A Fast and Reliable Transmission Mechanism of Urgent Information in Sensor Networks

Tetsuya Kawai, Naoki Wakamiya, and Masayuki Murata
Graduate School of Information Science and Technology
Osaka University, Osaka, Japan
Email: {t-kawai, wakamiya, murata}@ist.osaka-u.ac.jp

***Abstract*— A fast and reliable transmission mechanism of urgent information is essential for establishing a wireless sensor network infrastructure for a safe and secure living environment. In this paper, we propose a transmission mechanism where high reliability and low latency in transmitting urgent information are achieved by making an "assured corridor" where urgent information is forwarded preferentially by suppressing emission of non-urgent information and keeping nodes in the corridor awake. Our mechanism avoids packet loss and possible delay caused by collisions in the wireless transmission and sleeping nodes. We verified our proposed mechanism through simulation experiments and showed that it drastically improved the reliability and the latency of the urgent information transmission.**

I. Introduction

As the development of micro-electromechanical systems (MEMS) technology advances, wireless sensor networks (WSNs) have become popular in the field of information and communication technology and attracted much attention of many researchers [1], [2]. A WSN consists of a number of sensor nodes, each of which is equipped with one or more sensors, an analog-digital converter, a radio transceiver, a central processing unit with limited computational capability, a small amount of memory, and a battery power supply. Sensor nodes are deployed into a region to be monitored and they build up a network using radio communications in an autonomous and distributed manner. Sensor data obtained at nodes are transmitted through a network to a certain node called a base station (BS) or sink for further processing. WSNs have a wide variety of applications such as agricultural, health, environmental, and industrial purposes.

Although a number of research works on WSNs has been done so far, many of them assume that all of the information transmitted in a WSN is of the same attribute, which means the network handles all packets equally. However, when a WSN is deployed as a social infrastructure to make our life more safe, more secure, and more comfortable, it carries various types of information such as security, disaster, environmental, and vital conditions. In such a WSN, both urgent and non-urgent information, such as a fire alarm and humidity data, go through the same network and they apparently should not be handled equally. The urgent information has to be carried through the WSN with higher reliability and lower delay than other non-urgent information. It means that a WSN must be capable of differentiating and prioritizing packets according to requests from the application layer depending on their urgency and importance. In addition, it must provide a mechanism where packets with higher priority are transmitted preferentially.

Some publications on Quality of Services (QoS) support in WSNs aiming at the reliable transmission have been made, based on multipath and multipacket forwarding [3], [4], hop-by-hop broadcast [5], and congestion control [6]. However, they involve rather complicated communication and calculation and this could be a burden for a resource-constrained sensor node. Our goal is to provide a novel and simple mechanism where the transmission of urgent information to BS is guaranteed with high reliability and low latency in a WSN.

In this paper, we propose a fast and reliable transmission mechanism for urgent information in a WSN in which all sensor data are periodically collected at the BS. Although we assume a specific data gathering mechanism [7], [8] in this paper, our scheme can be applied to a variety of mechanisms with a different routing algorithm, a different sleep scheduling, and a different MAC protocol. The basic operation is as follows. A sensor node which has detected an emergency event emits a packet tagged as an "emergency packet". On receiving an emergency packet, nodes along the path from the origin of the emergency packet to the BS suspend their sleeping schedule and broadcast the packet. At the same time, by hearing the flooded emergency packet, the surrounding nodes which are not involved in forwarding the emergency packet suppress the transmission of normal packets in order to avoid collisions in Medium Access Control (MAC) layer. The emergency packet propagates along this "assured corridor" to the BS which consists of nodes forwarding emergency packets and surrounding silent nodes. The rest of the nodes are not aware of the emergency and they remain in the normal operation.

The rest of the paper is organized as follows. In Section II, we briefly review our previous work on the synchronization-based data gathering scheme for sensor networks. Then, the detailed description of the proposed mechanism for fast and reliable transmission of urgent information is discussed in Section III. Section IV gives the details of simulation experiments. Then, the results and discussion are presented in Section V. Finally we conclude the paper in Section VI.

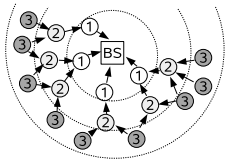


Fig. 1. The synchronization-based data gathering scheme for sensor networks.

