Environmental Monitoring and Data Collection System with Mobile Devices

Yukihiro Daidai and Masahito Shiba
Ryukoku University
y_daidai@www.vii.ss.i.ryukoku.ac.jp shiba@rins.ryukoku.ac.jp

ABSTRACT

We have developed a monitoring system for facilities that house important cultural assets, which require environmental information management. In general, administrators patrol such facilities at regular intervals. Our system provides administrators with wireless devices that collect environmental data from their wireless sensors. Using such wireless devices significantly increases the efficiency of data communication in these facilities. In addition, the system employs authentication and encryption features, which are useful for the preservation of important cultural assets. This paper describes the structure of the system and the method for securely collecting the observed data.

KEYWORDS

Sensor Networks, Environmental Monitoring, Encrypted Communication

1 INTRODUCTION

Recently, wireless sensor devices have seen increased use in the field of environmental monitoring[1, 2]. Such wireless sensor devices are not limited by location and can monitor across distances[3]. These devices are powered by internal batteries and therefore, they must be designed to consume very little electricity. Moreover, wireless communications are susceptible to a variety of malicious attacks such as spoofing, interception, and data tampering. In this paper, we propose a low-power wireless environmental monitoring system that securely transmits messages. This system has the following features:

- It can work with less computational resources.
- It sends and receives observation data with encrypted communication.
- Devices authenticate other devices.

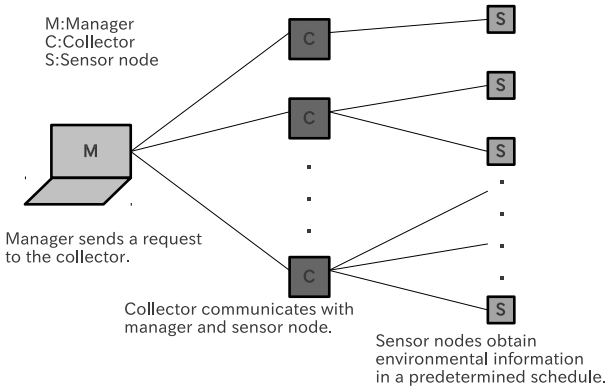

Figure 1. System configuration

In general, memory and computing power of wireless sensor devices are low. A system should operate even in such an environment. Malicious attackers can easily eavesdrop; therefore, it is necessary to encrypt messages[4]. In our system, wireless sensor devices are using public key cryptography to encrypt messages[5]. In the other words, in this system, the sensor devices are authenticated[6].

2 SYSTEM CONFIGURATION

The proposed system has three primary components: sensor nodes, collectors, and a manager (Figure 1). Sensor nodes positioned in a facility monitor and store environmental data on a regular basis. Then, a collector retrieves the stored data from the sensor nodes and passes it to the manager for storage in a database. The roles of sensor nodes, collectors, and the manager are as follows.

- Sensor nodes: observe environment and store data temporally.
- Collectors: retrieve data from the sensor nodes and send the data to the manager.
- Manager: stores the collected data in a database.

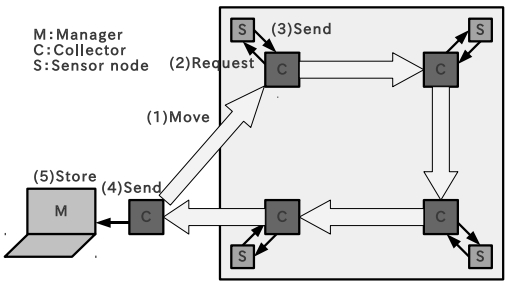

Figure 2. A mobile collector retrieves data from different sensor nodes

As illustrated in Figure 2, a collector performs the following functions:

(1) moves into the vicinity of a sensor node,
(2) sends a request for data to the sensor node,
(3) receives stored data from the sensor node, and
(4) sends the data to the manager.

The data sent by the collector is saved to a database maintained by the manager. Sensor nodes can communicate with other sensor nodes to extend the communication range; however, this increases power consumption. Therefore, in the proposed system, the communication range of devices is narrow and the collectors move, which reduces overall power consumption. The following sections explain the functions of the manager, collectors, and sensor nodes in more detail.

2.1 Manager

The manager communicates with the collectors and stores data in a database. The manager also manages the collectors, sensor nodes, and the scheduling of data collection of the sensor nodes. The manager is responsible for the sensor node information shown in Table 1. *ID* is a unique value that identifies sensor nodes. *Address* is the network address of a sensor node. *Observed data* is the collected environmental data, and *Collecter* identifies the collector with which a sensor node is communicating. The manager is also responsible for the collector information shown in Table 2. Here, *ID* is a unique value that identifies each collector. *Address* identifies a collector network address, and *Sensor node* is the node ID of sensor node that is managed.

