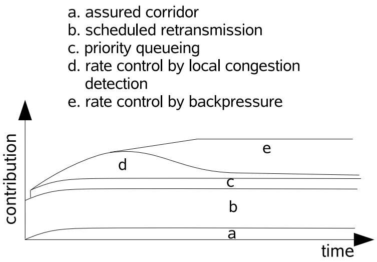

Fig. 6 The contribution of each mechanism for a large scale event

When a node detects congestion, it sets an explicit congestion notification (ECN) bit in the header of important packets which it relays toward the BS. By overhearing the packet, a preceding node recognizes that congestion occurs in the path to the BS. Then, it also sets an ECN bit of the next important packet which it relays to the next-hop node. Consequently, By means of overhearing, a congestion notification propagates to the source node. On receiving the notification, the source node reduces the emission rate of important packets, and the congestion is mitigated.

3.6 Discussion

By integrating the above mentioned five mechanisms, UMIUSI can adapt to a variety of emergencies. Now, let us consider some example scenarios. With a small emergency event, a gas leakage warning for example, only one or a few nodes would detect it. Among five mechanisms described in Section 3, the priority queueing is not used since all emergency packets are likely to belong to one class. In addition, the rate control of important class traffic by local congestion detection does not help much, since the number of nodes emitting important packets is small and the possibility of congestion is expected to be small. ACM is the most effective among five, because loss of emergency packets is mainly caused by collisions with normal packets without an assured corridor. In addition, the retransmission is necessary, since an emergency packet is not protected from normal packets until a corridor is established. Figure 5 is an intuitive sketch to show how much each mechanism contributes to fast and reliable transmission of emergency packets against time.

On the other hand, for large scale emergency, such as an earthquake, many nodes become a source of emergency packets. Figure 6 illustrates the degree of contribution of the mechanisms for the case of large emergencies. Since most of nodes are involved in transmission of emergency packets as source nodes in the *EMG_SEND* state or forwarding

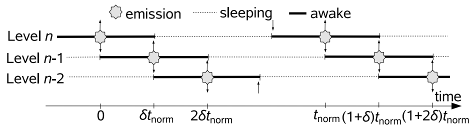
emission
sleeping
awake
Level n
Level n-1
Level n-2
time
0
δt_{norm}
$2\delta t_{\mathrm{norm}}$
t_{norm}
$(1+\delta)t_{\mathrm{norm}}$
$(1+2\delta)t_{\mathrm{norm}}$

Fig. 7 The synchronization-based data gathering scheme.

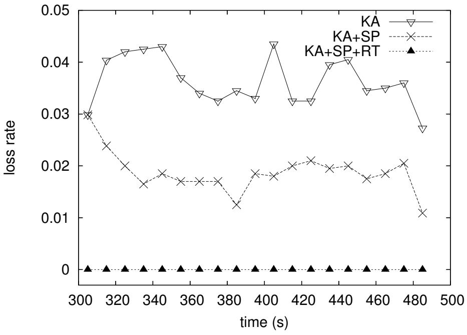

Fig. 8 The loss rate of emergency packets (small emergency).

nodes in the *EMG_FORWARD* state, an assured corridor to suppress the emission of normal packet does not help much. On the contrary, mechanisms to mitigate congestion within a corridor are effective. The priority queueing mechanism offers differentiated forwarding services to emergency packets in accordance with their class. Rate control is first applied locally at a source node to mitigate local congestion among neighboring source nodes. After this, congestion among emergency packets traversing different paths is solved by the backpressure mechanism.

All of these reactions against different types of emergency emerge as a consequence of autonomous and simple behavior of nodes. There is neither a mechanism to identify the type and scale of an emergency nor an explicit rule to choose and coordinate mechanisms.

4 Evaluation of Architecture

We implemented UMIUSI for the ns-2 network simulator package and conducted extensive simulation experiments. In all of the simulation experiments, 200 sensor nodes are uniformly and randomly distributed in a 20 m × 20 m two-dimensional region with a BS at its center. IEEE 802.15.4 non-beacon mode is used as the MAC protocol and the transmission range of radio signals is set to 2.5 m.