II. Synchronization-based data gathering scheme

As a sensor node usually has a limited power resource, saving energy is the primary concern in WSNs to prolong the network lifetime. Since radio communication between distant nodes dissipates a lot of energy, a multihop scheme is usually preferred to deliver the sensor data to the BS. In addition to that, in applications where the sensor data are collected periodically, emitting packets simultaneously among sensor nodes at regular intervals saves a great amount of energy at each node because it can sleep, or turn off its radio transceiver, between two successive emissions. The synchronization-based data gathering scheme [7], [8] is proposed for periodic data gathering using both multihop transmission and synchronization. First, the most distant sensor nodes from the BS (nodes numbered 3 in Fig. 1) broadcast their sensor data at the same time. Nodes closer to the BS in their vicinity (nodes 2) receive the data and aggregate or fuse it with their own sensor data. Then they emit the aggregated information simultaneously. In this way, sensor data propagates as a circular wave from the edge of a sensor network to the BS. Between successive receptions / emissions, a sensor node can turn off its modules to save power consumption. For efficient sleep control, emission of sensor data at a node is scheduled slightly before the emission timing of the nodes that are one-hop closer to the BS.

To accomplish such synchronized behavior, the synchronization-based data gathering scheme adopts a biologically inspired pulse-coupled oscillator model [9]–[12]. Each sensor node maintains a timer and a level value. A level value corresponds to the number of hops from the BS and is initialized to a sufficiently large value. Sensor nodes periodically emit packets containing sensor data and their level value in accordance with the phase of a timer. When a sensor node receives a packet from another node whose level is smaller, it sets its level as the received level plus one and adjusts its timer according to the pulse-coupled oscillator model. When a sensor node receives a packet from a node whose level is larger by one than its own, it deposits the sensor data of the packet into its local buffer. The BS periodically broadcasts beacon packets at the regular intervals of data gathering. The beacon includes a level value of zero. The neighboring nodes which receive a beacon set their own level to one and adjust their internal timer. As they repeatedly receive beacon packets, they begin to emit their sensor information at the same time, which is slightly before a beacon packet is emitted, by the pulse-coupled oscillator model. Those level-one nodes also periodically emit packets, which further adjust level and timer of neighboring one-hop distant nodes. Eventually all sensor nodes correctly identify their levels and adjust their timers. Once the synchronization is accomplished, sensor data begins to propagate from the edge of the network to the BS as intended. We should again note here that each sensor node only emits a packet in accordance with its own timer. There is no additional signaling or control to attain the synchronization. Thus, this scheme is fully distributed and self-organizing.

All communication in this scheme consists of broadcasts. A packet emitted by a node is received by all awake nodes in its vicinity and can be forwarded through multiple paths. However, it does not mean that the scheme consumes more energy than a single-path communication, because all nodes are inherently involved in data forwarding in a periodic data gathering from all nodes and each node only needs to send one packet per data gathering cycle with a help of data aggregation. A node keeps awake from the time slightly before and after the timing of its message emission by offset δt_n to receive messages from one-level larger nodes for relaying purpose and to receive messages from one-level smaller nodes for synchronization. Here, t_n corresponds to the interval of data gathering and δ is an offset coefficient. In the rest of the paper, we call one-level smaller nodes of a node as "parent nodes" and one-level larger nodes as "child nodes". As easily imagined from their names, the mechanism proposed in the paper can be applied to a tree-based data gathering scheme. In the case of MANET-type schemes, where one or more paths are explicitly built for communication between a node and a BS, parent nodes correspond to the next-hop nodes to the BS and child nodes correspond to the preceding nodes.

III. Description of the proposed mechanism

A. State transitions

Since many factors make a wireless network unstable and unreliable, it is a challenging issue to realize a fast and reliable transmission of urgent information in WSNs. Among them, collisions are the most influential and dominant, especially, when Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is used for a MAC protocol. A collision drastically increases the latency of the transmission of packets. Thus, it should be carefully considered how to avoid collisions and how to ensure the delivery of the packet to a parent node even if a collision occurs. Inserting a random backoff before transmission is helpful to some extent as it has already been incorporated into many CSMA/CA algorithms. However, CSMA/CA faces the so-called hidden terminal problem. In addition, collisions cannot be avoided if two or more sensor nodes occasionally start their carrier sense at the same time.