Table 1. Sensor node information

Name	Description
ID	ID is a unique value that identifies the device.
Address	Address is the network adress
Observed Data	Observed data is environmental information received from sensor nodes.
Collector	Collector is ID of the collector to which the sensor node belongs.

Table 2. Collector information

Name	Description
ID	ID is a unique value that identifies the collector.
Address	Address is own address.
Sensor node	Sensor node is ID of the sensor node to be managed.

2.2 Collector

Collectors are responsible for communicating with the sensor nodes. If a sensor node is within range of a collector, the collector can retrieve that sensor node's stored data. Although the manager cannot directly communicate with sensor nodes, they communicate through collectors.

2.3 Sensor Node

A sensor node sends requests to the manager through a collector. A sensor node has three operational states: data sensing, communication, and standby. Each state occurs at predetermined intervals. Sensor node state transitions are illustrated in Figure 3. Sensor nodes perform the following functions:

(1) observes environment at specific intervals,
(2) goes into standby state after storing observed data,
(3) transmits the data to the collector at a specified time, and
(4) returns to standby state after communicating with the collector.

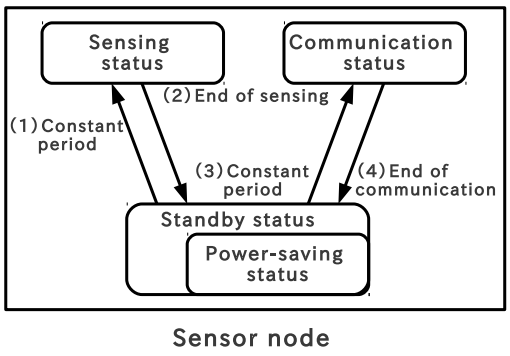

Figure 3. Sensor node state transitions

To reduce power consumption, sensor nodes change their state to standby to extend operational lifetime.

2.4 Encrypted Communication

Public key cryptography is used to encrypt wireless communication in the proposed system. The sensor node public key (PK) and manager secret key (SK) used for public key cryptography are stored in advance at the sensor node. Secure Socket Layer and Transport Layer Security (SSL/TLS) are cryptographic protocols in various fields. SSL/TLS communication requires negotiating multiple-algorithm encrypted key exchanges and digital certificates to connect to a node. In intermittent communication, sessions end quite often. SSL/TLS communication, which needs negotiation every time at communication, is not suitable for the system. Multi-hop communication carries data to a distant base station by communicating through other nodes; however, multi-hop communication is more susceptible to malicious interception than singlehop communication. In the proposed system, communication between the sensor nodes and collectors is singlehop communication, which reduces the risk of data interception.

3 CHARACTERISTICS AND BEHAVIOR

The proposed system has been designed to monitor important cultural facilities, such as art galleries and museums. In such facilities, if temperature or luminance is not properly managed, the exhibits can degrade. To prevent tampering by a malicious attacker, temperature and illumination data should be protected. The proposed system has the following features:

- Administrators may move freely while carrying the collectors.
- The system is low impact; it does not place an undue burden on administrators.
- Each sensor device accumulates data.
- Authentication is used to protect data transmission.

Multi-hop communication is often used in sensor networks because it is common to require multiple communication routes between sensor devices. Such communication requires high power consumption. In the proposed system, the collector moves to nearby sensor nodes. Then, the gateway collects the data. This reduces power consumption by reducing the number of communications. The proposed system also reduces the risk of data interception by reducing the number of communication hops. Equipment costs are reduced by employing a mobile base station. It is desirable to develop and implement an environmental monitoring system that does not burden facility administrators. The proposed system takes advantage of normal administrative patrols to collect data. Using mobile devices, the facility administrator can automatically collect data from the sensor nodes while performing routine duties. Therefore, the system only introduces an administrative burden during the initial installation of the wireless sensor devices, which can be easily set up. In addition, the wireless sensor devices used by the system are easy to replace.

