Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

An Enhanced System Security Structure for USN Environment

Jinweon Suk, Kyunghee Sun, Intae Ryoo*

Department of Computer Science and Engineering, Kyunghee University

ABSTRACT

Recently, USN (ubiquitous sensor network) technologies have been widely applied to various kinds of systems in society at large. In this paper, we identify security vulnerabilities in the systems using USN-based technologies and propose a security structure to securely protect the systems from malicious attacks. Most of the systems based on the USN technologies check a transmission error of the collected data by default during collecting and transmitting data in real time. However, these systems operate systematically without regard to security section. Therefore, these systems lack of the way to prevent and identify the data forgery and modulation when the data is transmitted and processed. The proposed scheme uses a public-key method to compensate for the security vulnerabilities in USN systems. By applying the secure structure to the automatic plant growth measurement system which is using one of USN-based technologies, we have checked whether the data is securely transmitted and processed or not on the system. The proposed method has been verified through safety analysis about the essential security requirements (confidentiality, authentication and integrity) of the threats (node authentication information disclosure, message content forgery and exposure) that may occur as typical type of attacks (node takeover, data forgery and eavesdropping) on USN systems.

KEYWORDS: Ubiquitous sensor network, Public key method, Growth measurement, Ubiquitous sensor network security, Network security

ARTICLE INFO: Received 2 September 2016, Revised 7 October 2016, Accepted 7 October 2016.

*Corresponding author is with the Department of Computer Science and Engineering, Kyunghee University, 1732, Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Republic of Korea.
E-mail address: itryoo@khu.ac.kr

1. 서 론

최근에 우리 주변에서는 유비쿼터스(Ubiquitous) 시스템 환경이 확대됨에 따라 원격지에서 실시간으로 데이터를 자동 수집 및 분석하거나 제어하려는 노력이 증가하고 있으며, 이를 실현하기 위해서는 센서 네트워크(Sensor Network)가 반드시 필요하다. 센서 네트워크는 유비쿼터스 환경 하에서 “필요한 모든 곳에 센서를 부착하여 사물에 대한 인식 정보를 기본으로 주변의 환경 정보(온도, 습도, 오염 정도, 균열 정도, 생장 정보 등)까지 탐지하고 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 네트워크 시스템”이다. 응용 분야로는 주요 기반 시설에 대한 실시간 원격 제어, 생산 및 유통, 의료 및 복지, 국방 및 교통, 농림수산업 분야 등 사회 전반에서 많은 기대를 모으고 있다[1][2].

그러나 USN 시스템들은 그 사용의 편리성과는 반대로 많은 보안 취약점을 가지고 있어 반드시 이에 대한 여러 가지 보안대책을 고려한 시스템을 설계하고 운용해야 한다. 따라서 본 논문에서는 USN 시스템의 보안 취약점을 해결하고자 USN 시스템에 활용할 수 있는 공개키 방식의 보안 구조를 제안하고, 기존의 USN 시스템에 적용하여 안전성 분석을 통하여 검증한다.

본 논문의 2장은 기존의 USN 시스템의 기본 구조와 이 시스템이 가진 보안 취약성 및 보안 요구사항에 대하여 논의한다. 3장은 공개키 방식의 USN 시스템을 위한 안전한 보안 시스템 구조를 제안하며, 4장은 제안한 보안구조에 대한 안전성 분석을 통하여 시스템의 보안 정도를 검증한다. 5장에서는 연구 결과를 돌아보고 향후 연구방향을 제시한다.

2. USN 기술 기반의 자동 생장 측정 시스템

2.1 USN 기술을 활용한 자동 생장 측정 시스템

본 논문에서 제안하는 보안 구조를 적용한 USN 시스템의 안정성 평가를 위하여 최신 USN 기술을 적용한 자동 생장측정 시스템을 사용한다[10][11][13][14]. 시스템의 기본 구성은 <그림 1>과 같으며 3개의 기본 요소로 구성된다[2][9][10]. 비접촉 식물 생장 측정 시스템(uPGMS; Real-time & Contactless Plant Thickening Growth Measurement System using the USN)은 원격관제센터의 서버에서 제어 명령을 받아 USN 센서에서 측정 대상을 측정하여 서버로 전송한다. 다음으로 데이터 수집 및 제어 시스템(uDGCS; Data Gathering & Control System based on the USN)은 uPGMS에게 생장 측정을 지시하고, USN을 통하여 데이터를 전송하고, 전송된 측정 데이터를 저장한다. 데이터 분석 및 표출 시스템(uDADS; Data Analysis and Display System on the Internet)은 센서에서 수집되어 저장된 측정 데이터를 분석하여 그 결과를 사용자에게 실시간으로 제공하는 구조를 가지고 있다.