In our mechanism, we generate an "assured corridor" where emergency packets are forwarded preferentially, suppressing emission of normal packets while emergency packets are being transmitted and keeping nodes in the corridor awake. We improve the reliability and the delay of the transmission of urgent information at the sacrifice of a larger propagation delay of non-urgent information and battery power of nodes in the

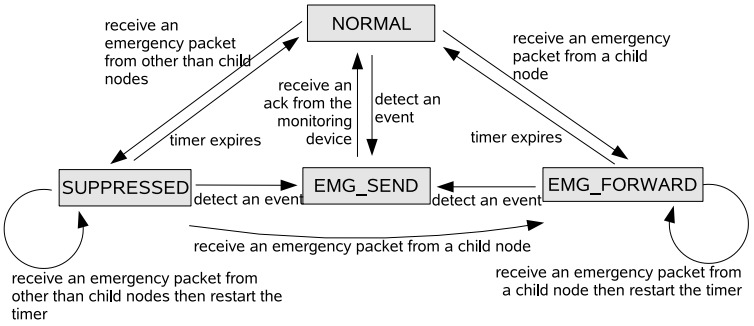


Fig. 2. State transitions of the urgent information transmission mechanism.

corridor. Sleep scheduling of nodes in the corridor is left as future work.

In the synchronization-based data gathering scheme, communication is flooding where the next-hop nodes are not specified. Therefore, if an emergency packet is emitted with an "emergency" tag, neighbors recognize that an emergency packet is passing through the network nearby. In the case of other data gathering schemes, we can consider the same scenario by introducing a special flag at the MAC layer or a special MAC / network address to an emergency packet to force all awake nodes in the range of radio signals receive the emergency packet. We propose the following state transitions for the transmission of urgent information. Figure 2 illustrates a state-transition diagram. Figure 3 gives a sketch of an assured corridor. Figure 4(b) shows how nodes change their states.

NORMAL — As long as there is no emergency event, the WSN operates as usual and sensor nodes are in the *NORMAL* state. They periodically wake up, emit sensor data, and go back to sleep at regular intervals of t_n.

EMG_SEND — When a sensor node detects an emergency event, *e.g.*, a fire, it enters the *EMG_SEND* state. It broadcasts emergency packets with the emergency flag at shorter intervals of $t_e < t_n$. Every emergency packet emitted is given a unique sequence number at the origin node.

EMG_FORWARD — A node which receives an emergency packet for the first time from its child nodes moves into the *EMG_FORWARD* state. It suspends the sleep schedule and sends the received emergency packet at its next timing of packet emission. The following emergency packets are broadcasted immediately.

SUPPRESSED — A node which receives an emergency packet from neighboring nodes which are not its child nodes moves into the *SUPPRESSED* state. A node in this state should suppress emitting some of normal packets, or stop emission completely.

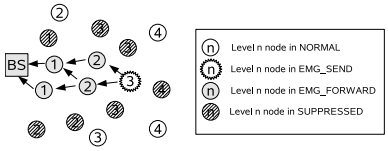


Fig. 3. An "assured corridor".

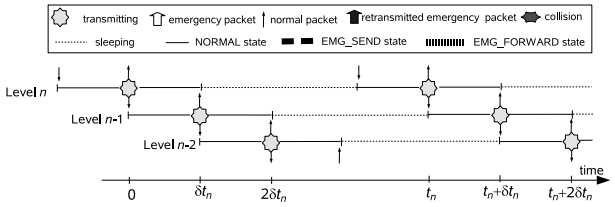
We assume that an observatory or a control center receives the urgent information through the BS. Then, an acknowledgment is sent back to the BS and it is forwarded to the origin node of the emergency packets. On receiving the acknowledgement, the *EMG_SEND* node returns back to the *NORMAL* state. The *EMG_FORWARD* and *SUPPRESSED* are soft states. Entering those states, a node starts a timer. When the timer expires, it returns to the *NORMAL* state. The timer is restarted every time when a node receives an emergency packet.

Note that when a normal node receives an emergency packet for the first time from one of its child nodes it does not send it immediately. This is because its parents are likely to be asleep at that moment, so transmitting the packet right away would be a waste of energy and causes collisions. It means that this first emergency packet must wait for the next timing of emission as in the ordinary data gathering. In addition, although the first emergency packet emitted by the origin node travels to the BS on multiple paths, it could be lost due to collisions. In such cases, any of following emergency packets plays the role of the first emergency packet to establish a corridor to the BS.

