PAPER

Proposal of an Assured Corridor Mechanism for Urgent Information Transmission in Wireless Sensor Networks

Tetsuya KAWAI[†], ***Student Member***, **Naoki WAKAMIYA**[†], ***Member***, ***and*** **Masayuki MURATA**[†], ***Fellow***

SUMMARY Wireless sensor networks are expected to play an essential role as a social infrastructure to realize our safe and secure living environment. In such a network, critical information must be transmitted faster and more reliably than other information. We propose a distributed transmission mechanism which enables emergency packets to be carried with high reliability and low latency along a preferential path, which is called an "assured corridor." In this self-organizing assured corridor mechanism (ACM), which works above the network layer and does not depend on any specific routing or MAC protocol, a corridor is gradually established as the first packet containing urgent information propagates to the base station. The nodes surrounding the corridor suppress the transmission of non-urgent information and nodes in the corridor are kept awake to forward emergency packets. ACM avoids packet loss and possible delay caused by collisions in the wireless transmission and normal sleep scheduling. An acknowledgment and retransmission scheme is incorporated into ACM in order to improve reliability of transmission of urgent information. Simulation experiments showed that, when only one node transmitted urgent information, the retransmission contributed to establish a corridor quickly and that ACM improved the delivery ratio and the delay of the urgent information transmission once a corridor is established. It was proved that ACM was effective to improve the reliability and the latency of urgent information as well in the cases where multiple nodes sent urgent information at once.

key words: *sensor networks, urgent information, fastness, reliability*

1. Introduction

Due to advances in the development of micro-electromechanical systems (MEMS) technology, 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. Nodes are deployed into a region to be monitored. 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.

Among a number of applications, 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 would carry both urgent and non-urgent information, which apparently should not be handled equally. The urgent information, such that for security, disaster, environmental, and vital conditions, has to be carried through a WSN with higher reliability and lower delay than other non-urgent information such that for regular monitoring for living and working space control. It means that a WSN must be capable of differentiating and prioritizing packets depending on their urgency and importance according to requests from the application layer. In addition, it must provide a mechanism where packets with higher priority are transmitted preferentially.

Since many factors make radio communication 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 (CSMA) MAC protocol is used. A collision drastically increases the latency of the transmission of packets due to backoff and retransmissions. Inserting a random backoff before transmission is helpful to some extent as it has already been incorporated into many CSMA algorithms. However, they face the so-called hidden terminal problem. In addition, collisions cannot be avoided if two or more nodes occasionally start their carrier sense at the same time.

In this paper, we propose an "assured corridor" mechanism, ACM in short, for fast and reliable transmission of urgent information in a WSN. In ACM, an assured corridor is eventually established where emergency packets are forwarded preferentially. Transmission of normal packets is suppressed along the corridor and emergency packets are forwarded by keep-awake nodes in the corridor. By suppressing transmission of normal packets, congestion among emergency and normal packets is avoided. Therefore, it contributes to reducing the latency caused by backoff and retransmissions and the loss probability caused by retransmission timeout. By keeping nodes awake on the path from the source node of emergency packets to the BS, the delay required to wait for the next-hop node to wake up from

[†]Graduate School of Information Science and Technology, Osaka University

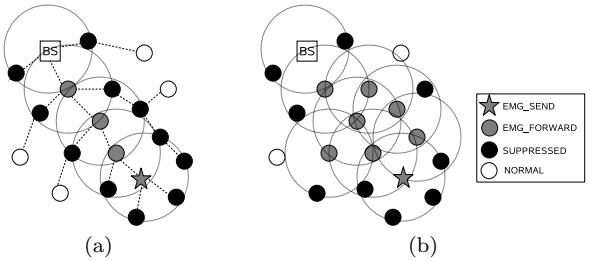


Fig. 1 An "assured corridor" in (a) a tree-based network and (b) a broadcasting-based network.

the sleep mode is avoided.

Examples of an assured corridor are illustrated in Fig. 1 for a tree-based sensor network and a broadcasting-based sensor network. In the figure, a star corresponds to a node which detects an emergency and grey circles correspond to nodes on a path to the BS. Nodes in ranges of radio signals of those grey nodes are denoted as filled circles, which suppress emission of normal packets.

The rest of the paper is organized as follows. Detailed description of ACM is discussed in Sect. 2. In Sect. 3, we show an example of application scenario of ACM to our previous work, *i.e.*, the synchronization-based data gathering scheme [3, 4]. Section 4 gives the details of simulation experiments. Then, the results and discussions are presented in Sect. 5. Finally we conclude the paper in Sect. 6.

2. Description of the proposed mechanism

In this paper, we assume a WSN deployed in a residence, a building, or a small area, used for a home security system, a building automation system, or a public surveillance system for example, in which sensor nodes are immobile. Although ACM works above the network layer and does not depend on any specific MAC or routing protocols, we assume a contention-based MAC protocol and a multihop routing protocol for their wide range of off-the-shelf products and research and development activities. For example, a TDMA protocol is also applicable, but we consider that it has many practical problems to be solved such as scheduling overhead and severe requirement for time synchronization. As for the network layer, a multihop scheme with limitation on the radio transmission energy is usually preferred to avoid contention among wireless communication and prolong the lifetime of batteries. ACM itself is not a routing protocol, although it uses routing information of the network layer. An assured corridor is established along a path that an underlying routing protocol or data gathering scheme builds for communication or data gathering in normal operation.