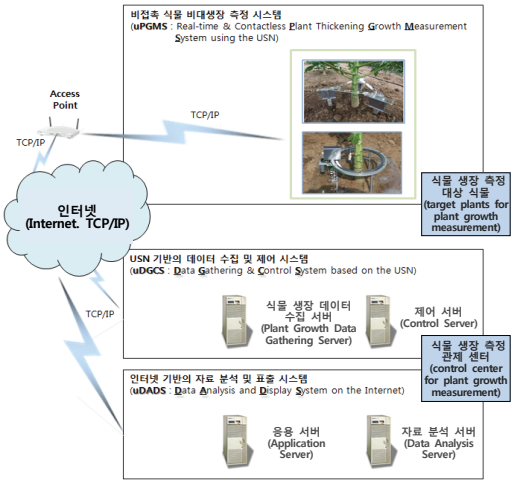

그림 1. 자동 생장 측정 시스템 구조
Figure 1. Structure of the Automated Growth Measurement System

2.2 USN을 통한 데이터 전송 처리과정

USN 기술을 이용한 자동 생장측정 시스템의 데이터 처리 과정을 살펴보면 먼저 관제 서버에서 식물 생장 측정을 위한 제어 신호를 측정 장치로 보내면 측정 장치의 USN 자율 센서들이 동작하여 대상 식물의 줄기생장을 측정한다. 측정된 신호는 디지털 신호로 변환되어 센서노드에서 싱크노드를 통하여 원격지 관제 서버에 보내져서 저장되며, 이 데이터는 실시간으로 분석되어 사용자에게 제공된다. <그림 2>는 USN 기술을 이용한 자동 생장측정 시스템의 생장 측정 및 데이터 전송과정을 나타낸 순차 다이어그램이다.

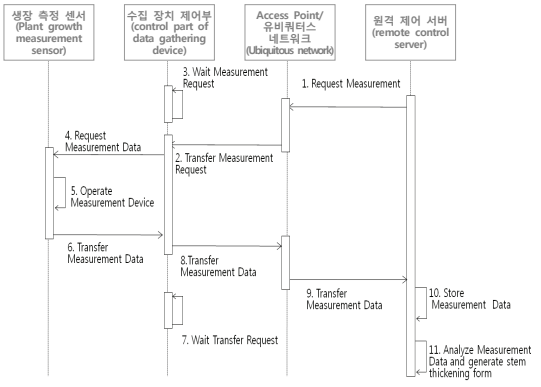

그림 2. 자동 생장측정 및 데이터 전송 과정
Figure 2. Process of Automated Growth Measurement and Data Transmission

2.3 USN 시스템의 보안 문제점

대부분의 USN 기술을 적용한 자동 생장측정 시스템과 같은 시스템들은 실시간으로 자료의 수집 및 전송 과정에서 수집 자료의 전송 오류를 검사하는 방법을 기본적으로 적용하고 있을 뿐 보안과 관련된 사항은 체계적으로 고려하여 운용하지 않고 있다. 따라서 자료의 전송 및 처리 중에 특정 데이터에 대한 위조나 변조 발생 시 이를 예방하거나 식별 및 대응할 수 있는 방법이 부족하다. 따라서 어떤 문제가 발생하면 시스템 규모나 중요성 등을 고려해 볼 때 그 피해 정도가 심각할 것으로 예상된다.