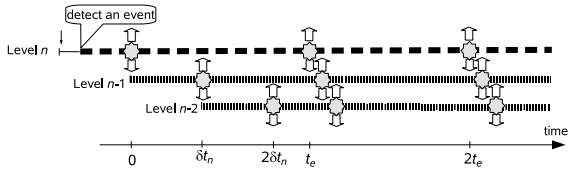
Once an emergency packet reaches the BS, which means that an "assured corridor" is established, the following emergency packets are transmitted to the BS preferentially in the corridor while non-urgent information transmission is delayed or blocked. The increase of the delay of non-urgent information depends on the desired reliability and throughput of the following emergency packets and the duration that the system stays in emergency mode. Understanding this trade-off is one of our future works.

B. Retransmissions

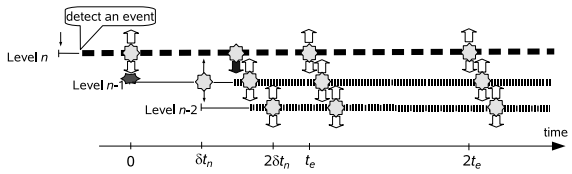
The first emergency packet is sent to the BS without any prioritization and can get lost. Although the following emer-



(a) Normal operation.



(b) Successful scenario for transmission of the first emergency packet.



(c) Scenario with retransmission of a first emergency packet.

Fig. 4. Sequences of the retransmission of the first emergency packet.

gency packet succeeds its role of establishing the corridor, it increases the transmission delay of emergency packets and can be critical to the safety and security of our living environment.

There are several possibilities to overcome the loss of (the first) emergency packets. For example, we could adopt a MAC protocol with prioritization or a packet-level priority control which can provide a differentiated forwarding service. Multipath routing / forwarding is another possibility to improve the reliability of packet transmissions. The synchronized data gathering scheme inherently establishes multiple paths from a node to the BS.

In this paper, we consider packet-level acknowledgements and retransmissions at a higher layer above MAC for the first emergency packet to establish a corridor as fast as possible. In the synchronized data gathering scheme, a sensor node confirms the reception of its emergency packet by observing a packet sent by one of its parent nodes as shown in Fig. 4(b). In other kind of schemes, a node can also expect to receive an emergency packet from its parent node at the timing of emission of the parent node. If it does not, the emergency packet is considered lost.

First, an *EMG_SEND* or *EMG_FORWARD* node of level n emits an emergency packet. In Fig. 4(b) and Fig. 4(c), level n node which detects an emergency event immediately moves to the *EMG_SEND* state. Then, it emits an emergency packet at the next timing of packet emission, $t = 0$. On receiving the emergency packet, a level $(n-1)$ node, which is a parent of the level n node and in the *NORMAL* state, moves to the *EMG_FORWARD* state and broadcasts an emergency packet at the next timing of packet emission at δt_n. If it does not receive the emergency packet, it remains in the *NORMAL* state and the packet to be broadcast is a normal packet as shown in Fig. 4(c). At time δt_n, if the level n node receives the emergency packet from any of its parent nodes, the transmission of the emergency packet was successful. Otherwise, the level n node receives a normal packet and retransmits the emergency packet with a retransmission flag in its header. A retransmission packet must be sent before the level $(n-1)$ node goes to sleep. The retransmission is repeated until it receives the emergency packet from any of its parent nodes or the time that parent nodes go to sleep as shown in Fig. 4(c). The level $(n-1)$ node immediately broadcasts an emergency packet so that level $(n-2)$ node receives the emergency packet before its regular timing of packet emission ($t = 2\delta t_n$ in Fig. 4(c)). Since the other nodes in the vicinity of a node retransmitting emergency packets do not emit any packets, we can avoid collisions and loss of retransmitted packets.

IV. Details of simulation experiments

We implemented the synchronized data gathering scheme and the urgent information transmission mechanism for the ns-2 network simulator package [13] in order to evaluate the reliability and the delay of our mechanism.

