Data Integrity for Energy Measurement of Sensor Nodes as Home Services

Warodom Werapun and Jakapan Suaboot
Department of Computer Engineering, Faculty of Engineering
Prince of Songkla University, Thailand
email: {warodom, jakapan}@coe.phuket.psu.ac.th

***Abstract*—Security and energy are popular research questions for wireless sensor networks (WSNs). However, these two factors are rarely considered together in sensor network environment. This paper advocates the use of data integrity and authentication with sensor nodes as home services in order to protect data alteration. Eventually, we studied the consequence between security mechanisms and energy consumption in the sensor network.**

Keywords— Integrity; Authentication; Home services; Energy consumption; Sensor network

I. INTRODUCTION

Nowadays, many of resource-constrained sensor technologies are growing very rapidly. There are different sensors which can be equipped with an embedded board. The benefit of having many sensors is to increase more information depending on the sensor types. Many different kinds of data such as temperature, humidity, rainfall, and several gases can be collected to gather environmental knowledge. Moreover, cost of sensors is not expensive to build WSNs. Thus, many residents can have these kinds of services. Basically, users are able to retrieve the data from both the meteorological department web site and a group of sensors in WSNs. However, the reported data from the meteorological department web site may not be precise or specific to the exact location since one city may have large area with one or two meteorological departments. A distributed network of sensors as a home service [1] can be the solution in order to increase a coverage area, one concept of WSNs. These related works are focused on WSNs management as indicated in [2][3]. In addition, some researchers have made an analysis on energy property in WSNs [4][5]. However, proposed work did not consider in term of data confidential. For example, temperature or rainfall may not be private data; therefore, they can be shared to others. The integrity is only required in this case while sensitive data such as photos or videos are concerned on both confidentiality and integrity.

In this paper, we propose an implementation of sensor node as home services with data integrity and authentication on the application layer. Energy consumption analysis has been done in order to illustrate on the different message digest algorithms.

II. BACKGROUND

A. *Security*

The security properties of a service regard to Integrity and Authentication. Integrity is a concept to make data communication unchanged. MD5 or SHA-1 methods are examples of data integrity. Authentication is a method to prove the corresponding identity. HMAC is an example to do data authentication with a shared secret key. Both SHA-1 and MD5 are the most widely known, trusted and used for information verification. However, HMAC-MD5 and HMAC-SHA1 are not considered to be very strong compare with other existing authentication mechanisms that may consume more energy.

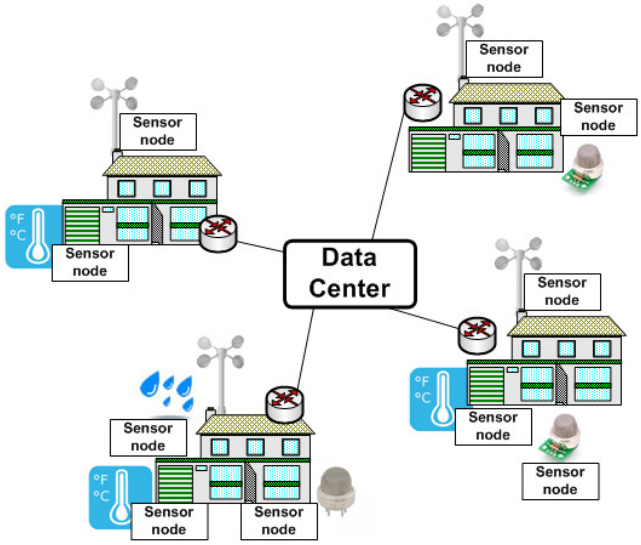

Fig. 1. Sensor node topology in centralized solution

B. *Centralized services*

Sensor nodes will be deployed in each home in order to report data more precise to the location. A home gateway will collect data and synchronize to the data center outside as shown in Fig 1. Since data are displayed to the public in data center, encryption mechanisms are not necessary for this deal while authentication and data integrity properties are vice versa.

III. IMPLEMENTATION AND EVALUATION

The metrological service for reporting temperature and humidity is selected as our tested application which is not required to have privacy and hence information integrity would be enough for these kinds of application services. We implemented sensor nodes using several sensor devices (e.g., MG-811, MQ-5, DHT-22 etc). Arduino and Raspberry PI boards are used to host sensors as shown in Fig 2.

These sensor nodes are low cost and provide data with acceptable errors. The aim of this project is to deploy a plenty of sensors in home environment and link them together in the data center. As we would like to keep them at low cost in terms of the price, data center may be one of embedded solution instead of a powerful centralized server.