USN 시스템은 센서를 통해 주변의 정보를 수집하여 정보를 처리하는데 유용하게 사용할 수 있으며 수많은 센서노드들이 무선 네트워크를 통해 수집된 정보를 전송하게 된다. 그러나 센서노드들의 제한된 메모리, 낮은 컴퓨팅 능력, 제한된 에너지 자원과 외부의 의도적인 물리적 탈취는 네트워크 상에서 센서노드의 삽입과 탈퇴를 발생시켜 토폴로지가 변할 수 있다. 이러한 특성들은 USN 시스템의 센서 네트워크에서 수집된 정보의 신뢰성을 저하시키는 원인이 된다.

3. 이중서명 방식을 적용한 USN 보안 시스템 제안

3.1 USN 환경에서의 보안 요구사항

일반적으로 USN 시스템 환경에 필요한 보안 요구사항은 기밀성, 무결성, 인증이다.

1) 기밀성

USN 시스템의 센서 네트워크는 주로 무선 매체를 이용하기 때문에 전송되는 데이터 및 정보에 대한 도청의 위험이 존재한다. 도청 방지를 위해서는 암호화를 통해 기밀성이 보장되어야 한다.

2) 인증

USN 시스템의 센서 네트워크는 무선 매체를 이용하므로 공격자가 쉽게 정당한 노드로 위장하여 도청 또는 정보를 위변조 할 수 있다. 따라서 네트워크에 참여한 노드가 정당한 노드인지 인증 기능이 필요하다.

3) 무결성

공격자는 도청 또는 정당한 노드로 위장하여 수집한 정보를 위변조 할 수 있다. 따라서 정보가 위변조 되었는지를 검증할 수 있는 무결성이 보장되어야 한다.

3.2 제안하는 시스템 보안구조

USN 시스템에서 측정된 데이터에 대한 안전한 통신절차는 <그림 3>과 같이 원격관제서버와 센서노드 간에 이루어진다. 상호 간의 안전한 보안 통신은 크게 상호 인증, 세션키 공유, 암호와 통신, 세션 해제 단계를 통해서 이루어진다.

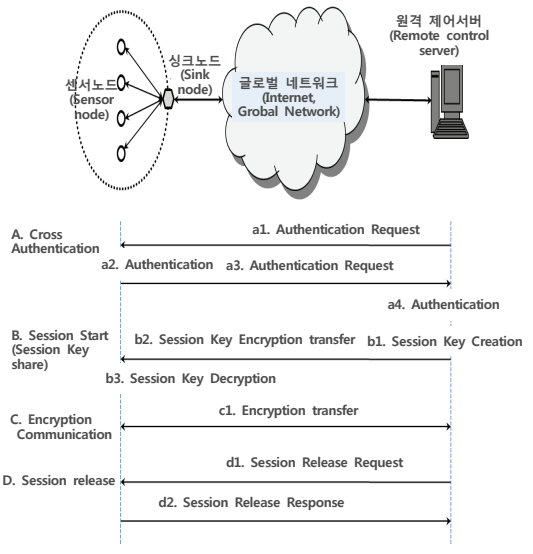

그림 3. USN 시스템을 위한 안전한 통신 절차
Figure 3. Secure Communication Process for USN System

본 논문에서 안전한 통신 절차를 설명하기 위하여 사용하는 표기법은 다음과 같다.

- SK_s, PK_s : 관제서버의 개인키와 공개키
- SK_c, PK_c : 센서노드의 개인키와 공개키
- K_s : 서버의 세션키
- $E(M)SK_s$: 메시지 M을 개인키 SK_s로 암호화
- $D(M)PK_s$: 메시지 M을 공개키 PK_s로 복호화
- h(M) : 메시지 M을 해시 함수 처리

3.3 상호 인증 절차

상호 인증은 공개키 방식을 이용하여 노드 상호간에 적법한 단말임을 인증하는 단계로써 사전에 센서노드에 기록해 놓은 센서노드의 공개키와 개인키에 기초하여 전자서명 절차로 상호 인증한다.

1) 관제서버의 인증 요청

관제서버가 자신의 인증정보를 센서노드에게 전달하여 인증을 받는 단계이다.