In our mechanism, a node follows the state transitions illustrated in Fig 2. A node stays in the *NORMAL* state in its normal operation. When a node detects an emergency event, its state is changed to the *EMG_SEND* state and it begins emission of emergency packets. An emergency packet is identified by an emergency flag in its header. When a neighbor node in the *NORMAL* state receives or hears the emergency packet, its state moves to either of the *EMG_FORWARD* or *SUPPRESSED* state depending on its location. If the node is on the path to the BS, in other words, if the node is a next-hop of the *EMG_SEND* node, it moves to the *EMG_FORWARD* state. It suspends its sleep schedule and forwards the emergency packet. If the node is not involved in forwarding the emergency packet, *i.e.*, not on the path to the BS, it moves to the *SUPPRESSED* state and suppresses transmission of normal packets in order to avoid collisions with emergency packets in the MAC layer.

Similarly, among neighbor nodes receiving or hearing an emergency packet forwarded by the *EMG_FORWARD* node, ones on the path to the BS become *EMG_FORWARD* nodes and the others become *SUPPRESSED* nodes. By repeating this process at every hop to the BS, an assured corridor, which consists of *EMG_FORWARD* nodes forwarding emergency packets along the path and *SUPPRESSED* nodes surrounding the path, is eventually completed when the first emergency packet arrives at the BS. We should note here that, if an emergency packet is lost due to a collision for example, *NORMAL* nodes around stay unaware of the emergency and keep the *NORMAL* state.

Once an assured corridor is established, following emergency packets propagate through the corridor which consists of awake nodes forwarding emergency packets and surrounding silent nodes. The rest of the nodes in the WSN are not aware of the emergency and they remain in their normal operation.

These mechanisms imply that the reliability and the latency of transmission of emergency packets are improved at sacrifice of the larger transmission delay of non-urgent information and the depletion of a battery of awake nodes. Although low energy consumption is one of the most important requirements in WSNs, we should not sacrifice the reliability and latency of transmission of emergency packets for the energy efficiency. Therefore, we do not pay much attention to energy efficiency in our mechanism. We believe that such a design policy is acceptable, because it is reasonable to assume that emergency events rarely happen. The lifetime of a WSN depends on energy efficiency not in urgent conditions but in normal operations. If allowed we can introduce a sleep schedule to nodes in a corridor, but it is left as one of future works.

Detailed description of the four states of a node in ACM is given in the following.

NORMAL As long as there is no emergency event, a WSN operates as usual and nodes are in the *NORMAL* state. They periodically wake up, re-

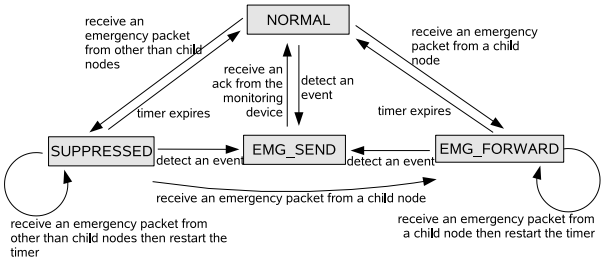


Fig. 2 State transitions.

ceive and transmit a data packet, and go back to sleep at regular intervals of t_{norm}.

EMG_SEND When a 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 $t_{\mathrm{emg}} < t_{\mathrm{norm}}$. Every emergency packet sent is given a unique sequence number at the source node.

EMG_FORWARD A node which receives an emergency packet for the first time from its preceding nodes moves into the *EMG_FORWARD* state. A preceding node is a node for which the node is responsible in forwarding a packet or data toward the BS. For example, if the WSN adopts tree topology whose root is the BS, a preceding node is a child node. On receiving the emergency packet for the first time, a node suspends the sleep schedule. Then, it sends the received emergency packet to the designated next-hop node on the path to the BS, after waiting for the activation of the next-hop node in the *NORMAL* state if it is in the sleep mode. The next-hop node also moves to the *EMG_FORWARD* state and keeps awake once it receives the emergency packet. Therefore, following emergency packets sent after the first emergency packet by the source node are immediately relayed by *EMG_FORWARD* nodes toward the BS.

SUPPRESSED A node which receives an emergency packet from a neighboring node which is not its preceding node moves into the *SUPPRESSED* state. A node in this state should suppress transmitting some or all of normal packets.

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 source node of the emergency packets. On receiving the acknowledgment, the *EMG_SEND* node returns back to the *NORMAL* state. *EMG_FORWARD* and *SUPPRESSED* are "soft states," which are controlled not by explicit signaling but by a timer. Entering these 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. A typical length of the timer is the interval of data gathering in the *NORMAL* state, *i.e.*, t_{norm}, since emergency packets are sent more frequent than normal packets to inform a control center of up-to-date emergency condition.

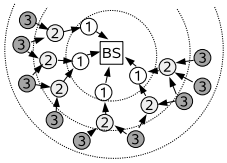


Fig. 3 The synchronization-based data gathering scheme.

Note that an assured corridor is established while the first emergency packet is being forwarded to the BS. Therefore, the transmission delay of the first emergency packet, in other words, the time needed to establish a corridor, depends on a sleep schedule of the data gathering scheme used for normal operation. After a corridor is established, following emergency packets are forwarded immediately by *EMG_FORWARD* nodes, which keep awake, thus the delay is minimal and independent of the sleep schedule. In case that the first emergency packet is lost, any of following emergency packets succeeds the role of the first emergency packet to establish a corridor. Here, we call an emergency packet sent by an *EMG_SEND* node for the first time "the first emergency packet." In addition, an emergency packet that a *NORMAL* node or the BS receives or hears for the first time is also called the first emergency packet. The first emergency packets contribute to establishment of a corridor. Other emergency packets are called "following emergency packets."