The delay is defined as the duration from the time when a node detects an emergency event to the time when the BS receives an emergency packet for the first time. That is, the delay corresponds to the time required to establish an assured corridor. We should note here that the emergency packet arriving at the BS is not necessarily the first emergency packet emitted from the origin node. The delivery ratio is defined as the ratio of the total number of the first emergency packets successfully reaching the BS to the total number of the first emergency packets emitted by the origin node during a simulation experiment. If more than two first emergency packets arrive at the BS by traversing multiple paths, they are counted as one.

In all the simulation experiments, 80 sensor nodes are uniformly and randomly distributed in a 100 m $\times$ 100 m two-dimensional region with the BS at its center. IEEE 802.15.4 [14] non-beacon mode is used as the MAC protocol [15] and the transmission range of the radio signals is set to 20 m. The BS emits beacon packets every 5 seconds, that is $t_n = 5$. The offset coefficient δ is 0.2, where each node wakes up δt_n, *i.e.*, one second before its packet emission and goes to sleep one second after emission of a packet. The interval between packet emission of level n nodes and level $(n-1)$ nodes is also δt_n of one second as shown in Fig. 4(a). Before sending a packet, the random backoff of maximum 10 ms is applied in the network layer in order to ease the collision situation. The size of sensor data is 16 bytes. We do not assume data fusion. Thus, N sensor information amounts to $16N$ bytes. The maximum size of the payload is limited to 80 bytes due to the limitation of IEEE 802.15.4 and sensor data beyond 80 bytes are discarded at each node.

Each simulation experiment lasts 3000 seconds including 50 seconds for initialization and synchronization without any

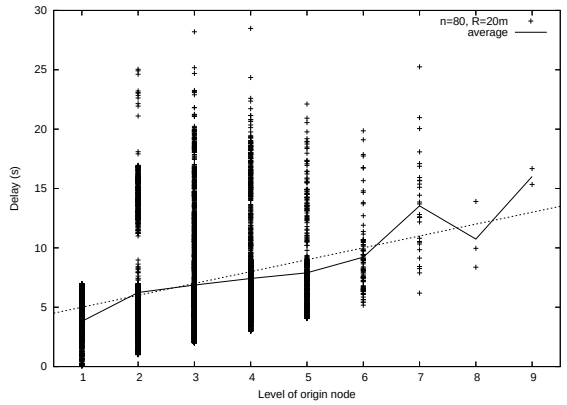


Fig. 5. Delay without retransmission.

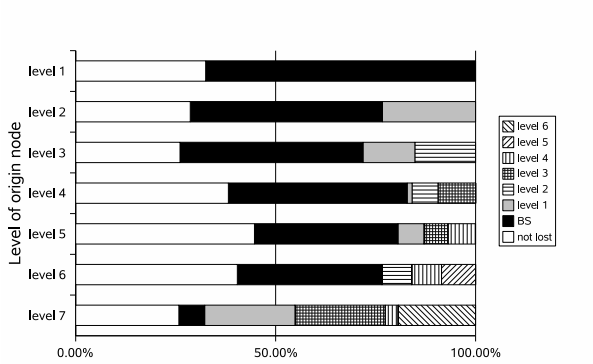


Fig. 6. Levels where the first emergency packets are lost.

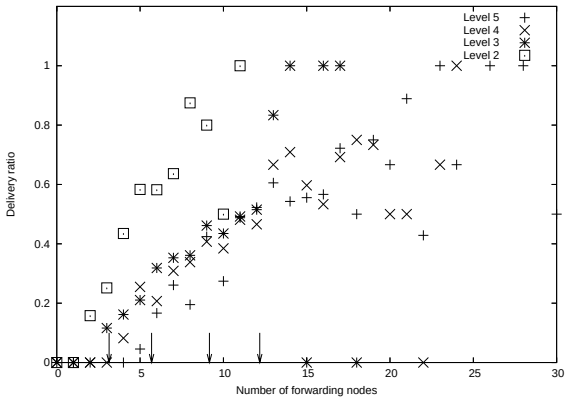


Fig. 7. Delivery ratio without retransmission.