These wireless sensor devices also have sufficient memory for data storage. Data can be accumulated on the sensor nodes and transmitted to the collector. Therefore, the burden of the administrator of the facility will be to only setup the wireless sensor devices. Wireless sensor devices can be setup easily. In addition, the system can exchange wireless sensor devices with less effort. The system uses wireless sensor devices having memory. Therefore, sensor node can store the observed data. Thereafter, the wireless sensor devices can reduce power consumption by sending more than one observed data in bulk to the base station. In this system, the collectors can acquire observed data stored on the sensor

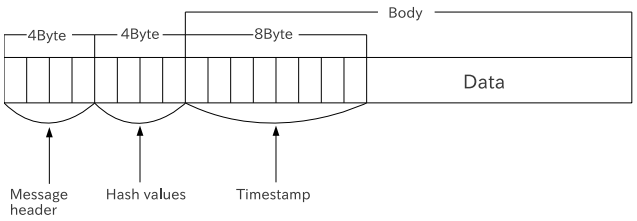

Figure 4. Internal message structure

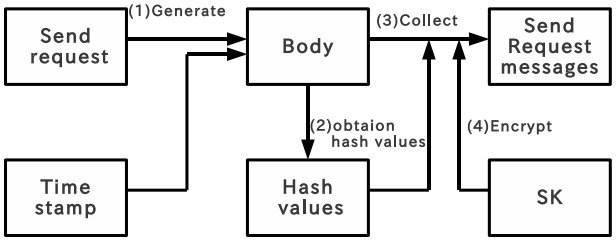

Figure 5. Send request message encryption

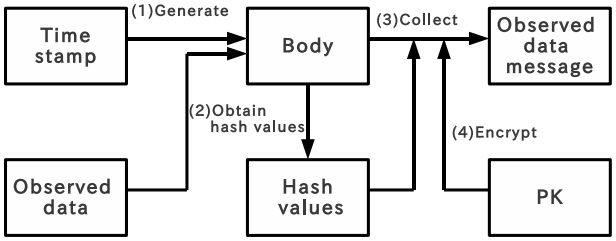

Figure 6. Observed data message encryption

nodes. The collector and sensor node in the system can communicate with the range sensor nodes of the radio wave intensity. Any devices other than the collectors should not be allowed to collect the observed data that is stored in the sensor nodes. Sensor nodes and collectors execute requests only from authorized devices and not from those that have past timestamps.

4 DATA COLLECTION

4.1 Message Structure

Figure 4 shows the internal structure of messages used in the system. The first four bytes is the message header, which identifies the type of message. The next four bytes contain the hash value, which uniquely identifies the message. The hash value is inserted into the body of the message and is used to check for tampering. The next eight bytes contain the message time stamp. Time stamps are used to protect against replay attacks by comparing the time stamp value stored by the collector when the message is sent with the time stamp value of the received message. Discrepancies between time stamp values can indicate malicious attacks. Figures 9–11 illustrate how the hash and time stamp values are used to secure messages. This will be discussed in more detail later in the paper.

4.2 Message Types

The system uses three types of messages.

- Send request: The message created by the manager to instruct the collector to retrieve accumulated data from a sensor node (Figure 5).
- Observed data: The message created by a sensor node to transmit accumulated data (Figure 6).
- Delete request: The message created by the collector to instruct the sensor node to delete data (Figure 7).

Delete requests are only sent to the sensor node after successful data transmission. If a sensor node fails to deliver an observational data message, it will resend the failed message when it responds to the next send request message. The following outlines the flow of messages between the manager, collectors, and sensor nodes, as illustrated in Figure 8.

(1) The manager transmits send request messages to a collector.
(2) The collector transmits send request messages to a sensor node.
(3) The sensor node that receives the send request message transmits an observed data message to the requesting collector.
(4) The collector sends a delete request message to the sensor node.
(5) The receiving collector sends the observed data message to the manager.

Send request messages are generated by the following procedure (Figure 5).

(1) The manager generates a message body from a send request and a time stamp.