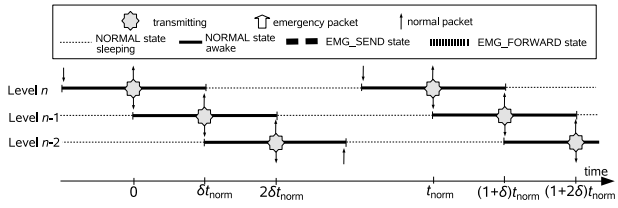
3. Application to the synchronization-based data gathering scheme

3.1 Overview

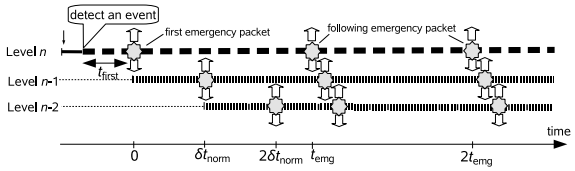
Although ACM does not depend on any specific routing algorithm, we employ the synchronization-based data gathering scheme [3, 4] to evaluate the behavior of our mechanism in this paper. The synchronization-based data gathering scheme is proposed to accomplish energy-efficient data gathering in a WSN without any centralized control. Combined with ACM, it enables a distributed and self-organizing control of fast and reliable transmission of urgent sensor information.

Figure 3 illustrates how sensor data propagate from all nodes to the BS. A number in each circle, *i.e.*, node, corresponds to the number of hops from the BS, which is maintained by each node as a level value. Figure 4(a) shows timings that level $n-2$, $n-1$, and n nodes wake up, receive and send packets, and go to sleep. Here, the interval of data gathering is given as t_{norm}.

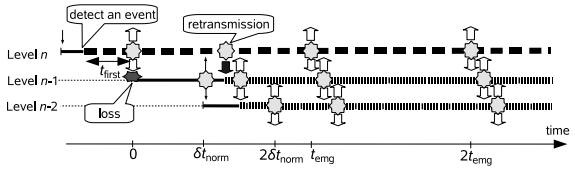
In the synchronization-based data gathering scheme, sensor nodes with the same level value behave in synchrony. When so-called global synchronization



(a) Normal operation.



(b) Successful scenario for transmission of emergency packets.



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

Fig. 4 Transmission sequences in the synchronization-based data gathering scheme.

is accomplished, an interval between packet emission of level i nodes and that of level $i-1$ nodes becomes $\delta t_{\rm norm}$. Now assume that the most distant nodes are at n hops from the BS. First, all level n nodes wake up and then broadcast a packet at the same time. This broadcasting is scheduled slightly before timing of packet emission of level $n-1$ nodes by $\delta t_{\rm norm}$. At this time, all level $n-1$ nodes wake up. They receive packets from level n nodes in their vicinity and aggregate or fuse the received data with their own data. Then, they broadcast a packet containing the aggregated sensor data slightly before timing of packet emission of level $n-2$ nodes by $\delta t_{\rm norm}$, so that level $n-2$ nodes, which are awake at this time, can receive the packet. At the same time, level n nodes also receive packets emitted by level $n-1$ nodes to maintain the synchronization and then go to sleep. Therefore all sensor nodes need to be awake for $2\delta t_{\rm norm}$ during the interval of data gathering as illustrated in Fig. 4(a). For further details of the synchronization-based data gathering, refer to [3].

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 this paper can directly be applied to a tree-based data gathering scheme as shown in Fig. 1(a). 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.

3.2 In emergency

Transmission of urgent information in the synchronization-based data gathering scheme with ACM is depicted in Fig. 4(b). When a node detects an emergency event, it moves into *EMG_SEND* state. It defers emission of the first emergency packet for $t_{\rm first}$ until its next timing of packet emission ($t = 0$, in Fig. 4(b)), since its parent nodes in the *NORMAL* state are asleep at the moment of event detection and can not receive any packet until they wake up. To minimize this delay, one possible way is to have a mechanism to wake up parent nodes by sending a wake-up signal. ACM can be combined with such a mechanism, however, a special hardware for the wake-up mechanism is needed on every node, which leads additional production cost.

When the first emergency packet is broadcast at $t = 0$, parent nodes move to the *EMG_FORWARD* state while neighboring nodes of the same or a larger level move to the *SUPPRESSED* state. By hop-by-hop broadcasting of the first emergency packet, all intermediate nodes move to the *EMG_FORWARD* state.

If the first emergency packet is lost at one of intermediate nodes due to collision for example, the transmission is delayed for $t_{\rm norm}$ until the next timing of packet emission. Letting $t^i_{\rm relay}$ time taken for an *EMG_FORWARD* node of level i to wait for level $i-1$ nodes to wake up, the total delay of the first emergency packet originating at level n is given by,

$$D_n = t_{\rm first} + \sum_{i=1}^{n-1} t^i_{\rm relay} + k t_{\rm norm}, \tag{1}$$

where k is the number of packet loss events.

The maximum of $t_{\rm first}$ is $t_{\rm norm}$, and all intermediate nodes have to wait for $\delta t_{\rm norm}$, if they are in the *NORMAL* state,

$$\max(t_{\rm first}) = t_{\rm norm}, \tag{2}$$

$$\max\left(\sum_{i=1}^{n-1} t^i_{\rm relay}\right) = (n-1)\delta t_{\rm norm}. \tag{3}$$

Thus the maximum of delay D_n for the first emergency packet originating at an *EMG_SEND* node of level n to reach the BS is given by

$$\max(D_n) = t_{\rm norm} + (n-1)\delta t_{\rm norm} + k t_{\rm norm}. \tag{4}$$

The *EMG_SEND* node keeps sending emergency packets at intervals of $t_{\rm emg}$ after its emission of the first emergency packet. These following emergency packets are forwarded to the BS immediately along the corridor. If $\delta t_{\rm norm}$ is relatively large compared to the transmission delay of following emergency packets, a following emergency packet may catch up the preceding first emergency packet at an intermediate node. In

this case, the following emergency packet takes over the first emergency packet and propagates to the BS establishing a corridor as being treated as the first emergency packet.