emergency. After the initial 50 seconds, a randomly chosen node is moved into the *EMG_SEND* state. The node stays in the *EMG_SEND* state for 25 seconds and then gets back to *NORMAL* state. After this, 10 seconds are taken to allow *EMG_FORWARD* and *SUPPRESSED* nodes to return to the *NORMAL* state. Then, after a random interval of up to 5 seconds, the next node is randomly chosen and moves to the *EMG_SEND* state. The same procedure is repeated during a single simulation experiment. Under this scenario, we had around 84 cases of urgent information transmissions in each simulation experiment. We conducted two series of 100 simulation experiments; with and without retransmission. We generated 100 different layouts and used them for both series. The maximum number of hops to the BS was ten in our experiments, since paths were constructed to detour around a void caused by the random distribution of sensor nodes. In the case with retransmission, the first retransmission takes place 1.5 seconds after the transmission of an emergency packet, which is 0.5 seconds after the parents' transmission, and the second retransmission is 0.2 seconds after the first retransmission.

Note that the results without retransmission indicate the average performance of transmission of emergency packets without our mechanism, since a corridor is not established when the first emergency packet is sent to the BS.

V. Results and Discussion

A. Without Retransmission

Figure 5 illustrates the delay for each level of the origin node. A solid line corresponds to the average and a dashed line shows the maximum delay when the transmission is completed without loss. Theoretically, this delay consists of the waiting time until the next timing of packet emission at the origin node, *i.e.*, 5 seconds maximum, and 1 second offset for each hop to the BS. (See Fig. 4(b)) Therefore, the delay should be less than $5 + (n - 1) = n + 4$ seconds where n is the level of the origin, ignoring the propagation delay of radio signals. However, Fig. 5 shows that, in many cases, the delay exceeds this value. Only 70.3 % successfully reach the BS within $(n+4)$ seconds. Note that this includes the cases where the first emergency packet is lost and one of the following emergency packets reaches the BS within this maximum delay.

Figure 6 shows the distribution of levels where the first emergency packets are lost due to collisions. As mentioned in Section III-A, one packet emitted by an origin node would be forwarded to the BS along multiple paths. In the figure, the smallest level at which the first emergency packet is lost is depicted. Between 25 % and 40 % of first emergency packets are successfully transmitted to the BS. Most of lost packets encounter a collision from level 1 nodes to the BS. It is partly because we put the BS at the center of the region thus it has many child nodes. In our simulation experiments, there are about 10 nodes around the BS. Emergency packets originated from nodes of level 4, 5 and 6 have a higher delivery ratio than the others, since they have more paths to the BS. However, those packets from level 7 experience higher loss probability in spite that they should have a larger number of paths. This implies that the negative effect of too many hops is more influential than the positive effect of multipath. The fact that the first emergency packets from level 7 are lost mostly at levels other than the BS is consistent with this interpretation.

In order to analyze the effect of multipath, we plot the delivery ratio versus the number of *EMG_FORWARD* nodes involved in the transmission of emergency packets in Fig. 7. The four arrows attached on the horizontal axis show the average numbers of forwarding nodes for the level 2-5 nodes

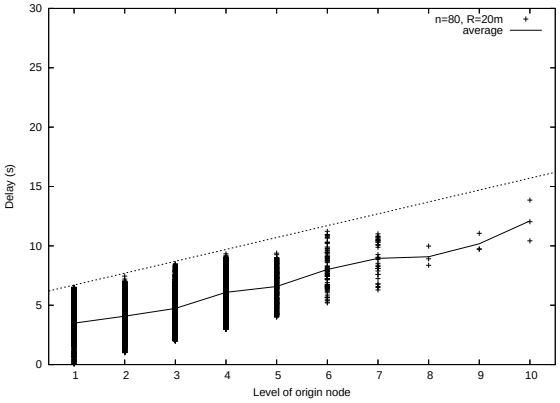


Fig. 8. Delay with the retransmission.

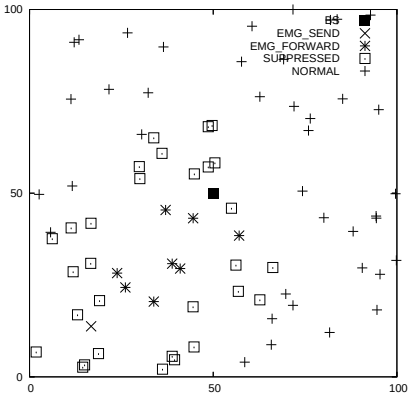


Fig. 9. An "assured corridor" in a simulation experiment.

