최종연구보고서	KISA-WP-2009-0043

USN 환경에서의 키관리 기술의 적용 모델 개발

Application Model Development of key Management Schemes in Ubiquitous Sensor Network

수 탁 기 관 : 국 민 대 학 교 산 학 협 력 단

2009. 09.

한국인터넷진흥원
Korea Internet & Security Agency

제 출 문

한국인터넷진흥원장 귀하

본 보고서를 " USN 환경에서의 키 관리 기술의 적용모델 "의 최종 연구개발 결과 보고서로 제출합니다.

2009 년 9 월 30 일

수탁 기관 : 국민대학교 산학협력단
연구책임자 : 교 수 이 상 환 (국민대학교 컴퓨터공학부)
참여연구원 : 연 구 원 차 선 민 (국민대학교 컴퓨터공학부)
연 구 원 정 민 선 (국민대학교 컴퓨터공학부)
연 구 원 임 일 우 (국민대학교 컴퓨터공학부)
연 구 원 이 영 준 (국민대학교 컴퓨터공학부)

요 약 문

1. 제목

USN 환경에서의 키관리 기술의 적용모델 개발

2. 연구개발의 목적 및 중요성

본 연구의 목적은 USN 보안 기술에서 활용되는 키에 대한 분배 및 관리 기술의 적용모델 개발이다. USN의 다양한 키 관리 기술을 USN의 상황에 따라 적절하게 사용할 수 있도록 하는 모델을 제시하는 것은 USN의 설치에 있어서 매우 필수적이라 할 수 있다.

3. 연구개발의 내용 및 범위

USN 환경에서의 키 관리 기술 및 표준화 동향 분석 : Pairwise 키, Group 키, 마스터 키 기반 등의 사전키 분배 및 공개키 기반 분배 기법을 분석하고, IP-USN 기술, ZigBee, IEEE802.15.4 등 USN 보안 기술 표준화 동향을 분석한다.

USN 공격 형태별 키 관리 유형 분류 : 전송 정보에 대한 도청 및 데이터 위변조 등 USN 키 분배 기술에 대한 공격 형태를 분석하고, USN 키 분배에 대한 공격 형태별 키 관리 기술 분류 및 요구사항을 도출한다.

USN 키 관리 기법의 효율성 분석 및 적용 모델 개발 : u-City 등 국내 USN 시범 서비스에 적용을 위한 USN 키 관리 기술 구현 및 효율성을 분석하고, 시범 서비스 내 활용 가능한 USN 키 관리 기술 적용모델을 개발한다.

4. 연구결과

USN 환경에서 사용되는 키 관리 기법 기술 조사 및 비교 분석 : 사전키 기반 분배 기법(마스터 키, Pairwise 키(Random Pairwise key), 확률론적 키(Blom's Polynomial, q-합성수, Multi-path), 그룹 키), 공개키 기반 분배 기법(ECC, ECDH), 센서 네트워크 보안 프로토폴(SPIN, LEAP)등의 다양한 키 관리 기술을 조사하여 분류.

USN 공격 형태 조사 및 분석 : USN 환경에서 일어날 수 있는 대표적인 공격 형태 -도청, 데이터 위변조, 서비스 거부 공격, 라우팅 공격, 물리적 공격-조사 및 분석, 기존에 다양한 기준으로 공격 형태를 분류한 것을 조사 및 분석.

USN 보안 기술 표준화 동향 분석 : USN 보안 기술 표준화에 대한 필요성과 국내외 보안 기술 표준화 동향 분석

u-City 시범 서비스 조사 및 분석 : 다양한 u-City 시범 서비스의 실제 사례를 조사하여 분석

USN 환경에서의 키 관리 기술의 적용 모델 도출 연구 : 조사한 u-City 시범 서비스를 바탕으로 시범 서비스에 적용을 위한 USN 키 관리 기술 적용 모델 개발

USN 환경에서의 키 관리 기법의 효율성 분석 시뮬레이션 : USN 환경에서의 키 관리 기술의 적용 모델에 대한 USN 키 관리 기술 구현 및 시뮬레이션과 효율성 분석 연구

5. 활용에 대한 건의

USN 환경의 보안 기술 표준화로 국내와 국제 보안 기술 표준화를 위해 센서 노드 간의 인증 및 키 분배를 통하여 보안 세션을 수립할 수 있도록 활용 및 접목 가능

6. 기대효과

USN 보안 기술의 표준화로 국내뿐만 아니라 국외의 USN 보안 기술 표준화 발전에 기여

SUMMARY

1. Title

Application Model Development of Key Management Scheme in Ubiquitous Sensor Networks

2. Purpose of the study

The purpose of this study is to application model develop of key management scheme in USN. Providing an appropriate key distribution model that can accommodate specific conditions and environments of USNs is critical to the deployment of USN.

