

Randomized RFID Identification system for Protecting User's Privacy

My Name

Division of Computer Science

Hoseo University

29-1 Sechul-Ri, Baebang-Myun, Asan, Chungeongnam-Do, Korea

myname@office.ac.kr

Your Name

Information Lab.

School of Information

Sungkyunkwan University

300 Chunchun-Dong, Jangan-Gu, Suwon, Gyeonggi-Do, 440-746, Korea

yourname@dosan.ac.kr

Abstract—Recently, the RFID system has been studied actively in ubiquitous computing as main technology. While the RFID system has much advantages, it may create new problems to the user privacy. In this paper, we present a description of previously proposed mechanisms for protecting user's privacy and their problems. A new RFID system that provides privacy protection in ubiquitous computing is then proposed. The proposed system as a way of protecting user's privacy from unwanted scanning and tracking by an adversary, however, it can traceable to the tag by an authorized administrator when necessary.

traceable to the tag by an authorized administrator when necessary.

I. INTRODUCTION

The RFID(Radio Frequency Identification) system is one of the common and useful manufacturing technologies such as supply chain management and inventory control. This identification technology uses RF signals, and it is the subject of active research as an appropriate recognition system in the ubiquitous environment. The low-cost RFID tag can read or write information on an entity without physical contact, at the same time possessing high recognition and relatively greater storing ability compared to the bar-code. Thus, this RFID tag is expected to replace the bar-code in the materials handling and distribution system [1].

Still, the RFID system unknowingly gives way to a new privacy problem, i.e., exposing too much user information such as credit information and purchase pattern. Thus, in order to utilize the RFID technology extensively in industrial fields including the materials handling and distribution system, solving the relevant security problem is definitely necessary. Several methods of protecting user's privacy have been proposed, including "Kill command" [2], "Blocker Tag" [3], "Hash-lock" [4], "Randomized Hash-lock" [5], "Re-encryption" [6] and "Hash-chain based protocol" [7].

This paper presents a description of previously proposed mechanisms and their problems. A RFID system that provides privacy protection in ubiquitous computing is then proposed. The proposed system protects user information from unwanted scanning and tracking by unauthorized users, although it can

II. RELATED WORKS

A. Introduction to RFID System

The RFID system is composed of three main elements : RFID tag, RFID reader and back-end database [8].

REFERENCES

- [1] ACI Committe 318, *Building code requirements for structural concrete (ACI 318-02) and commentary (ACI 318R-02)*, American Concrete Institute, Farmington Hills, Michigan, 2002.
- [2] A. Der Kiureghian, "Lecture note for CE193 Engineering risk analysis," in *Dept. of Civil and Environmental Eng., Univ. of California, Berkeley*, California, USA, 2001.
- [3] A. Der Kiureghian and J.-B. Ke, "The stochastic finite element method in structural reliability," *Probabilistic Engineering Mechanics*, vol. 3, no. 2, pp. 83–91, 1988.
- [4] J. W. Baker and C. A. Cornell, "Uncertainty specification and propagation for loss estimation using FOSM methods," in *Proc. of ninth Int. Conf. on Applications of Statistics and Probability in Civil Eng., ICASP9, San Francisco, California, USA, July 6-9, 2003*, Der Kiureghian, Madanat, and Pestana, Eds., 2003, pp. 669–676.
- [5] R. D. Bertero and V. V. Bertero, "Performance-based seismic engineering: the need for a reliable conceptual comprehensive approach," *Earthquake Engineering and Structural Dynamics*, vol. 31, no. 3, pp. 627–652, 2002.
- [6] H. Bottenbruch, G. I. Schuëller, and H. J. Pradlwarter, "The influence of spatial correlation of concrete strength on the failure probabilities of R/C chimneys," *Materials and Structures*, vol. 22, no. 130, pp. 255–263, 1989.
- [7] V. S. Camelo, J. L. Beck, and J. F. Hall, *Dynamic characteristics of woodframe structures*, Richmond, CA, Consortium of Universities for Research in Earthquake Engineering, 2001.
- [8] O. Chaallal and N. Ghlamallah, "Seismic response of flexibly supported coupled shear walls," *Journal of Structural Engineering, ASCE*, vol. 122, no. 10, pp. 1197–1197, 1996.