We employ the synchronization-based data gathering scheme [6] for the underlying data gathering mechanism. In the synchronization-based data gathering scheme, the number of hops is maintained as a level value at each node and timing of packet emission is the same among nodes of the same level, see Fig. 7. In our simulation experiments, the data gathering cycle t_{norm} and offset coefficient δ are set at 10 seconds and 0.1.

Each simulation experiment lasts for 500 seconds including 300 seconds for initialization without any emergency. To simulate a small scale and large scale emergency, one or 32 nodes respectively are randomly chosen after the initial 300 seconds, and they detect an event at randomly chosen time within following 10 seconds respectively. They wait for next-hop nodes to wake up, then starts transmitting emergency packets with intervals of 0.5 seconds. For a large scale emergency, four out of 32 *EMG_SEND* nodes are of the critical class and the others are of the important class. The nodes stay in the *EMG_SEND* state for 180 seconds and then get back to the normal state. The same experiment is repeated for 100 times with different node layouts. The retransmission schedule of emergency packets is the same as in Fig. 4. For the AIMD rate control, the parameter α in Eq.(1) is 0.05 and β in Eq.(2) is 0.5 taken from [5].

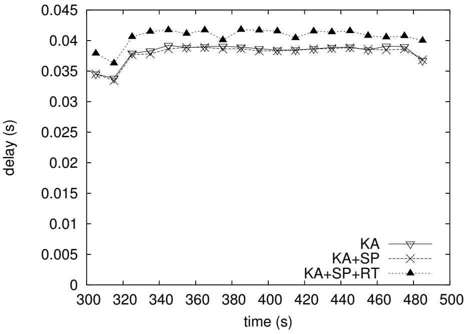

Fig. 9 The delay of emergency packets (small emergency).

In order to evaluate the effect of mechanisms comprising UMIUSI, we compared five variants of integration of the mechanisms. One is KA (keep awake), in which nodes in a corridor keep awake but neither suppression of normal packets nor other mechanisms is conducted. The second is called KA+SP (suppression) and equivalent to ACM, in which an assured corridor is established by suppressing emission of normal packets. Other three are KA+SP+RT, KA+SP+RT+PQ, and KA+SP+RT+PQ+RC, where RT, PQ, and RC denote the retransmission, priority queueing, and rate control mechanisms respectively.

4.1 Small scale event

For experiments of a small scale event, KA+SP+RT+PQ and KA+SP+RT+PQ+RC show the identical results as those of KA+SP+RT, since there is no important class traffic. Therefore, the results of these two variants are not shown in the figures.

The loss rate of emergency packets is shown in Fig 8. The loss rate here is defined as the ratio of emergency packets which did not arrive at the BS out of all emergency packets emitted from a source node. The horizontal axis corresponds to the simulation time. In KA, the loss rate rises since collisions with normal packets are unavoidable. On the other hand, in KA+SP, although the initial value is the same as

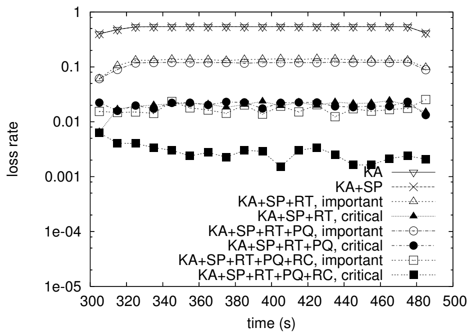

Fig. 10 The loss rate of emergency packets (large emergency).