서버는 인증 메시지 M_s와 자신의 개인키로 전자서명을 한 서명값 $E(h(M_s))S_s$를 센서노드에 전달하여 자신에 대한 인증을 요청한다. 이 때 인증에 사용되는 메시지 M_s는 서버 아이디 ID_s와 센서노드 아이디 ID_c, 인증시점의 시간값인 T_i로 구성된다.

$$server\_auth\_request = \{ M_s, E(h(M_s))SK_s \}$$
$$M_s = \{ ID_s, ID_c, T_i \}$$

2) 관제서버 인증

센서노드는 관제서버로부터 수신한 암호화된 $E(h(M_s))SK_s$ 값으로부터 복호화 된 $h(M_s)$ 값과 수신된 $\{ ID_s, ID_c, T_i \}$로부터 구한 $h'(M_s)$를 비교하여 일치 여부로 관제서버를 인증한다.

$$h(M_s) = D(E(h(M_s))SK_s)PK_s$$
$$h'(M_s) = h(ID_s, ID_c, T_i)$$

3) 센서노드의 인증 요청

센서노드가 관제서버에게 자신의 인증정보를 전달하여 인증을 받는 단계이다.

센서노드는 인증 메시지 M_c와 자신의 개인키로 전자서명을 한 서명값 $E(h(M_c))SK_c$를 관제서버에 전달하여 자신에 대한 인증을 요청한다. 이 때 인증에 사용되는 메시지 M_c는 센서노드 아이디 ID_c와 서버 아이디 ID_s, 수신된 T_i 값으로 구성된다. 이 때 T_i 값은 센서노드가 새롭게 생성하지 않고 관제서버로부터 수신한 T_i 값에 1을 더한 값을 사용한다.

client_auth_request = { M_c, $E(h(M_c))SK_c$ }
Mc = { ID_c, ID_s, T_i+1 }

4) 센서노드 인증

관제서버는 센서노드로부터 수신한 암호화된 $E(h(M_c))SK_c$ 값으로부터 복호화 된 $h(M_c)$ 값과 수신된 { ID_c, ID_s, T_i }로부터 구한 $h'(M_c)$를 비교하여 일치 여부로 관제서버를 인증한다. 이 때 관제서버는 복호화된 M_c로부터 추출하여 계산한 T_i와 자신이 센서노드로 보낸 T_i가 일치함을 확인함으로써 센서노드가 정상적으로 자신이 보낸 메시지를 수신했음을 확인한다.

$h(M_c) = D(\ E(h(M_c))SK_c\ )PK_c$
$h'(M_c) = h(ID_c, ID_s, T_i+1)$

3.4 세션키 공유 절차

상호 인증을 마친 관제서버가 세션 동안에 사용할 세션키를 대칭키 방식으로 생성하여 공개키 방식을 이용하여 암호화하고 센서노드에게 전달하는 과정이다.

1) 센서노드로 세션키 전송

관제서버는 세션 동안에 측정 데이터 전송에 사용할 세션키 K_s를 생성하여 센서노드의 공개키 P_c로 암호화하여 센서노드에게 전달한다.

server_sessionkey_transfer = { $E(K_s)PK_c$ }

2) 센서노드의 세션키 복호화

센서노드는 암호화되어 수신된 세션키를 자신의 개인키 SK_c로 복호화하여 세션키 K_s를 확보한다.

$K_s = D(\ E(K_s)PK_c\ )SK_c$

3.5 암호화 통신절차

세션키 K_s를 공유하게 된 관제서버와 센서노드는 대칭키 방식을 이용하여 전송할 데이터를 암호화하여 상대에게 전달하는 과정이다.

1) 센서노드의 측정 데이터 암호화 전송

센서노드는 전송 메시지 M_c를 세션키 K_s로 대칭키 방식으로 암호화해 관제노드로 전송한다. 이 때 센서노드의 전송 메시지 M_c는 측정 데이터 D_c와 측정 데이터를 해시함수로 처리한 $h(D_c)$로 구성된다.

client_data_transfer = { $E(M_c)K_s$ }
M_c = { D_c, $h(D_c)$ }

2) 관제노드의 측정 데이터 복호화

관제서버는 센서노드로부터 수신한 암호화된 데이터를 세션키 K_s로 복호화하여 복호화 된 D_c로부터 $h'(D_c)$ 값을 구하여 수신된 $h(D_c)$와 비교하여 그 결과의 일치 여부에 따라 수신된 데이터에 대한 무결성을 확인한다.

