ACM: A Transmission Mechanism for Urgent Sensor Information

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

Abstract

The wireless sensor network (WSN) is one of the most promising technologies which helps making our society safe, secure, and comfortable. A WSN as a social infrastructure must transmit critical information faster and more reliable than other information. In this paper, we propose an autonomous and distributed mechanism, called an "assured corridor" mechanism (ACM), for fast and reliable transmission for urgent information in WSNs. In ACM, a self-organizing corridor consists of nodes surrounding the path from the source node to the base station and nodes in the path. The former refrains from transmitting non-urgent information to avoid collisions with emergency packets, and the latter suspends their sleep schedule and keeps awake to avoid delay caused by sleeping. We conducted simulation experiments with a tree-based and broadcast-based network. It was shown that ACM improved the delivery ratio and the delay of emergency packets.

1. 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 [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 information obtained at nodes is 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 so-

cial 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.

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 in an autonomous and distributed manner, where emergency packets are forwarded preferentially. Transmission of normal packets is suppressed along the corridor and emergency packets are forwarded by keepawake 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 collisions and 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 a next-hop node to wake up from the sleep mode is avoided.

There has been some research works to realise reliable transmission in WSNs, [3, 4, 9] for example. In [3, 4], each node relays received packets stochastically according to the forwarding probability, and the reliability of transmission is improved through multipath or retransmission mechanisms. The authors assume a collision-free TDMA MAC layer protocol and packet losses caused by random channel error. However, with a contention-based MAC protocol, which is widely used for WSNs for the ease of deployment and simplicity of a protocol, collision is one of the most dominant



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

causes of packet losses. Collision drastically increases the latency of the transmission of packets due to backoff and retransmissions, especially when a flooding-based protocol is used. Besides, we focus on achieving as high delivery ratio as possible for urgent sensor information, instead of achieving desired reliability for all types of information. In [9], the emission rate of source nodes are dynamically updated according to the feedback from the BS to realize desired reliability. This is a centralized control where the BS makes every decision, but we emphasize a distributed approach in order to obtain high scalability of a WSN.

As for delay of sensor information, some protocols have been proposed [1, 5, 8]. These protocols are designed to find the best path in terms of delay. On the contrary, we aim to design a transmission mechanism which minimize the delay of critical information independent of any routing protocol.

Priority-based mechanisms such as a priority queueing are also helpful to offer a preferential forwarding service to urgent information. ACM works above the network layer and by combining such lower layer mechanism we can expect more reliable and faster transmission of urgent information.

The rest of the paper is organized as follows. Detailed description of ACM is discussed in Section 2. Section 3 gives the details of simulation experiments. Then, the results and discussions are presented in Section 4. Finally we conclude the paper in Section 5.

2. Description of the proposed mechanism

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 multihop routing protocol. 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.

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 becomes a source node of emergency packets. Grey circles correspond to nodes on a path from the source node to the BS and they keep awake during the emergency. Nodes in ranges of radio signals of those grey nodes are denoted as filled circles, which suppress emission of normal packets.

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 states 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 the 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.

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 latency of transmission of emergency packets are improved at sacrifice of the lower delivery ratio and 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



Figure 2. State transitions.

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 operation. If allowed we can introduce a sleep schedule to nodes in a corridor, but it is left as one of our 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, receive 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 $t_{\rm emg} < t_{\rm norm}$. 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 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, a node first suspends its 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 if it is in the sleep mode. The next-hop node also 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 acknowledgement, the *EMG_SEND* node returns back to the *NORMAL* state. On the other hand, the *EMG_FORWARD* and *SUPPRESSED* are "soft states." 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.

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 the 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.

Although ACM reduces packet losses due to collisions between normal packets and emergency packets, a hop-byhop acknowledgment and retransmission scheme can be applied to recover losses due to collisions among emergency packets in a corridor. The acknowledgment is done by 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 lost. Retransmission is repeated until it is acknowledged. However, a packet waiting for retransmission is discarded when the next emergency packet originating at the same source node arrives at the node.

3. Details of simulation experiments

We implemented the proposed mechanism for the ns-2 network simulator package [10] and conducted extensive simulation experiments. In all of the simulation experiments, 200 sensor nodes are uniformly and randomly distributed in a 20 m \times 20 m two-dimensional region with a BS at its center. IEEE 802.15.4 [6] non-beacon mode is used as the MAC protocol [12] and the transmission range of radio signals is set to 2.5 m.