3.3 Retransmission

Since a corridor is not established, the first emergency packet is forwarded to the BS without any prioritization and can get lost. Although a following emergency packet succeeds the role of a lost first emergency packet in establishing a corridor, it increases the transmission delay of emergency packets and can be critical to the safety and security of our living environment. Following emergency packets can be lost as well, because of possible collisions among emergency packets.

There are several possibilities to overcome the loss of emergency packets. In this paper, we take a hop-by-hop acknowledgement and retransmission scheme at a higher layer above MAC. Our scheme does not exclude other techniques and they are helpful to improve the reliability of transmission. For example, we could adopt a MAC protocol with prioritization [5] or a packet-level priority control. In [6, 7], the authors consider service differentiation in terms of delivery ratio based on DiffServ model. Delay-based differentiation is proposed in, for example, [8, 9]. Multipath routing / forwarding is another possibility to improve the reliability of packet transmission [6, 7, 10]. We will consider effective and efficient coordination of several techniques for fast and reliable transmission of urgent information in the next research work.

The synchronization-based data gathering scheme inherently enables hop-by-hop acknowledgement since a node receives a packet from a parent node for synchronization. In other kind of schemes, a node can also expect to receive an emergency packet from its parent node at the timing of packet emission of the parent node. A node can confirm the successful transmission of its emergency packet by observing a packet sent by one of its parent nodes. If a node does not receive an emergency packet from its parent node or an emergency packet broadcast by its parent node does not contain urgent information it sent, the emergency packet is considered lost. Then, it retransmits the emergency packet. The retransmission scheme of the first emergency packet in the synchronization-based data gathering scheme is shown in Fig. 4(c).

First, level n node which detects an emergency event immediately moves to the *EMG_SEND* state. Then, it transmits an emergency packet at the next timing of packet emission, $t = 0$. A level $n-1$ node, which is a parent node of the level n node, is expected to move to the *EMG_FORWARD* state and broadcast the emergency packet at the next timing of packet emission at $t = \delta t_{\rm norm}$. However, the first emergency packet can be lost, due to the collision with a normal packet transmitted from a neighbor node or random channel error, for example. In this case, the level $n-1$ node remains in the *NORMAL* state and broadcast a normal packet at its timing of packet emission, $t = \delta t_{\rm norm}$ as shown in Fig. 4(c). Receiving a normal packet from its parent node, the level n node detects the loss and immediately retransmits the emergency packet with a retransmission flag in the packet header. Retransmission is repeated until it receives the emergency packet from any of its parent nodes. Therefore, the duration for retransmission is at most $\delta t_{\rm norm}$, *i.e.*, until parent nodes go to sleep. If the next emergency packet originating at the same source node arrives while an emergency packet is waiting for retransmission at an intermediate node, the waiting packet is discarded. This is because that sensor data in the waiting packet is obsoleted by the new data. It is also possible to merge them and generate a new emergency packet depending on an application's requirement.

If a level $n-1$ node receives an emergency packet with a retransmission flag while it is awake, it immediately broadcasts the emergency packet so that level $n-2$ nodes can forward the packet at the next timing of regular emission ($t = 2\delta t_{\rm norm}$ in Fig. 4(c)). The emergency packet sent by the level $n-1$ node also confirms the successful reception to the level n node. Since the other nodes in the vicinity of a node retransmitting emergency packets do not transmit any packets during retransmission interval, we can avoid collisions and losses of retransmitted packets.

Now, consider the delay of the first emergency packet for the worst case scenario with retransmission. The maximum delay of transmission is $\delta t_{\rm norm}$ as far as retransmission succeeds before a parent node, which is still in the *NORMAL* state, goes to sleep (see retransmission from level n node to level $n-1$ node in Fig. 4(c)). If a node fails in retransmission, it must wait for the next cycle of packet emission at $t_{\rm norm}$ later because its parent node are asleep until that time. Therefore, the maximum of transmission delay with retransmission, $D_n^{\rm R}$, is given by,

$$\max(D_n^{\rm R}) = t_{\rm norm}+(n-1)\delta t_{\rm norm}+k' t_{\rm norm}+t^1_{\rm retrans}. \quad (5)$$

where k' is the the number of retransmission failures, which incur delay of $t_{\rm norm}$. $t^1_{\rm retrans}$ corresponds to the time for level 1 node to transmit the emergency packet to the BS. Since the BS is always ready to receive a packet, level 1 node can try retransmitting the emergency packet until the next emergency packet catches up, which is at most $t_{\rm emg}$ after it receives the first emergency packet. Therefore,

$$\max(D_n^{\rm R}) = t_{\rm norm}+(n-1)\delta t_{\rm norm}+k' t_{\rm norm}+t_{\rm emg}. \quad (6)$$

4. Details of simulation experiments

We evaluated the synchronization-based data gather-

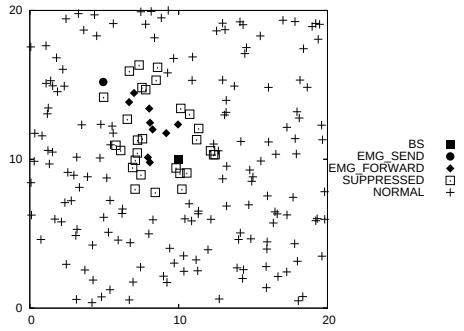


Fig. 5 An "assured corridor" in a simulation experiment.