3. Contents and scope

Survey on the USN key management schemes and the trends on standardization of the USN Key management schemes. : We analyze the pairwise key, Group key, Master key based key predistribution schemes and public key based key distribution schemes and several USN security enhancement technologies such as IP-USN, ZigBee, IEEE 802.15.4.

Categorization of key distribution scheme depending on the attack types : We analyze several attack schemes to the key distribution schemes

including eavesdropping, data modification and categorize the key management schemes depending on the attack types. We build requirements on the key management schemes for various attack types.

Analysis on the performance of key management schemes and development of an application model : We analyze the performance of several USN key management schemes that can be used in many domestic USN services such as u-City. We develop an application model of the key management schemes that can be used in the testbeds of domestic USN services.

4. Results of the study

Survey and analysis on the key management schemes for the USN : We conduct a survey on various key management schemes including Key predistribution schemes (Master key, pairwise key (Random pairwise key), Probabilistic Key (Blom's Polynomial, q-composite, Multi-path), Group key), Public key based key distribution schemes (ECC, ECDH), sensor network security protocol (SPIN, LEAP).

Survey and analysis on USN attack types : We categorize and list the various attacks that can be launched against USNs - Eavesdropping, Data modification, Denial of Service, Routing Attack, Physical Attack. We investigate and analyze many categorization proposals of attacks based on various criteria.

Analysis on the trends of USN security standardization procedures : We identify the necessity of the standardization of the USN security technology and analyze the trends of USN security standardization procedures.

Analysis on the testbeds of u-City : We collect various cases of u-City testbeds and analyze the characteristics.

Application model of the key management schemes in USN environments : Based on the characteristics of u-City testbeds, we develop a unified key predistribution framework that can be applied to the various u-City testbeds.

Simulation based evaluation on the performance of various key predistribution schemes in the USN environments : We develop a simulation tool to evaluation the performance of the unified framework and other existing schemes and evaluation the performances.

5. Expected effects and applications

The proposed unified framework can be used for various USN deployments. Our framework is easily applied to various USNs and the standardization of the key management schemes can enhance the security of the USNs. To be specific, the key predistribution schemes enable communications among sensor nodes to be secure and robust.

목 차

Contents

그림 목차

표 목차

제 1 장 서 론

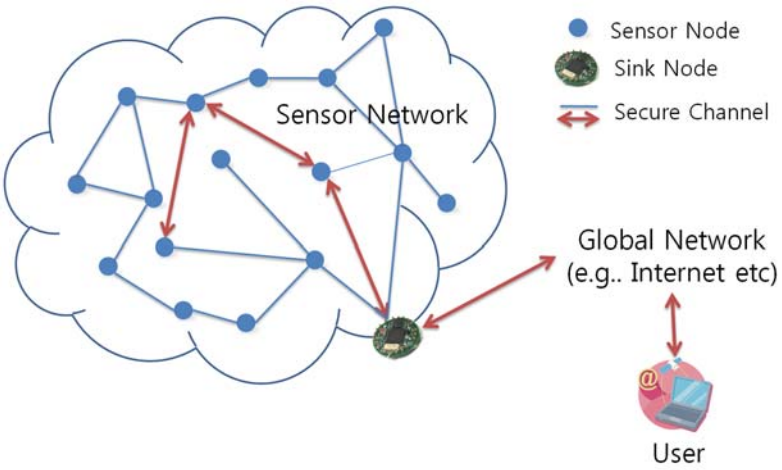
본 장에서는 USN 환경에서의 키 관리 기술의 적용 모델을 개발하기 위해서 배경 지식이 될 수 있는 USN 키 관리 기술과 공격 및 보안을 간략히 설명한다. 1절에서는 USN과 USN에서 일어날 수 있는 공격 및 보안의 정의를 설명한다. 2절에서는 USN에서 사용 할 수 있는 키 관리의 범위와 그에 따른 키 관리 기술의 종류를 설명한다. 3절에서는 USN 환경에서 보안의 정의와 필요성을 설명하고, 기밀성, 무결성, 가용성, 익명성 등과 같은 USN 보안 요구사항을 알아본다. 4절에서는 USN 환경에서 일어날 수 있는 공격들을 다양한 관점에서 분류되어진 것이다.