We employ a general broadcast-based or tree-based routing protocol for the underlying network layer. In both routing protocols, we assume that each node knows its own hop distance from the BS. In the broadcast-based routing, a packet contains the sensor data and the hop distance of the



Figure 3. The transmission sequences in normal operation.

sender. A node forwards a packet, if the hop distance of the sender is larger than that of itself. Otherwise, it simply drops the packet. Since a packet can be received and forwarded by multiple nodes in the sender's vicinity, the broadcast-based routing can be categorized into multipath routing protocols without explicit path establishment. An example of such a routing protocol is the synchronizationbased data gathering scheme [11]. In the tree-based routing, every node chooses a next-hop node among neighbors which are closer to the BS by one hop, based on the received signal strength. This is equivalent to choosing the nearest one-hop-closer node in the simulation experiments.

The schedule of transmission is shown in Fig. 3 for normal operation. In the *NORMAL* state, a node sends packets at regular intervals of t_{norm} . The instant that a node at n hops from the BS sends a packet is earlier than the instant that an (n-1)-hop node sends a packet by δt_{norm} . It means that it takes $(n-1)\delta t_{norm}$ for sensor data of n-hop node to reach the BS. Here, δ is a coefficient which governs the interval of packet emission between nodes of adjacent hops. Based on the sleep schedule, an n-hop node wakes up at δt_{norm} before the timing of its packet emission to receive packets from preceding (n+1)-hop nodes. It aggregates the received data with its own sensor data and then it sends the packet at the time when (n-1)-hop node at δt_{norm} after the emission, it goes to sleep.

In our simulation experiments, t_{norm} and δ are set at 10 seconds and 0.1, respectively. Thus the transmission delay is one second per hop in normal situation. In addition, in both normal and emergency situation, a random backoff of 10 ms at maximum is applied in the network layer before sending a packet to avoid collision.

The size of sensor data is 6 bytes. Since we do not assume data fusion, N sensor data amount to 6N bytes. The maximum size of the payload in a packet is limited to 78 bytes due to the limitation of IEEE 802.15.4. Sensor data exceeding this limitation are discarded at each node.

Each simulation experiment lasts for 500 seconds including 300 seconds for initialization without any emergency. After that, each of randomly chosen 1, 2, 4 or 8 nodes moves to the *EMG_SEND* state at randomly chosen time in follow-



Figure 4. An "assured corridor" in the broadcast-based network.

ing 10 seconds. They begin sending emergency packets at the rate of 2 packets/s, *i.e.*, $t_{\rm emg} = 0.5$ seconds. Each of them goes back to the *NORMAL* state at 180 seconds after it moves to the *EMG_SEND* state. The same experiment is repeated for 100 times with different node layouts. Fig. 4 shows a snapshot in one of the simulation experiments with one *EMG_SEND* node.

For comparison purposes, we considered three variants of the mechanism. One is called as KA (keep awake), in which only the *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, in which retransmission is applied in addition.

4. Results and discussions

In this section, some results of simulation experiments are presented. Since the performance without ACM fully depends on underlying routing and data gathering schemes, we do not present results without ACM. Similarly, emergency packets sent before an assured corridor is established are not taken into the results shown in this paper.

4.1. Loss rate of emergency packets

First, we consider the case of one *EMG_SEND* node. The loss rate of emergency packets against simulation time is shown in Fig. 5. The loss rate is defined as the ratio of the number of emergency packets not received by the BS to the number of those sent from the source node after a corridor is completely established.

In the tree-based network without suppression (KA in



Figure 5. Loss rate of emergency packets in (a) a tree-based network and (b) a broadcast-based network with one *EMG_SEND* node.



Figure 6. Delay of emergency packets in (a) a tree-based network and (b) a broadcast-based network with one *EMG_SEND* node.

Fig. 5(a)), about 2 % of emergency packets are lost due to collision with normal packets. By keeping surrounding nodes quiet (KA+SP), the loss rate becomes almost zero. In the broadcast-base network (Fig. 5(b)), the loss rate with KA is larger than in the tree-based network, since there occur additional collisions among emergency packets traversing multiple paths. On the other hand, with KA+SP, although the initial value is the same as that of KA, the loss rate drops gradually in about 20 seconds. The reason why the loss rate does not become zero is that suppressing transmission of normal packets can not prevent collisions among emergency packets in a corridor. With retransmission, *i.e.*, KA+SP+RT, no packet loss occurs. However, the total number of emergency packets that *EMG_SEND* and *EMG_FORWARD* nodes send including retransmission is larger than that of KA+SP by 15 % and this increase leads to additional energy expenditure.