$M_c = D(\ E(M_c)K_s\ )K_s$

3.6 세션 해제

세션 해제는 관제서버의 해제요청에 대해 센서노드가 응답함으로써 성립된다. 관제서버는 세션종료 요청정보를 세션키 K_s로 암호화하여 센서노드에게 보내고, 센서노드는 세션종료 응답정보를 세션키 K_s로 암호화하여 관제노드에게 응답하는 것으로써 이루어진다.

1) 관제서버의 세션해제 요청

관제서버는 세션종료 요청정보 M_s를 세션키 K_s로 암호화하여 센서노드에게 보낸다. 이 때 세션종료 요청에 사용되는 메시지 M_s는 서버 아이디 ID_s와 센서노드 아이디 ID_c, 세션종료 요청 시점의 시간값인 T_i로 구성된다.

$$server\_sessionover\_request = \{ E(M_s)K_s \}$$
$$Ms = \{ ID_s, ID_c, T_i \}$$

2) 센서노드의 세션해제 응답

관제서버로부터 세션해제 요청정보를 받은 센서노드는 관제서버에게 세션해제 응답정보를 세션키로 암호화하여 응답하는 것으로써 세션 해제가 이루어진다. 이 때 센서노드가 사용하는 세션해제 응답 메시지 M_c는 센서노드 아이디 ID_c와 서버 아이디 ID_s, 관제서버에서 수신한 M_s로부터 추출한 T_i 값에 1을 더한 값으로 구성된다.

$$client\_sessionover\_reply = \{ E(M_c)K_s \}$$
$$Mc = \{ ID_c, ID_s, T_i+1 \}$$

세션해제 응답정보를 수신한 센서노드는 복호화된 M_c로부터 추출하여 계산한 T_i와 자신이 센서노드로 보낸 T_i가 일치함을 확인함으로써 센서노드가 정상적으로 자신이 보낸 메시지를 수신했음을 확인하고 세션을 종료한다.

4. 안전성 평가

본 논문에서 제안한 보안구조를 적용한 USN 시스템인 농산물 재배관리 시스템에 발생 가능한 대표적인 공격 유형은 노드 탈취, 데이터 위변조이다[13]. 따라서 제안한 시스템에서도 가능한 공격의 유형들을 노드 탈취, 데이터 위변조, 도청으로 가정하였으며, 이러한 공격 유형에 대하여 안정성을 분석하였다.

4.1 노드 탈취에 대한 안전성 분석

본 논문에서 제안한 시스템 보안구조에서는 관제서버와 센서노드 간 데이터 교환 이전에 공개키 방식에 의한 상호인증 과정을 통해 적법한 노드인지 확인을 하고, 상호 인증이 확인된 후에 세션키를 교환하여 세션키에 의한 비밀 통신을 함으로써 탈취된 노드에 대한 인증과 기밀성을 제공한다. 상호 인증 단계에서 인증 요청자는 수신한 인증 메시지와 자신이 구한 해시함수 결과를 비교하여 송신자 개인키로 서명한 결과에 대한 무결성 입증을 함으로써 당사자를 정당한 상대로 인증할 수 있다.

4.2 데이터 위변조에 대한 안전성 분석

제안한 보안구조는 관제서버와 센서노드 간에 상호인증을 마친 상태에서 공개키 방식을 이용하여 비밀리에 상호 세션키를 공유하고, 공유된 세션키를 이용하여 비밀 통신을 함으로써 데이터 전송에 대한 기밀성을 제공한다. 또한 세션키를 이용한 데이터 전송 시 전송 데이터에 대한 해시값을 함께 전송하여 전송 데이터에 대한 무결성도 제공한다.

4.3 데이터 도청에 대한 안전성 분석

제안한 보안구조에서는 관제서버와 센서노드 간 데이터 전송은 비밀리에 공유한 세션키를 이용한 대칭키 방식의 암호화 전송을 함으로써 데이터 전송에 대한 기밀성을 제공한다. 또한 데이터 전송 시 해시값 전송에 의한 무결성을 제공함으로써 암호화된 데이터가 노출되면 위변조는 불가능하다.

제안한 USN 시스템을 위한 보안 구조의 안전성 분석결과는 다음 <표 1>에 제시하였으며, 제안한 보안 시스템의 설계목표인 기밀성, 인증 및 무결성을 모두 충족시키는 것을 확인 할 수 있다.