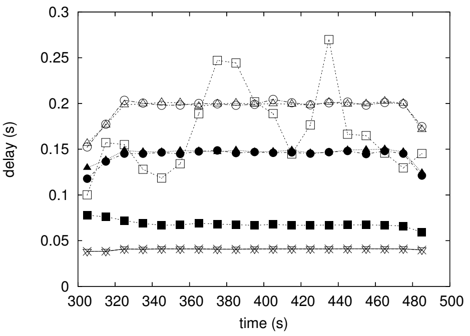

Fig. 11 The delay of emergency packets (large emergency). The legends are the same as in Fig. 10.

that of KA, the loss rate drops gradually in about 20 seconds. This corresponds to time required to establish an assured corridor from a source to the BS, which further depends on the hop distance of the source node and the sleep schedule of the synchronization-based data gathering scheme. With retransmission, *i.e.*, KA+SP+RT, there is no packet loss. However, the total number of emergency packets emitted is larger than that of KA+SP by 15 % and this increase leads to additional energy expenditure.

As for the end-to-end delay (Fig. 9), which is time needed to deliver an emergency packet from the source node to the BS, suppression of normal packets in KA+SP contributes to slight reduction of the delay by shorter backoff in MAC layer than KA. However, retransmission introduces additional delay in waiting for retransmission and the resultant delay of KA+SP+RT becomes larger than the case of KA.

4. 2 Large scale event

The loss rate of emergency packets in a large emergency with 32 *EMG_SEND* nodes is shown in Fig. 10. By comparing results of KA and KA+SP, it can be seen that suppression of emission of normal packets has little effect in a large scale event, since most of packet loss is caused by collisions among emergency packets. By introducing the retransmission mechanism, the loss rate of critical class traffic is further decreased than important class traffic due to retransmission scheduling. With the rate control mechanisms, *i.e.*, KA+SP+RT+PQ+RC, the loss rate of the critical class is reduced to about 0.25 %, while that of KA+SP+RT+PQ is around 2 %.

Figure 11 shows the delay of emergency packets in a large emergency. The delay is almost the same between KA and KA+SP and they are the smallest among the five variants since there is no retransmission involved. In KA+SP+RT, the delay rises in the first 20 seconds for both classes, reflecting retransmissions due to collisions among emergency packets. The scheduled retransmission contributes to smaller delay of critical class traffic than that of important class traffic. The rate control mechanisms further decrease the delay of critical class traffic to about 7 ms, since the number of retransmission and backoff become small due to reduction of important class traffic.

5 Conclusion

Urgent sensor information is needed to be transmitted preferentially in a WSN used as a social infrastructure. In this paper, we presented a network architecture called UMIUSI designed for fast and reliable transmission of urgent information in wireless sensor networks. Sensor information is categorized into three traffic classes. In order to prioritize transmission of the critical class, five simple mechanisms, *i.e.*, assured corridor mechanism, retransmission, priority queueing, rate control by local congestion detection, and rate control by backpressure, collaborate consistently. We verified that the architecture successfully improved the delivery ratio and the delay of emergency packets independently of the scale of emergency through simulation experiments.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci: “Wireless sensor networks: a survey”, Computer Networks, **38**, 4, pp. 393–422 (2002).

[2] C. Intanagonwiwat, R. Govindan and D. Estrin: “Directed diffusion: a scalable and robust communication paradigm for sensor networks”, Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom 2000), Boston, Massachusetts, United States, pp. 56–67 (2000).

[3] T. Kawai, N. Wakamiya and M. Murata: “A fast and reliable transmission mechanism of urgent information in sensor networks”, Proceedings of the 3rd International Conference on Networked Sensing Systems (INSS 2006), Chicago, Illinois, USA (2006).

[4] B. Hull, K. Jamieson and H. Balakrishnan: “Mitigating congestion in wireless sensor networks”, Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys 2004), Baltimore, Maryland, USA, pp. 134–147 (2004).

[5] A. Woo and D. E. Culler: “A transmission control scheme for media access in sensor networks”, Proceedings of the 7th annual international conference on Mobile computing and networking (MobiCom 2001), Rome, Italy, pp. 221–235 (2001).

[6] N. Wakamiya and M. Murata: “Synchronization-based data gathering scheme for sensor networks”, IEICE Transactions on Communications, **E88-B**, 3, pp. 873–881 (2005).