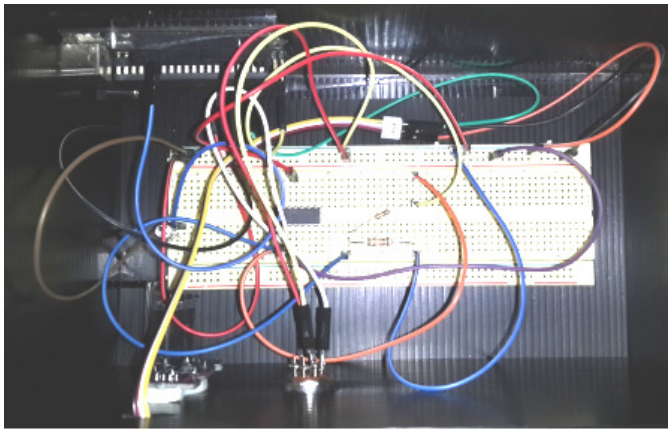

Fig. 2. Example of LPG and CO2 sensors

We evaluate and compare energy consumption of two types of data integrity and authentication for different number of nodes. The energy consumption in Joules (E) calculation is given by (1).

$$E = \alpha * N * S \quad (1)$$

α denotes energy factor for security mechanism (µjoules/byte) [6], N denotes number of nodes in a system, and S denotes an average size of messages. The trunked Pareto distribution is assumed for packet length with an average equal to 480 bytes [7].

The experimental results illustrate that SHA-1 consumes more energy than MD5 in term of data integrity. MD5 uses 128-bit algorithm while SHA-1 uses 160-bit algorithm, which digests the message slower than MD5. Moreover, HMAC-MD5 consumes energy less than SHA-1 by the reason that the digest algorithm has more impact in term of delay and also energy consumption than the input message with a secret key for the authentication purpose. In addition, both MD5 and SHA-1 consume energy in the same trend as shown in Fig 3. However, these security mechanisms consume energy in operable lifetime of sensor nodes [8].

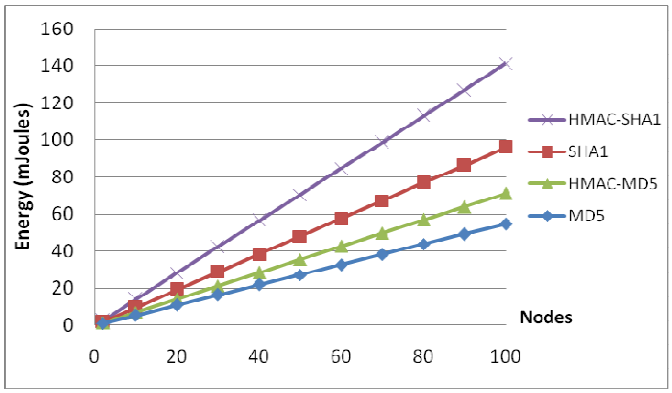

Fig. 3. Energy consumption of sensor nodes

IV. CONCLUSION AND FUTURE WORK

We introduced the concept of data integrity and authentication with sensor nodes. The prototype of sensor nodes was presented. In addition, we examined energy consumption in sensor nodes with security properties. This work showed that security mechanisms satisfy the sensor nodes with resource-constrained. In the future, we will analyze energy consumption in term of transmission powers on distributed network with other service applications.

ACKNOWLEDGMENT

This work is funded by Department of Computer Engineering, Prince of Songkla University, under the INFAR research team.

REFERENCES

[1] W. Werapun and A. Heednacram, "A Case Study of Home Service Sharing Using RELOAD," Proceedings of the 8th IASTED International Conference on Advances in Computer Science (ACS2013), pages 351-356, Phuket, Thailand, Apr 2013.

[2] S. Olariu, Q. Xu and A. Y. Zommaya, "An Energy-Efficient Self-Organization Protocol for Wireless Sensor Networks," Intelligent Sensors, Sensor Networks and Information Processing Conference, 2004, Dec 2004.

[3] J. Kim, J. Lee and S. Kim, "An Enhanced Cross-Layer Protocol for Energy Efficiency in Wireless Sensor Networks," Third International Conference on Sensor Technologies and Applications, Jun 2009.

[4] Y. Han, H. Li and J. Qiu, "The Analysis and Summary About Energy Saving Technologies of Wireless Sensor Network," 2011 International Conference on Electronic & Mechanical Engineering and Information Technology, Aug 2011.

[5] R. Hartwell, "Wireless Sensor Network Energy Use While Tracking Secure Area Intrusions," IEEE Military Communications Conference, Nov 2013.

[6] Z. Guo, W. Jiang, N. Sang and Y. Ma, "Energy Measurement and Analysis of Security Algorithms for Embedded Systems," 2011 IEEE/ACM International Conference on Green Computing and Communications, China, Aug 2011.

[7] D. Tarchi, R. Fantacci, M. Bardazzi, "Quality of service management in IEEE 802.16 wireless metropolitan area networks," In Proc of IEEE International conference on communication (ICC), Turkey, Jun 2006.

[8] O. Landsiedel, K. Wehrle and S. Gotz, "Accurate Prediction of Power Consumption in Sensor Networks," Embedded Networked Sensors, 2005. EmNetS-II. The Second IEEE Workshop, May 2005.