표 1. 제안한 USN 시스템 보안 구조의 안전성 분석
Table 1. Safety analysis of the proposed security structure for USN system

type of attacks	the threats that may occur	the essential security requirements	Whether the security provided
node takeover	node authentication information exposure	confidentiality	O
	node authentication information possession	authentication	O
data forgery and modulation	message content forgery and modulation	integrity	O
eavesdropping	message content exposure	confidentiality	O

5. 결 론

본 논문은 USN기반 기술을 활용한 시스템들의 보안 취약점을 파악하고, 이를 개선하기 위하여 안전한 보안 구조를 제안하였다. 제안된 방법은 공개키 기반의 이중서명 방식을 사용하였으며, 이를 USN 기반 시스템인 자동 식물 생장 측정 시스템에 적용하여 안전성을 검증하였다. 안전성 분석결과 USN 시스템에서 발생할 수 있는 대표적인 공격유형인 노드 탈취, 데이터 위변조, 도청의 위협에 대해 필수적인 보안 서비스인 기밀성, 인증, 무결성이 안전하게 제공되는 것을 확인하였다.

본 연구에서 제안한 보안 구조를 적용하여 검증한 USN 시스템은 노드의 수가 제한적이므로 향후 대규모 센서노드 운용을 위해 라우팅 보안을 포함한 가용성, 익명성, 권한 관리, 안전한 로밍 등에 대한 연구와 빅데이타, 클라우드 컴퓨팅 및 포그 컴퓨팅을 포함하는 IoT(Internet of things) 환경에서의 다양한 종류의 센서 장치 및 라우팅, 데이터베이스 관리 정책 등의 연구가 필요하다.

References

[1] M. Weiser, *Hot topics - ubiquitous computing*, IEEE Computer, Vol. 26, Issue: 10, pp. 71-72, 1993.

[2] S-Y. Nam, *The ubiquitous sensor network architecture and applications*, SangHakDang, 2006.

[3] S-G. Lee, H-D. Lee, G-I. Jeong, and D-H. Choe, *Trend of secure USN information protection technology*, Electronics and telecommunications trends, Vol. 23, No. 4, pp. 72-79, 2008.

[4] S-W. Lee, *Application model development of key management schemes in ubiquitous sensor network*, Korea Internet & Security Agency, Final Research Report (KISA-WP-2009-0043), 2009.

[5] S. H. Park, S. M. Park, and S. H. Shin, *Design of protocol for RFID/USN security*, Journal of Korea Safety Management & Science, Vol. 9, No. 3, pp. 103-109, 2007.

[6] S. H. Kim, Y. S. Kang, B. H. Chung, and K. I. Chung, *Technical trend of security in ubiquitous sensor networks*, Electronics and

telecommunications trends, Vol. 20, No. 1, pp. 93-99, 2005.

[7] H. W. Kim, S. J. Kim, and K. H. Oh, *Trend of security technical development in Sensor network*, KIISC review. Vol. 18, No. 2, pp. 33-39, 2008.

[8] S. H. Na, *Secure ID-based proxy authentication scheme and secure mobility support employing PMIPv6 for wireless sensor network*, Kyunghee University Master's Thesis, 2010.

[9] Y. C. Lee, S. U. Cho, and C. H. Oh, *Implementation of crops monitoring system using wireless sensor networks*, The Journal of Korea navigation institute Vol. 12, No. 4, pp. 324-331, 2008.

[10] J. W. Suk, and I. T. Ryoo, *Implementation of non-contact plant growth measurement system based on USN technologies*, Journal of the Korea Society of Computer and Information, Vol. 15, No. 10, pp. 137-145, 2010.

[11] J. W. Suk, S. H. Kim, and I. T. Ryoo, *Non-contact plant growth measurement method and system based on ubiquitous sensor network technologies*, Sensors, 2011, 11(4), pp. 4312-4334, 2011.

[12] S-C. Jang, S-I. Ham, Y-J. Hwang, I-M. Na, G-P. Yun, Y-J. Lee, J-G. Lee, and B-M. Jeong, *RFID/USN-based cultivation monitoring system*, Journal of Korea Institute of Industrial Engineering/Korean Operations Research and Management Science Society Joint Conference/Spring 2006, pp. 1264-1271. 2006.