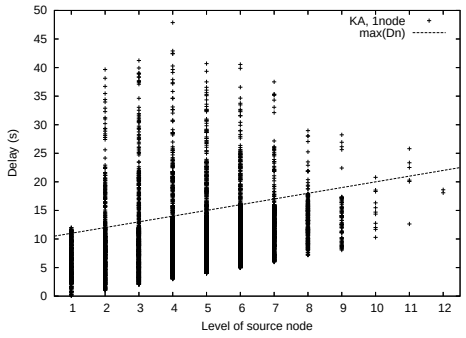


Fig. 6 Delay of the first emergency packets.

ing scheme with ACM on the ns-2 network simulator package [11]. In all of the simulation experiments, 200 nodes are uniformly and randomly distributed in a 20 m $\times$ 20 m two-dimensional region with the BS at its center and the transmission range of radio signals is set to 2.5 m. The high density of node distribution is for the reason that we assume an indoor application such as building automation. The maximum number of hops to the BS was twelve in our experiments. The reason why the number is large for a small region is that paths were constructed to detour around a void caused by the random distribution of nodes. Figure 5 shows a snapshot in one of the simulation experiments with one *EMG_SEND* node. A corridor is established from the source node, which is represented by a circle, towards the BS, filled square. Nodes in the *SUPPRESSED* state surrounding the corridor are illustrated as a open square.

IEEE 802.15.4 [12] non-beacon mode is used as the MAC protocol [13]. The interval t_{norm} of data gathering is set to 10 seconds. The offset coefficient δ is 0.1, where each node wakes up δt_{norm}, *i.e.*, one second before its packet emission and goes to sleep one second after the emission. 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 6 bytes and we do not assume data fusion. Thus, N sensor information amounts to $6N$ bytes. The maximum size of the payload is limited to 78 bytes due to the limitation of IEEE 802.15.4 and sensor data beyond 78 bytes are discarded at each node.

Each simulation experiment lasts 20,000 seconds including 300 seconds for initialization, synchronization, and normal operations without any emergency. After the initial 300 seconds, nodes are randomly chosen and moved into the *EMG_SEND* state. The *EMG_SEND* nodes emit emergency packets at intervals of $t_{\mathrm{emg}} = 2$ seconds. They stay in the *EMG_SEND* state for 40 seconds and then go back to *NORMAL* state. After this, 90 seconds are taken to allow *EMG_FORWARD* and *SUPPRESSED* nodes to return to the *NORMAL* state. Then, after a random interval of up to 10 seconds, the next nodes are randomly chosen and moved to the *EMG_SEND* state. The same procedure is repeated during a single simulation experiment. Under this scenario, we had around 150 emergencies in each simulation experiment. The same experiment is repeated for ten times with different node layouts. In Section 5.1 and 5.2, one node is moved to the *EMG_SEND* state at the same time, whereas multiple nodes detect an emergency in Section 5.3.

For comparison purposes we considered three variants of the mechanism. One is called as KA (keep awake), in which only *EMG_SEND* and *EMG_FORWARD* states are applied and no suppression of normal packets is conducted. Another is called KA+SP (suppression), in which an assured corridor is established by suppressing emission of normal packets, but lost packets are not recovered by retransmission. The other is called KA+SP+RT (retransmission), which is equivalent to ACM.

When a node detects a loss of packet, it first waits for a random duration between 0.05 and 0.15 seconds for the first emergency packet and between 0.1 and 0.2 for a following emergency packet and then retransmits the packet. If the first retransmission fails, a node waits for a random duration between 0.2 and 0.3 seconds and then retries again. After the second retransmission, the interval between retransmission is doubled, that is, a binary back-off scheme is applied.

5. Results and discussions

In following subsections, simulation results of delay and loss rate of emergency packets are presented. Note that, in Figs. 7 through 10, the number of samples over level 10 is so small that large variation is observed in these data.

5.1 Late arrival ratio and delay of first emergency packets

In ACM, the first emergency packet propagates to the BS while establishing a corridor. Thus the delay of urgent information D_n, which is defined here as the duration from the time when a level n node detects an

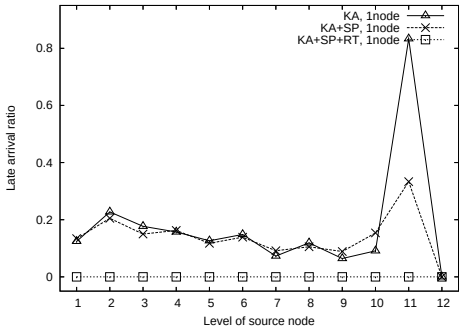


Fig. 7 Late arrival ratio of the first emergency packets.

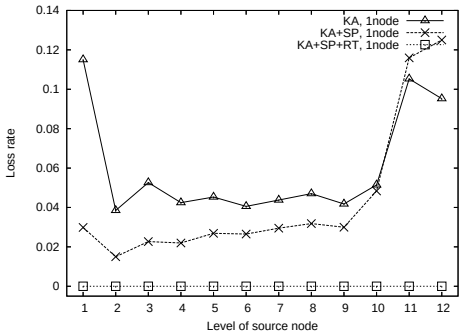


Fig. 9 Loss rate of following emergency packets.

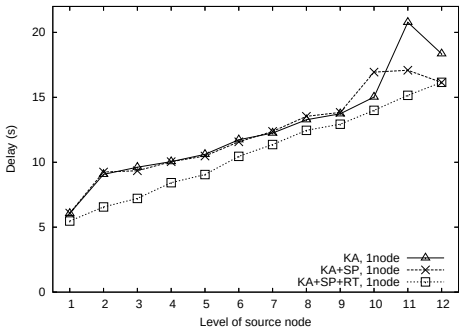


Fig. 8 Delay of the first emergency packets.