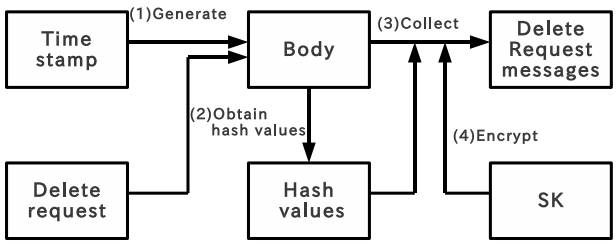

Figure 7. Delete request message encryption

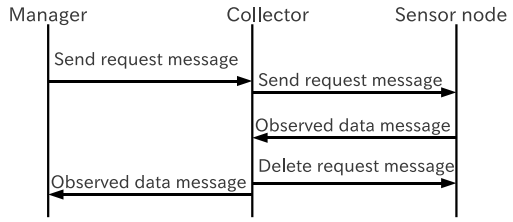

Figure 8. Message flow

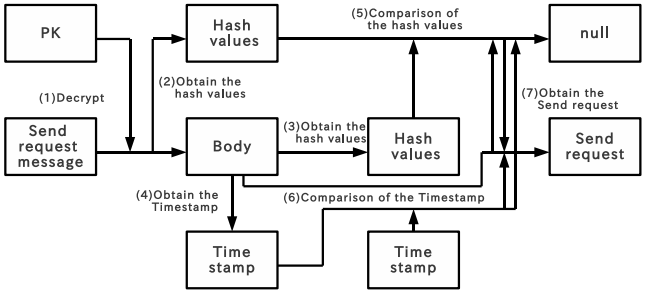

Figure 9. Decoding the Send request message

(2) The manager obtains a hash value from the body.
(3) The manager combines the body and hash value.
(4) The manager encrypts combined message in SK.

This allows the system to encrypt all communications. Delete request (Figure 7) and Observed data (Figure 6) messages are created in the same manner. Received send request messages are decoded as follows (Figure 9).

(1) The sensor node decrypts message in PK.
(2) The sensor node extracts the hash value from the send request message.
(3) The sensor node obtains the hash value stored in the message body.
(4) The sensor node obtains the time stamp stored in the message body.

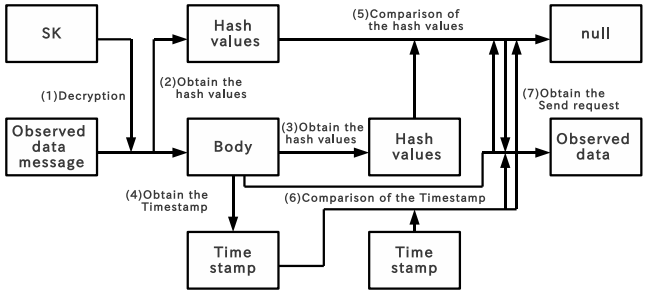

Figure 10. Decoding the Observed data message

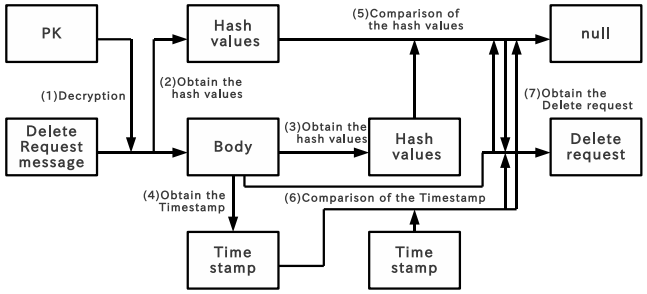

Figure 11. Decoding the Delete request message

(5) The sensor node compares the hash values from Steps (1) and (2).
(6) The sensor node compares the time stamp from Step (3) with the original time stamp.
(7) The sensor node obtains the send request.

This allows the sensor node to confirm the legitimacy of a send request message received from a collector. The system decrypts Observed data (Figure 10) and Delete request (Figure 11) messages in the same manner.

5 SECURITY

The proposed system verifies messages to protect against tampering, eavesdropping, and spoofing.

5.1 Security Prerequisite

Message transmission is secure under the following conditions.

- The collectors cannot be stolen by malicious attackers.
- The manager cannot be the target of an attack.

The manager and sensor nodes exchange messages through the collectors because the sensor nodes cannot directly communicate with the manager. If the collectors are stolen, the sensor nodes will continue to communicate with the stolen collectors. This could result in a malicious attacker obtaining system data. Therefore, collectors must be protected at all times. In addition, if the server's private key is stolen, the system could be compromised. The manager server is the central component of the system, and as such, if it is compromised by an attack, the entire system will be at risk. Therefore, the manager server must be secured and protected at all times.

5.2 Mitigating Attacks

When collectors or sensor nodes communicate, the messages are decrypted using public key cryptography. Devices that do not have the key cannot retrieve the content of the messages. Messages are composed of the hash value and the body. In this system, we can detect message tampering by comparing the original hash value with the hash value that has been stored in the message body. The message body is composed of a request and the time stamp. The time stamp is stored every time a message is generated. The manager compares the time stamp of the received message with the stored time stamp. This allows the system to prevent replay attacks. An attacker cannot impersonate messages because they cannot obtain the secret or public keys.