from left to right respectively. Basically the more forwarding nodes are involved, the better is the delivery ratio. On average, level 2 nodes have about 3.1 forwarding nodes, and thus the delivery ratio becomes around 0.3. For the other nodes, level 3 nodes have 5.7 forwarding nodes and the delivery ratio of 0.3, level 4 nodes have 9.2 forwarding nodes and the delivery ratio of 0.4 and finally level 5 nodes have 12.2 forwarding nodes and the delivery ratio of 0.5. This observation leads to the conclusion that level 2 and 3 nodes do not have enough number of paths for reliable transmission of emergency packets. For example, increasing transmission power of level 2 and 3 nodes would contribute to improving the delivery ratio. However, it also causes more frequent collisions.

B. With Retransmissions

As shown in Section V-A, more than 60 % of first emergency packets are lost due to collisions and consequently the delay becomes higher than the maximum theoretical bound. With the retransmission scheme, the theoretical maximum delay increases for retransmission, but the delivery ratio should become higher. The maximum delay consists of the delay stated in Section V-A and the possible waiting time for retransmission at level 1. With our simulation parameters, the former is $(n + 4)$ seconds maximum and the latter is 1.7 seconds maximum, consisting of 1.5 seconds for the first retransmission and 0.2 seconds for the second retransmission. Therefore the delay should be less than $(n + 5.7)$ seconds for a smooth transmission without any loss.

Figure 8 shows that the delay is drastically reduced by introducing the retransmission in comparison with Fig. 5. Emergency packets reach the BS within the maximum theoretical delay, which is shown as a dashed line in the figure. The absolute value of the delay may seem too large, but this depends on the interval of data gathering t_n and the offset coefficient δ. With a smaller δ, we can shorten the theoretical bound. For example, when δ is 0.02, the offset δt_n becomes 0.1 seconds. With the first retransmission of 0.15 seconds after transmission and the second retransmission of 0.02 seconds after the first retransmission, the bound becomes $5+0.1(n-1)+0.15+0.02 = 0.1n+5.07$ seconds. However, due to the sleeping schedule, the maximum delay to wait until a parent node wakes up is unavoidable. One possible way is to have a mechanism to wake up a parent node by sending a wake-up signal, but we do not consider this in this paper.

In our mechanism, the following emergency packets emitted every t_e, which is set to 2 seconds in our simulation experiments, at the origin are immediately flooded through the "assured corridor" towards the BS, see Fig. 9. Table I shows the delivery ratio and the delay of these packets. Here the delay is derived for each of the following emergency packets as the duration between the emission of the emergency packet at the origin and the time when the first copy of this packet is received at the BS. In the table, the averaged value among all following emergency packets emitted by origin nodes during a simulation experiment is shown. The delivery ratio is defined as the ratio of the total number of the following emergency packets successfully reaching the BS to the total number of the following emergency packets emitted by the origin node during a simulation experiment. If more than two following emergency packets of the same sequence number arrive at the origin by traversing multiple paths, they are counted as one. The average delivery ratio of following emergency packets is 96.8 % and the average delay is as low as 21.4 ms. The reason why the delivery ratio is not 100 % is that there are collisions between emergency packets traversing multiple paths in a corridor. We do not apply the retransmission scheme to following emergency packets. A loss of an emergency packet is immediately compensated by a following emergency packet.

VI. Conclusion

In this paper, we proposed a fast and reliable transmission mechanism for urgent information in sensor networks. An emergency packet first establishes an assured corridor from the origin node to the BS. In the corridor, all nodes keep awake for fast transmission of emergency packets. Along the corridor, all nodes refrain from the emission of normal packets to avoid disturbing transmission of emergency packets in the corridor. The other nodes stay in normal operation. We also introduced a retransmission scheme to achieve reliable transmission of the first emergency packets. Although we considered a severe condition where data emission of nodes were synchronized,

TABLE I

DELAY AND THE DELIVERY RATIO OF THE FOLLOWING EMERGENCY PACKETS.

Origin level	1	2	3	4	5	6	7	8	9	10	average
Delivery ratio (%)	99.5	94.9	96.9	96.9	97.3	97.3	99.0	95.2	93.3	100.0	96.8
Average delay (ms)	4.3	14.1	22.7	31.4	39.4	49.1	56.3	65.7	81.1	88.4	21.4

data were gathered to the single center point, and no node keeps awake for saving energy consumption, simulation experiments showed that the corridor was quickly established and then emergency packets are transmitted to the BS with a high reliability of more than 90 % delivery ratio and a low latency of less than 90 ms.