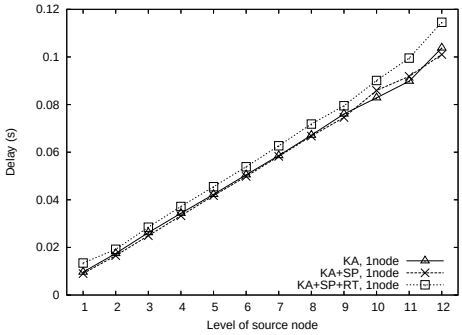


Fig. 10 Delay of following emergency packets.

emergency event to the time when the BS receives an emergency packet for the first time, indicates the time required to establish an assured corridor.

The delay of first emergency packets of KA with one *EMG_SEND* node is plotted in Fig. 6 for each level of the source node. A dashed line shows the maximum delay $\max(D_n)$ without loss, *i.e.*, $k = 0$ in Eq. (4), given by

$$\max(D_n)_{k=0} = t_{\rm norm} + (n-1)\delta t_{\rm norm}. \quad (7)$$

As shown in Fig. 6, the delay exceeds $\max(D_n)_{k=0}$ in about 15 % of the transmission. In these cases, there is at least one packet loss on the way to the BS. Although the lost packet is compensated by a following emergency packet, the loss leads to the increased delay.

The late arrival ratio and the averaged delay of first emergency packets for each source level for KA, KA+SP, and KA+SP+RT are shown in Figs. 7 and 8 respectively. The late arrival ratio is defined here as the ratio of cases where the delay exceeds $\max(D_n)_{k=0}$ for KA and KA+SP, and $\max(D_n^R)_{k'=0}$ for KA+SP+RT substituting $k' = 0$ into Eq.(6),

$$\max(D_n^R)_{k'=0} = t_{\rm norm} + (n-1)\delta t_{\rm norm} + t_{\rm emg}. \quad (8)$$

As seen in the figures, suppression of transmission of normal packets has little effect for first emergency packets because they collide with normal packets in establishing an assured corridor. In KA+SP+RT, in contrast to the others, all of the first emergency packets reached the BS within $\max(D_n^R)_{k'=0}$ in Eq.(8), which means that all first emergency packets are delivered to the BS within one cycle due to successful retransmission. This is the reason why the delay of KA+SP+RT is smaller than that of KA and KA+SP. As stated in Section 3.3, since no normal packets are transmitted at the time of retransmission of emergency packets, retransmission does not suffer from collisions with normal packets and is successful unless there is a collision with another emergency packet.

One might think that the absolute value of the delay is too large. However, this delay depends largely on a sleep schedule of a data gathering scheme, since a node must wait for a parent node to wake up in forwarding the first emergency packet. In the case of the synchronization-based data gathering scheme, we can shorten the delay with smaller δ in Eq.(4) and Eq.(6), but $t_{\rm first}$ is unavoidable without a wake-up mechanism. The results shown in this paper can be regarded as the expected performance in the worst case scenario. The typical delay of a fire alarm for a home security system is from several tens of seconds to one minute and thus the delay of our mechanism is acceptable under the simulation setting. We plan to conduct additional experiments to see the applicability of the proposal.

5.2 Loss rate and delay of following emergency packets

The loss rate of following emergency packets is shown in Fig. 9 while changing the level of source node. The loss

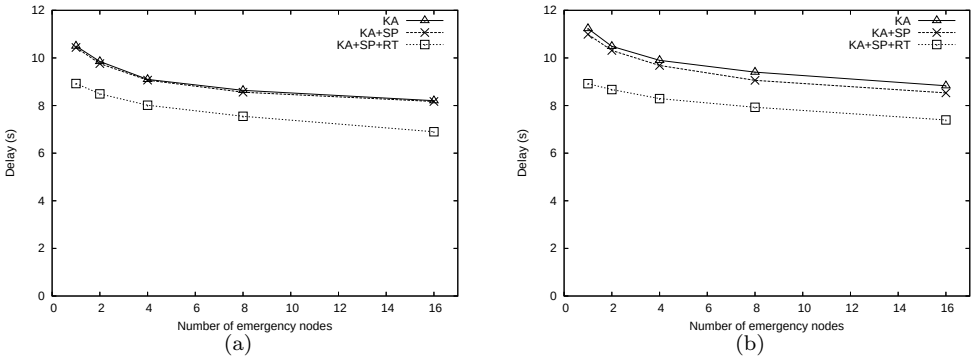


Fig. 11 Delay of the first emergency packets in (a) a broadcast-based network and (b) a tree-based network with multiple *EMG_SEND* nodes.

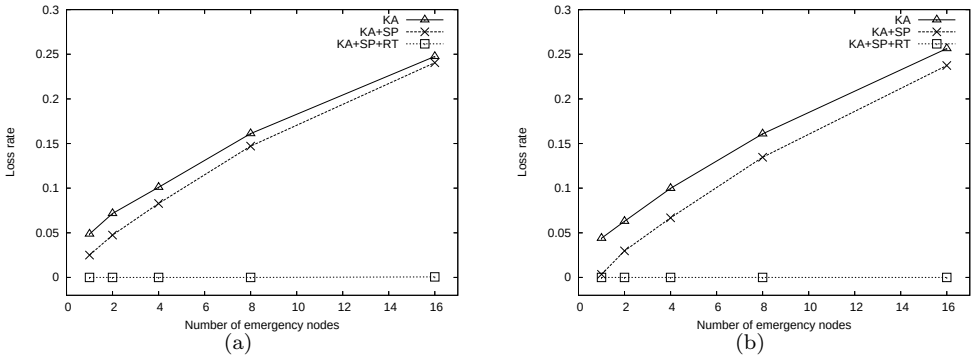


Fig. 12 Loss rate of following emergency packets in (a) a broadcast-based network and (b) a tree-based network with multiple *EMG_SEND* nodes.

rate is defined as the ratio of the number of following emergency packets not received by the BS to the number of those sent from source nodes after a corridor for each source node is completely established.