4.2. Delay of emergency packets

As for the end-to-end delay (Fig. 6), which is defined as the time taken for an emergency packet emitted by a source node to arrive at the BS, we can observe that the delay of KA+SP is a little smaller than that of KA. In KA+SP, since surrounding nodes are quiet, the number of backoff due to contention in the MAC layer is smaller than in KA [7].

The delay of KA+SP+RT becomes larger than the others for retransmission in the broadcast-based network as shown in Fig. 6(b). However, in the tree-based network (Fig. 6(a)), such drawback is not observed. As we saw in Fig. 5(a), the



Figure 7. Loss rate of emergency packets in (a) a tree-based network and (b) a broadcast-based network with multiple *EMG_SEND* nodes.

suppression is highly effective in the tree-based network, which means that there is little need of retransmission. On the contrary, in the broadcast-based network, there are collisions among emergency packets which incur retransmission. Retransmission is conducted in only 0.4 % cases of packet transmission in the tree-based network, while 11 % in the broadcast-based network.

Comparing Fig. 6(a) and Fig. 6(b), we can see that the delay of KA and KA+SP is larger in the tree-based network than in the broadcast-based network. The reason is that a random backoff is applied before packet emission in the network layer in the experiments. The BS in the broadcast-based network receives multiple emergency packets with the same sequence number which traverse different paths. Among them, the first packet which arrives at the BS is taken into account in the delay. On the other hand, in the tree-based network, there is only one path for an *EMG_SEND* node. Thus the delay in the tree-based network.

4.3. 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. The loss rate of emergency packets are plotted against the number of *EMG_SEND* nodes in Fig. 7. The more the number of *EMG_SEND* nodes is, the more frequently collisions occur. More than 25 % of emergency packets are lost in the cases of eight *EMG_SEND* nodes without retransmission. This is because that emergency packets originated from different source nodes collide with each other in the same or merged assured corridor.

In comparing results of KA and KA+SP, the effect of suppression of normal packets in reduction of loss rate be-

comes slightly smaller as the number of *EMG_SEND* nodes increases in both the tree-based and broadcast-based networks. With the help of retransmission, in KA+SP+RT, the loss rate is less than 0.3 % and 0.4 % with eight *EMG_SEND* nodes in the tree-based and the broadcast-based networks respectively.

Fig. 8 shows the delay of emergency packets against the number of EMG_SEND nodes. For KA and KA+SP, results are close since most of nodes are in EMG_SEND or EMG_FORWARD states and suppression of normal packets is not effective. In addition, the delay slightly decreases as the number of EMG_SEND nodes increases in both the treebased and broadcast-based networks. The reason for this can be explained as follows. In calculating the delay, we take into account only emergency packets that successfully arrive at the BS. Therefore, there is a bias in favor of emergency packets emitted by EMG_SEND nodes closer to the BS than those of distant EMG_SEND nodes, for their less loss rate. For supporting this, the per-hop delay of KA and KA+SP, which is not shown because of space limitations, slightly increases as the number of EMG_SEND nodes becomes larger due to contention in the MAC layer among more EMG_SEND and EMG_FORWARD nodes. On the contrary, the delay of KA+SP+RT increases with the number of EMG_SEND nodes reflecting more frequent retransmission due to collisions among emergency packets within a corridor.

In concluding the above results, we can say that suppression of normal packets contributes reduction of the loss of emergency packets. With retransmission, most of emergency packets from a source node can reach the BS at the probability of higher than about 99.6 %. However, it is accomplished at the sacrifice of the increased delay, which is proportional to the number of *EMG_SEND* nodes, for con-



Figure 8. Delay of emergency packets in (a) a tree-based network and (b) a broadcast-based network with multiple *EMG_SEND* nodes.



Figure 9. The total number of packet emission and the loss rate.

tention among emergency packets.

4.4. ACM and stochastic forwarding

Finally, we show results of comparison with a stochastic forwarding scheme in the broadcast-based network, in which a node decides whether it forwards or drops a received packet in a probabilistic way. One example of such scheme is proposed in [3]. In the stochastic forwarding scheme, if the forwarding probability is equal to one, a node forwards all packets that it receives. The forwarding probability can be greater than one, which means that a node stochastically retransmits a packet in addition to its first emission in order to improve reliability of the transmission.

