LiDSN: A Method to Deploy Wireless Sensor Networks Securely based on light communication

Giang Doan Minh Nguyen
Keio University
spider@ht.sfc.keio.ac.jp

Takuya Takimoto
Keio University
tacky@ht.sfc.keio.ac.jp

Takuro Yonezawa
Keio University
takuro@ht.sfc.keio.ac.jp

Jin Nakazawa
Keio University
jin@ht.sfc.keio.ac.jp

Kazunori Takashio
Keio University
kaz@ht.sfc.keio.ac.jp

Hideyuki Tokuda
Keio University, JST CREST
hxt@ht.sfc.keio.ac.jp

ABSTRACT

Deploying Wireless Sensor Networks (WSN) securely still requires users to have certain skills and exert effort. In the near "sensor everywhere" future, a much simpler method for deploying WSN will be necessary for end-users. We propose LiDSN(**Li**ght **C**ommunication for **D**eploying **S**ecure Wireless Sensor **N**etworks) which enables users to achieve deployment tasks via simple interaction. LiDSN leverages light-based communication between an LED and a light sensor in order to add a new sensor node securely into existing WSN. Through touching interaction, a new sensor node ID and secret key can be transmitted to the WSN, and then the WSN is able to identify which node should be added while maintaining the security of the WSN.

Author Keywords: Light communication, deployment, wireless sensor network.

ACM Classification Keywords: H.5.2 [User Interfaces]: Interaction styles; L.5[Pattern Recognition]: Interactive Systems.

General Terms: Design, Experimentation, Human Factors.

INTRODUCTION

Today WSN have become more and more popular. Using a WSN, we can perform tasks such as environmental observation and surveillance on remote health services. The "Sensor-everywhere" era is will be arriving shortly and users are expected to be capable of installing applications on home servers and be able to set up required sensor nodes all by themselves in order to create WSN.

For that purpose, the home environment has to meet the certain requirements. First, because it is to be applied at home, data privacy is necessary requiring a secure WSN. When WSN became popular, people in the same area will also have their own WSN. The next requirement is to identify exactly which WSN will be added. Furthermorethe that sensor node adding interface should be simple enough for regular users. The last requirement is low cost.

Although there has been much research conducted in creating secure WSNs or WSN interface set-ups, much more work is necessary to fulfill the goal of simplicity and security simultaneously for the installation of WSN. Example:[1] uses smartphone camera and QR code of the node to identifies the node. The problem is that with only QR code there is no safe data to use as secure key. Therefore data could not be sent with safe in adding process. Other research in Reliable Set-Up of Medical Body-Sensor Networks [2], which uses IrDA communication to transfer unique code to identify the exact sensor node for adding to secure WSN. This method can solve all of the requirements, but this method use IrDA hardware, which is not included in most of sensor nodes. Therefore, this makes the sensor node more expensive and difficult to apply with current sensor nodes.

To fulfill the requirements of simplicity and security at a low cost, we focus to leverage light communication for deploying WSN. Almost every sensor node has built-in LEDs to indicate their state and a built-in light sensor to receive light signals. Thus, we propose "LiDSN", which uses light communication for adding new sensor nodes to WSNs easily and securely. Light communication which is provided by LiDSN is similar to NFC(Near Fied Communication). This, in turn makes the deployment process secure because lights for communication are hidden (see Figure 1). Users can easily add required sensor nodes to secure WSN by simply touching a sensor node to be added with a Connector, which is a device like a sensor node but has both a light sensor and LED. This also stores WSN identification and secure protocol information and automatically is added to WSN when turned on.

LIDSN MODEL

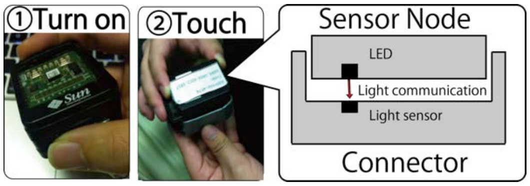

Figure 1. Add new node interaction.

In LiDSN, each WSN has one Connector. This plays a role in transferring data between sensor nodes and the WSN at the deployment phase. With thesensor node, if it has an LED it is used as a Sender. If not, it is used as Receiver.

Copyright is held by the author/owner(s).
UbiComp'12, September 5-8, 2012, Pittsburgh, USA.
ACM 978-1-4503-1224-0/12/09.

Step by Step Process of Adding A New Sensor Node

To add a new sensor node, users only have to take two simple steps: (1) Turn on the sensor node then (2) touch the sensor node with the Connector. At the Connector, depending on whether the light-pattern is received or not, we can know whether the sensor node has a LED or not. Transferred data will be changed correlatively. If the sensor node has an LED, it will send its ID and temp key to the Connector. On the other hand, if the sensor node does not have an LED but a light sensor, the Connector will send WSN identification and a temp key to the sensor node. With the ID we can identify the exact node and WSN. With the temp key we can encrypt data when sending over wireless communication and safely send all required data over a secure protocol.