The mechanism proposed here distinguishes packets in two categories, normal and emergency. In addition, the suppressed nodes completely stop transmitting any packets in the simulation experiments. In the event of a wide area disaster such as an earthquake, a lot of urgent information would arise at once. We believe that our assured corridor mechanism is also useful in such events, but we need to introduce some techniques to control collisions among multiple emergency packets. We now consider to develop a mechanism to effectively establish and handle multiple corridors and relief congestion by a flexible transmission control for urgent information with multiple levels of priority in order to accomplish fast and reliable transmission of multiple urgent information. A WSN should function properly under this kind of situation and we believe that this is one of the network layer functions needed for a WSN as a social infrastructure.

ACKNOWLEDGMENT

This research was partly supported by “New Information Technologies for Building a Networked Symbiosis Environment” (The 21st Century Center of Excellence Program) and a Grant-in-Aid for Scientific Research (A)(2) 16200003 of the Ministry of Education, Culture, Sports, Science and Technology, Japan.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] K. Akkaya and M. Younis, “A survey on routing protocols for wireless sensor networks,” *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, May 2005.

[3] S. Bhatnagar, B. Deb, and B. Nath, “Service differentiation in sensor networks,” in *Proc. of the 4th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, Sept. 2001.

[4] B. Deb, S. Bhatnagar, and B. Nath, “ReInForM: Reliable information forwarding using multiple paths in sensor networks,” in *Proc. of 28th Annual IEEE conference on Local Computer Networks (LCN 2003)*, Bonn, Germany, Oct. 2003, pp. 406–415.

[5] B. Deb, S. Bhatnagar, and B. Nath, “Information assurance in sensor networks,” in *Proc. of the 2nd ACM international conference on Wireless sensor networks and applications*, San Diego, USA, Sept. 2003, pp. 160–168.

[6] Y. Sankarasubramaniam, B. Akan, and I. F. Akyilidiz, “ESRT: Event-to-Sink reliable transport in wireless sensor networks,” in *Proc. of the 4th ACM International symposium on Mobile ad hoc networking and computing (MobiHoc 2003)*, Annapolis, Maryland, USA, June 2003, pp. 177–188.

[7] N. Wakamiya and M. Murata, “Scalable and robust scheme for data gathering in sensor networks,” in *Proc. of the International Workshop on Biologically Inspired Approaches to Advanced Information Technology (Bio-ADIT 2004)*, Lausanne, Switzerland, Jan. 2004, pp. 412–427.

[8] S. Kashihara, N. Wakamiya, and M. Murata, “Implementation and evaluation of a synchronization-based data gathering scheme for sensor networks,” in *Proc. of IEEE International Conference on Communications, Wireless Networking (ICC 2005)*, Seoul, Korea, May 2005, pp. 3037–3043.

[9] R. E. Mirollo and S. H. Strogatz, “Synchronization of pulse-coupled biological oscillators,” *Society for Industrial and Applied Mathematics Journal on Applied Mathematics*, vol. 50, no. 6, pp. 1645–1662, Dec. 1990.

[10] X. Guardiola, A. Díaz-Guilera, M. Llas, and C. Pérez, “Synchronization, diversity and topology of networks of integrate and fire oscillators,” *Physical Review E*, vol. 62, no. 4, pp. 5565–5569, Oct. 2000.

[11] M. B. H. Rhouma and H. Frigui, “Self-organization of pulse-coupled oscillators with application to clustering,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 2, pp. 180–195, Feb. 2001.

[12] I. Wokoma, I. Liabotis, O. Prnjat, L. Sacks, and I. Marshall, “A weakly coupled adaptive gossip protocol for application level active networks,” in *Proc. of IEEE 3rd International Workshop on Policies for Distributed Systems and Networks (Policy 2002)*, Monterey, California, USA, June 2002, pp. 244–247.

[13] The network simulator – ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns/

[14] IEEE 802.15.4, “Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks,” 2003.

[15] J. Zheng and M. J. Lee. Ns2 simulator for 802.15.4. [Online]. Available: http://www-ee.ccny.cuny.edu/zheng/pub/