[13] J. W. Suk, *Non-contact plant growth measurement method and system based on ubiquitous sensor network technologies*, Kyunghee University PhD thesis, 2011.

[14] J. W. Suk, I. T. Ryoo, and W. S. Na, *Implementation and evaluation of communication middleware for real-time distributed simulation system,* Journal of The Knowledge Information Technology Society, Vol. 5, No. 5, pp. 141-148, 2010.

[15] B-C. Jeon, S-Y. Cho, and S-J. Lee, *An implementation of agricultural monitoring and automation system based on embedded server PDF icon,* Journal of The Knowledge Information Technology Society, Vol. 9, No. 3, pp. 387-399, 2014.

USN 환경 기반 시스템을 위한 강화된 보안 구조

석진원, 선경희, 유인태

경희대학교 컴퓨터공학과

요 약

최근 USN(유비쿼터스 센서 네트워크) 기술은 사회 전반의 다양한 시스템에 폭넓게 적용되고 있다. 본 논문에서는 USN기반 기술을 활용한 시스템들의 보안 취약점에 대하여 파악하고, 이를 개선하기 위한 안전한 보안 구조를 제안한다. 대부분의 USN 기술을 적용한 시스템들은 실시간으로 자료의 수집 및 전송 과정에서 수집 자료의 전송 오류를 검사하는 방법을 기본적으로 적용한다. 그러나 보안과 관련된 사항은 체계적으로 고려하여 운용하지 않고 있다. 따라서 자료의 전송 및 처리 중에 데이터에 대한 위조나 변조 발생 시 이를 예방하거나 식별할 수 있는 방법이 부족하다. 제안하는 방법은 USN 시스템의 보안 취약점을 보완하기 위해 공개키 방식을 사용하였으며, 이를 USN 기반 시스템인 자동 식물 생장 측정 시스템에 적용하여 데이터의 안전한 전송 및 처리가 가능하도록 제안하였다. 그리고 제안한 방법이 USN 시스템에서 발생할 수 있는 대표적인 공격유형(노드 탈취, 데이터 위변조, 도청)의 위협(노드 인증 정보 노출 및 소유, 메시지

내용 위변조 및 노출)에 대해 필수적인 보안 서비스(기밀성, 인증, 무결성)를 제공하는지 여부를 안전성 분석을 통해 검증하였다.

Jin Weon Suk received the bachelor's degree in the Department of Electronic Engineering from Kumoh National Institute of Technology in 1990. He received the M.S. degree in the Department of Defense Science from Korea National Defense University in 1996. He received the Ph.D. degree in the Department of Computer Science and Engineering from Kyunghee University in 2011. He is director at V&BT Corporation. His current research interests include IT convergence, Ubiquitous sensor network, project management, and network security. He is a member of the KKITS.

E-mail address: sjw0176@unitel.co.kr

Kyunghee Sun received the bachelor's degree in the Department of Computer Science and Statistics from Jeju University in 1998. She received the M.S. degree in the Department of Computer Science and Statistics from Jeju University in 2008. She completed the Ph.D. course in the Department of Computer Science and Engineering from Kyunghee University in 2016. From 2006 to 2014, she was a senior researcher at Jeju Technopark. Her current research interests include IoT, IT convergence, network protocol, and network security. She is a member of the KKITS.

E-mail address: sunkh0507@khu.ac.kr

Intae Ryoo received the bachelor's degree in the Department of Electronic Engineering from Yonsei University in 1987. He received the M.S. degree and the Ph.D. degree in the Department of Electronic Engineering from Yonsei University in 1989 and 1994, respectively. He received the Ph.D. degree in the Department of Computer Engineering from Tokyo University in 1997. From 1997 to 1999, he was a senior researcher at Samsung Electronics Co., Ltd. He has been a professor in the Department of Computer Science and Engineering at Kyunghee University since 1999. His current research interests include IoT, internet technology, network QoS/QoE, traffic management, wireless communication, and network security. He is a member of the KKITS.

E-mail address: itryoo@khu.ac.kr