LIGHT COMMUNICATION

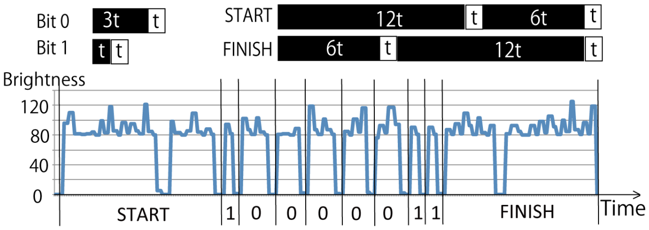

Figure 2. Light pattern and light signal.

To encode data to a light pattern, we divide time into a period called ”t”. Light pattern has 0 bit, 1 bit, START flag, FINISH flag. We construct the light pattern with time period t as shown in the Figure 2. The black period time performs during high brightness. The white period illustrates the LED in a turned off state. The reason for this is the limit of sensor node, this make it difficult to identify exact numbers of bit in long string of the same bits, if using t(on) as bit 1 and t(off) as bit 0.

To identify light patterns, we add a START flag at the first bit pattern, and also a FINISH flag at the end of the bit pattern. In addition, we also add checksum byte of data at first to make sure data has been successfully sent. For example, ”10000011” binary data is encoded as shown in Figure 2.

EVALUATION

For the experimental LiDSN, we used the SunSpot sensor node to make a single-hop and multi-hop WSN with Network-Wide-Key secure protocol [3]. For basic light communication evaluation, we sent random 128bit data and checksum byte over 382 times in 25 bit/sec with 100% accuracy results.

We also asked 20 participants to evaluate the usability of LiDSN by comparing the addition ofnew sensor nodes with LiDSN and the basic method without LiDSN. The basic method means that participants have to select correct sensor nodes from the broadcasting sensor node list and input correlative security code by hand to connect to this sensor node. Out of the 20 participants, 5 people (1-5 in Figure 3) are familiar with WSN, and 15 people (6-20 in Figure 3) are unfamiliar with WSN. We measured the time length of each user when deploying both single-hop and multi-hop WSNs with eight sensor nodes that have a LED and two that have a light sensor. After that, we also asked participants to fill out a questionnaire survey about each methods with the following contents: Is it simple to deploy?; Is it useful?; Was it tiring to deploy? Each question scores from 1 to 4. The result is shown in Table 1 and Figure 3.

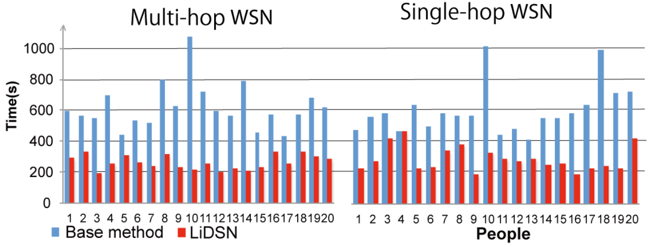

Figure 3. Construct time (second).

	Simply	Useful	Tire
Base	2.10/4	2.25/4	3.45/4
LiDSN	3.90/4	3.50/4	1.65/4

Table 1. Average question score.

The average time to finish the task was 229 seconds for LiDSN and 488 seconds without LiDSN. We recognized the efficiency of LiDSN as twice faster than without LiDSN. There is not much difference between two groups of users. With the result shown in Table 1, we can conclude that LiDSN is simpler and less tiring than base method.

CONCLUTION AND FUTURE WORKS

In this paper, we propose LiDSN, a simple interface to add a new node to secure WSNs. To add a new sensor node, users only touch the sensor node with the Connector. LiDSN uses LED and light sensors, and therefore it does not require any special hardware. In future works, we desire to experiment with LiDSN to add more than one type of sensor nodes within one WSN by using a smartphone with an accessory such as the Connector, which will also make the Connector more friendly and simple in providing feedback to the user.

ACKNOWLEDGEMENT

This research was partly supported by National Institute of Information and Communications Technology (NICT).

REFERENCES

1. Simon Duquennoy, Niklas Wirström, and Adam Dunkels. 2011. Demo: Snap: rapid sensornet deployment with a sensornet appstore. In Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems (SenSys '11)
2. Baldus, H., Klabunde, K.:Reliable Set-Up of Medical Body-Sensor Networks. In: Computer Science, pp. 353–363. (2004)
3. Marcos, A.S.J., Paulo S.L.M.B., Cintia B.M., Tereza C.M.B.C.: A survey on key management mechanisms for distributed Wireless sensor networks. In: Computer Networks, vol. 54, pp.1389–1286, (2010)