In the experiments, we set the interval t_{norm} for normal packets at 10 seconds and the interval t_{emg} for emergency packets at 2 seconds. Therefore, without suppression of normal packets, one emergency packet out of five meets normal packets at parent nodes of a source node. Since the density of nodes is the highest around the BS in our node distribution, the loss rate of emergency packets in KA is the highest for source nodes of level 1 in Fig. 9. When transmission of normal packets is suppressed, the loss rate decreases to about the half. Remaining losses are for collisions among emergency packets traversing different paths. With retransmission, there was no packet loss for about 20,000 following emergency packets.

Figure 10 shows the delay of following emergency packets. The delay is roughly proportional to the hop distance from the BS. Retransmission introduces additional delay in waiting for retransmission and the resultant delay becomes larger than the others.

5.3 Multiple emergency nodes

Next we consider cases where multiple nodes detect an emergency event and move to the *EMG_SEND* state at the same time. In addition to the synchronization-based data gathering scheme, which is a broadcast-based routing algorithm, we evaluated the performance of ACM with a tree-based routing algorithm. In this case, each node chooses a parent node among neighbors one hop closer to the BS, based on the received signal strength. This is equivalent to choosing the nearest one-hop-closer node in the simulation experiments. The transmission schedule is the same as in the broadcast-based network, which is shown in Fig. 4.

Figure 11 shows the delay of the first emergency packets against the number of *EMG_SEND* nodes in both of the broadcast-based and tree-based networks. Against intuition, the delay decreases as the number of *EMG_SEND* nodes increases. As stated before, once an assured corridor is established, emergency packets are forwarded immediately since all nodes are awake in the corridor. For example, the first emergency packet sent from an *EMG_SEND* node which is located in or near a corridor established by another *EMG_SEND*

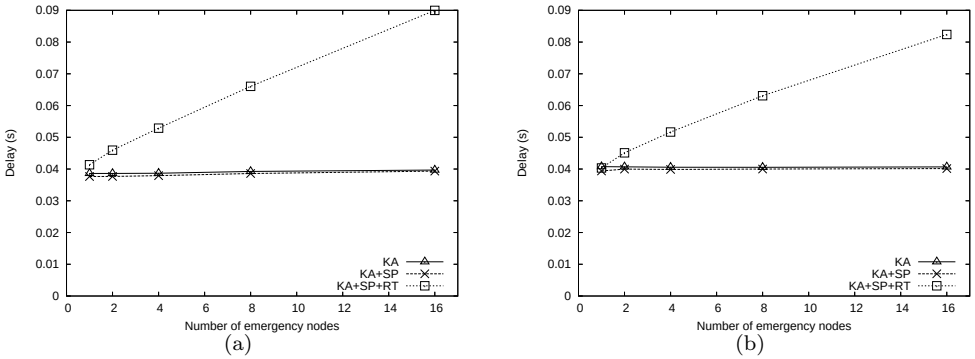


Fig. 13 Delay of following emergency packets in (a) a broadcast-based network and (b) a tree-based network with multiple *EMG_SEND* nodes.

node would be carried through the corridor with shorter delay. Therefore, the more *EMG_SEND* nodes exists, the larger is the probability that the first emergency packets can use a corridor established by another *EMG_SEND* node. The smaller delay of KA+SP+RT compared to KA and KA+SP reflects the smaller loss rate of the first emergency packets. The delay of KA and KA+SP is smaller in the broadcast-based network (Fig. 11(a)) than in the tree-based network (Fig. 11(b)), since multipath effect in the former decreases losses of the first emergency packets.

The loss rate and average delay of following emergency packets are plotted against the number of *EMG_SEND* nodes in Figs. 12 and 13 respectively. The effect of suppression of transmission of normal packets in reduction of loss rate becomes smaller as the number of *EMG_SEND* nodes increases. The more nodes are in the *EMG_SEND* state, the more dominant are packet losses caused by collisions among emergency packets within a corridor not with normal packets. With retransmission, in KA+SP+RT, the loss rate is less than 0.1 % with 16 *EMG_SEND* nodes in both networks. Comparing Fig. 12(a) and Fig. 12(b), the contribution of the suppression of normal packets is smaller in the broadcast-based network. This is because, in the broadcast-based network, some of collisions occur within a corridor among emergency packets traversing different paths. The suppression of normal packets can not avoid collisions within a corridor.

The delay in KA and KA+SP is independent of the number of *EMG_SEND* nodes, see Fig. 13, since the increase of delay due to the contention in the MAC layer among more *EMG_SEND* and *EMG_FORWARD* nodes is deducted by decrease of the average hop count of emergency packets which arrive at the BS. There is a bias in favor of emergency packets originating at *EMG_SEND* nodes closer to the BS than those of distant *EMG_SEND* nodes, for their less loss rate. For supporting this, per-hop delay becomes larger with the number of *EMG_SEND* nodes, although these results are not shown because of space limitation. The delay of KA+SP is slightly smaller than that of KA. The reason is that the number of backoff in the MAC layer is smaller in KA+SP due to suppression of normal packets at surrounding *SUPPRESSED* nodes. This effect decreases as the number of *EMG_SEND* nodes increases. The more nodes are in the *EMG_SEND* state, the more nodes move to the *EMG_FORWARD* state, which means less *SUPPRESSED* nodes. On the other hand, the delay increases in proportional to the number of *EMG_SEND* nodes with retransmission. Again, the reason is collisions among emergency packets within an assured corridor, which cause more retransmission and larger delay. The delay for KA+SP+RT in the broadcast-based network (Fig. 13(a)) is a little larger than in the tree-based network (Fig. 13(b)) since there occur more frequent collisions within a corridor which incur delay due to retransmission.