In our simulation experiments, only *EMG_SEND* and *EMG_FORWARD* nodes adopt the scheme for reliable

transmission of urgent information. Although the forwarding probability is dynamically updated in accordance with the reception ratio at the BS in [3], we used fixed forwarding probability in comparisons. We conducted a number of experiments to find forwarding probabilities with which the stochastic forwarding scheme shows the same level of reliability as ACM. The suppression of normal packets is not applied in experiments with the stochastic forwarding scheme.

Fig. 9 shows results of the loss rate of emergency packets and the transmission overhead. The transmission overhead is defined as the ratio of the total number of emergency packets emitted at *EMG_SEND* and *EMG_FORWARD* nodes to the number of emergency packets successfully delivered to the BS.

The stochastic forwarding scheme with the forwarding probability of one, denoted as SF(1.0) in the figure, is equivalent to KA. By increasing the forwarding probability to 1.35, SF(1.35) can attain the same level of reliable transmission of emergency packets as KA+SP. However, the total number of emergency packets needed is larger by 33 % than that of KA+SP. To avoid loss of emergency packets, the forwarding probability for the stochastic forwarding scheme must be set at 2.0. As a result, the transmission overhead of the stochastic forwarding scheme becomes larger than that of ACM by 84 %, whereas KA+SP+RT also introduces additional overhead in retransmission. Although not shown in figure, the delay of emergency packets in SF(1.35) is 10 % larger than in KA+SP, and 7 % larger in SF(2.0) than in KA+SP+RT.

5. Conclusion

In this paper, we proposed ACM, a fast and reliable transmission mechanism for urgent information in WSNs. An assured corridor is eventually established from a source node to the BS. In the corridor, all nodes keep awake for fast transmission of emergency packets. Beside the corridor, all nodes refrain from transmission of normal packets to avoid disturbing transmission of emergency packets in the corridor. The other nodes stay in normal operation. Simulation experiments showed that the loss rate of emergency packets was successfully decreased, and the latency of emergency packets was improved for both a tree-based and broadcastbased networks.

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

- K. Akkaya and M. Younis. Energy and QoS aware routing in wireless sensor networks. *Cluster Computing*, 8(2–3):179– 188, July 2005.
- [2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38(4):393–422, Mar. 2002.
- [3] S. Bhatnagar, B. Deb, and B. Nath. Service differentiation in sensor networks. In *Proceedings of the 4th International Symposium on Wireless Personal Multimedia Communications (WPMC 2001)*, Aalborg, Denmark, Sept. 2001.
- [4] B. Deb, S. Bhatnagar, and B. Nath. ReInForM: Reliable information forwarding using multiple paths in sensor networks. In *Proceedings of 28th Annual IEEE conference* on Local Computer Networks (LCN 2003), pages 406–415, Bonn, Germany, Oct. 2003.
- [5] T. He, J. A. Stankovic, C. Lu, and T. Abdelzaher. SPEED: a stateless protocol for real-time communication in sensor networks. In *Proceedings of 23rd International Conference on*

Distributed Computing Systems (ICDCS 2003), pages 46–55, Providence, Rhode Island, USA, May 2003.

- [6] IEEE 802.15.4. Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks, 2003.
- [7] K. Leibnitz, N. Wakamiya, and M. Murata. Modeling of IEEE 802.15.4 in a cluster of synchronized sensor nodes. In Proceedings of the 19th International Teletraffic Congress (ICT-19), pages 1345–1354, Beijing, China, Aug. 2005.
- [8] A. Mahapatra, K. Anand, and D. P. Agrawal. QoS and energy aware routing for real-time traffic in wireless sensor networks. *Computer Communications*, 29(4):437–445, Feb. 2006.
- [9] Y. Sankarasubramaniam, B. Akan, and I. F. Akyilidiz. ESRT: Event-to-sink reliable transport in wireless sensor networks. In *Proceedings of the 4th ACM International symposium on Mobile ad hoc networking and computing (MobiHoc 2003)*, pages 177–188, Annapolis, Maryland, USA, June 2003.
- [10] The network simulator ns-2, http://www.isi.edu/ nsnam/ns/.
- [11] N. Wakamiya and M. Murata. Synchronization-based data gathering scheme for sensor networks. *IEICE Transactions* on Communications, E88-B(3):873–881, Mar. 2005.
- [12] J. Zheng and M. J. Lee. Ns2 simulator for 802.15.4, http: //www-ee.ccny.cuny.edu/zheng/pub/.