6 PERFORMANCE EVALUATION

The wireless sensor device used in the experiment was the Sun SPOT[7], a Java-capable sensor that can detect both temperature and illumination. In addition, the Sun SPOT has sufficient memory to store collected observation data. Table 3 shows some Sun SPOT specifications. The Sun SPOT also has the following three power management states, which facilitate efficient power consumption.

- Deep sleep: minimal power consumption. Battery life is approximately 909 days.
- Shallow sleep: mid-level power consumption. Battery life is approximately 23 h.
- CPU busy: active processing state. Battery life is approximately 7 h.

Deep sleep, which is the power state that consumes the least power, allows for limited long term use. In this state, the sensor cannot monitor, collect, or communicate data. In addition, all programmatic threads cease operating while the device is Deep sleep. When the device is in the Shallow sleep state, it cannot monitor or communicate data, and no active threads are running on the CPU. We measured the power consumption under the following two conditions.

- Sensor nodes collected environmental data every 10 min.
- Sensor nodes transmitted data every four hours.

In this evaluation, the collectors were always within communication range of the sensor nodes. The power required to run the experiment was approximately 4.6 mAh per day. We estimated the number of theoretical working days: estimated working days = battery capacity / daily power consumption. The number of potential working days was estimated to be approximately 160. This system is intended for facilities such as museums and galleries, which are usually closed often. Therefore, the system operates long enough to be maintained when the facility is closed. In addition, to facilitate security, the encryption key will be changed when new sensor devices are installed.

7 RELATED RESEARCH

A previous study has examined an environmental monitoring system, AiryNotes[1], which uses sensor networks and micro-distributed storage architecture[3]. The goal of this system was the promotion of green living and appropriate conservation of city green space to help achieve harmony between human activities and the natural environment. The micro-distributed storage architecture was used to store data from a peer-to-peer (P2P) data pod using a JXTA dynamic ad-hoc network. However, this system did not consider data transmission security.

Table 3. Specifications of Sun SPOT

SunSPOT	
Processor board	180MHz 32bit ARM920Tcore 512KB RAM/4MB Flash memory 2.4GHz IEEE 802.15.4 of wireless USB interface 3.7V 720mAh Lithium-Ion Battery 32uA Deep Sleep mode
General-purpose sensor board	2G/6G 3-axis acceleration sensor Temperature sensor Illuminance sensor Momentary switchx2 LEDx8 of 3 colors

Therefore, we assume it would be vulnerable to attack. In contrast, our proposed system is focused on data security. There is ongoing discussion regarding authentication mechanisms used in sensor networks[6]. It is believed that the hierarchical authentication model is effective in an ad hoc network. In addition, a valid authentication system has been considered for mobile environments. Decentralized encryption/decryption methods have also been considered. In such systems, the communication can be reduced by limiting the number of key management components.

8 CONCLUSION

In this paper, we described an environmental monitoring system that collects data from wireless sensor devices that securely transmit messages. Illumination and temperature management is important in museums and other facilities that store important cultural artifacts. We used a wireless sensor device capable of operating the program. We also allowed the behavior of the wireless sensor devices to change according to the environment. The proposed system use power efficiently and is suitable for installation in facilities that cannot support wired infrastructure. Most importantly, the system ensures the secure transmission of environmental data to reduce the possibility of malicious attacks and ensure the safety and integrity of significant cultural artifacts.

References

1. Masaki Ito, Yukiko Katagiri, Mikiko Ishikawa, and Hideyuki Tokuda: Airy Notes : Environmental Monitoring by Wireless Sensor Network System for Landscape Planning Information Processing Society of Japan, Vol. 49, No. 1, pp.69 - 82 (2008).
2. Noboru Yamaguchi, Masahito Shiba, and Yoshihiro Okada: Environmental Monitoring System with a Method to Reduce the Number of Transmissions USN2008-81, pp.111-116 (2009)
3. Yuki Fujisaki, Kazuhisa Suzuki, Yusuke Yokota, and Eiji Okubo: P2P Data Pot: A Distributed Micro Storages Architecture for Sensor Networks DEW2007 D1-1
4. Yukihiro Daidai, Masahito Shiba, and Yoshihiro Okada: Encrypted communication in small wireless devices Information Processing Society of Japan, pp.483 - 485 (2011)
5. The Legion of the Bouncy Castle: http://www.bouncycastle.org/java.html
6. Naoko Ohara, Masato Oguchi: A Study of Authentication in Mobile Ad-hoc Network FIT2005, pp. 125–126 (2005)
7. Sun SPOTWorld - Home of Project Sun SPOT: http://www.Sun SPOTworld.com/