In summary, for the first emergency packet, suppression of transmission of normal packets along a corridor does not help much by itself. However, by additionally introducing a retransmission scheme, the loss is completely avoided and the delay is effectively reduced. On the contrary, for following emergency packets, suppression contributes to reduction of the loss. With retransmission, the loss rate of following emergency packets becomes close to zero at the sacrifice of the increased delay in proportional to the number of *EMG_SEND* nodes. The increase in the delay is for collisions among emergency packets. We expect that the delay can be reduced by introducing other techniques such as prioritization among emergency packets. We are now working on those issues.

6. Conclusion

In this paper, we proposed ACM, a fast and reliable transmission mechanism for urgent information in sensor networks, where nodes in a corridor are kept awake for fast transmission while adjoining nodes are kept silent for less collisions.

Among data gathering schemes, we adopted the

synchronization-based scheme as an example of application scenarios. Although we considered a severe condition where data transmission of nodes were synchronized, data were gathered to the single center point, and sleep scheduling is adopted, simulation experiments showed that the corridor was quickly established, the loss rate of emergency packets was successfully decreased, and the latency of following emergency packets was improved.

ACM distinguishes packets in two categories, *i.e.*, normal and emergency. In addition, suppressed nodes completely stop transmitting any packets in the simulation experiments. We now consider to develop a mechanism for more severe conditions with many *EMG_SEND* nodes and multiple corridors. We combine several techniques, such as prioritization among emergency packets and rate control with a backpressure mechanism, with ACM. A WSN should function properly under this kind of situation and we believe that this is one of network layer functions needed for a WSN as a social infrastructure.

Acknowledgments

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, March 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] N. Wakamiya and M. Murata, "Synchronization-based data gathering scheme for sensor networks," IEICE Transactions on Communications, vol.E88-B, no.3, pp.873–881, March 2005.

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

[5] L. Chenyang, B.M. Blum, T.F. Abdelzaher, and H. Tian, "RAP: a real-time communication architecture for large-scale wireless sensor networks," Proceedings of the 8th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2002), San Jose, California, USA, pp.55–66, Sept. 2002.

[6] S. Bhatnagar, B. Deb, and B. Nath, "Service differentiation in sensor networks," Proceedings of the 4th International Symposium on Wireless Personal Multimedia Communications (WPMC 2001), Aalborg, Denmark, Sept. 2001.

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

[8] K. Akkaya and M. Younis, "Energy and QoS aware routing in wireless sensor networks," Cluster Computing, vol.8, no.2–3, pp.179–188, July 2005.

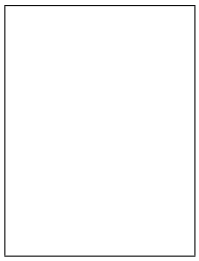
[9] A. Mahapatra, K. Anand, and D.P. Agrawal, "QoS and energy aware routing for real-time traffic in wireless sensor networks," Computer Communications, vol.29, no.4, pp.437–445, Feb. 2006.

[10] B. Deb, S. Bhatnagar, and B. Nath, "Information assurance in sensor networks," Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications (WSNA 2003), San Diego, California, USA, pp.160–168, Sept. 2003.

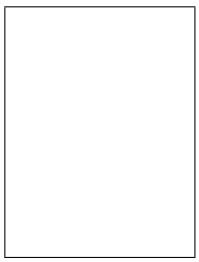
[11] Network simulator ns-2, `http://www.isi.edu/nsnam/ns/`.

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

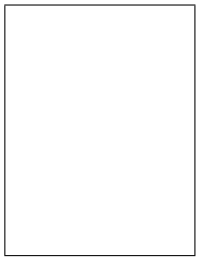
[13] J. Zheng and M.J. Lee, "Ns2 simulator for 802.15.4," `http://www-ee.ccny.cuny.edu/zheng/pub/`.



Tetsuya Kawai received M.Sc. in physical and inorganic chemistry from Osaka University, Japan, in 1994. In April 2005, he became a Ph.D. student in Graduate School of Information Science and Technology, Osaka University, after 11 years experience in an electric manufacturer in Osaka, Japan. His research interests include wireless sensor networks. He is a student member of IEICE.



Naoki Wakamiya received M.E. and Ph.D. from Osaka University, Japan, in 1994 and 1996, respectively. He was an Assistant Professor of Graduate School of Engineering Science from April 1999 to March 2002. Since April 2002, he is an Associate Professor of Graduate School of Information Science and Technology, Osaka University. His research interests include overlay networks, sensor networks, and mobile ad-hoc networks. He is a member of IEICE, IPSJ, ACM, and IEEE.



Masayuki Murata received the M.E. and D.E. degrees in Information and Computer Science from Osaka University, Japan, in 1984 and 1988, respectively. In April 1999, he became a Professor of Cybermedia Center, Osaka University, and is now with Graduate School of Information Science and Technology, Osaka University since April 2004. His research interests include computer communication networks, performance modeling and evaluation. He is an IEICE fellow and a member of IEEE, ACM, The Internet Society, and IPSJ.