제 1 절 USN(Ubiquitous Sensor Network)

1. USN 개요

유비쿼터스 센서 네트워크(USN : Ubiquitous Sensor Network)는 유비쿼터스 컴퓨팅을 위한 네트워크로 RFID 태그 노드(RFID tag node) 또는 센서 노드(sensor node) 등으로 이루어진 무선 네트워크이다.

USN은 다수의 센서 노드, 싱크 노드 및 게이트웨이를 통해 언제 어디서나 쉽게 사물 및 환경 정보를 감지·저장·가공·통합하여 무선으로 전송 할 수 있다. 즉, USN의 다수의 센서 노드들이 시간과 장소에 구애 받지 않고 사물 및 환경적 변화를 감지하여 싱크 노드로 정보를 전달한다. 그러면 싱크 노드와 무선으로 연결된 서버를 통해 노드에게 정보가 전달된다[1, 2, 3, 4]. (그림 1-1)은 센서 네트워크 기본 구성도이다. 즉, 센서 노드들이 센싱 된 정보를 송수신하여, 이러한 정보를 싱크 노드에게 전달하면 네트워크(혹은 인터넷)를 통해 사용자에게 전달되는 것이다.



(그림 1-1) 센서 네트워크 기본 구성도

USN은 센서 노드를 이용하여 우리의 삶을 자동화 시키고, 편리함을 제공한다. 이러한 USN은 국가 경쟁력을 높일 수 있는 차세대 성장 동력이자 사회적으로 기술 혁신을 가져 올 수 있는 중요한 미래 기술 중 하나이다. USN 기술을 이용하여 홈 네트워크, 텔레매틱스, RFID 서비스 등의 기반 구조를 형성하고, 국방, 제조, 건설, 교통, 교육, 환경, 물류/유통 및 농/축산업 등의 다양한 분야에 걸쳐 사용되고 있다[5, 6, 7].

(그림 1-2) USN(Ubiquitous Sensor Network)

2. USN 공격

일반적으로 센서 네트워크(Sensor Network)는 컴퓨팅 파워, 저장 공간(메모리), 대역폭 등의 제약 사항 때문에 기본 유선 PC 환경에서 사용하는 정보 보호 서비스를 그대로 적용하는데 어려움이 있다. 따라서 기존의 네트워크 환경과 다르게, 노드들이 지리적으로 넓게 분산되어 있어서 공격자로부터 노드 탈취 및 공격을 당하기 쉽고 노드의 메모리나 컴퓨팅 파워, 전원, 대역폭 등의 제약 사항 때문에 물리적 공격에 약하며 무선 통신으로 망을 관리하고 데이터를 전송 하므로 이를 이용한 네트워크 공격이 쉽게 이루어진다.

USN에서의 공격 모델은 크게 외부자/내부자 공격과 능동적/수동적 공격으로 분리 된다. 공격 종류는 센서 정보의 도청, 노드 캡쳐, 비정상적인 패킷의 유통에 의하여 인한 네트워크 전체를 마비시킬 수 있는 서비스 거부 공격(DoS : Denial-of-Service), 허위 노드 침입, 메시지 재사용 등의 데이터 위변조, 라우팅 공격, 물리적 공격, 강경파 사용을 통한 서비스 방해 공격 등이 있다[6, 8, 9, 10].

3. USN 보안

센서 네트워크 환경에서 센싱(Sensing)된 데이터는 개인의 프라이버시 및 기업의 비밀정보와 관련되어 있다. 그렇기 때문에 데이터에 대한 도청 또는 위변조 등과 같은 공격에 노출되지 않도록 해야 한다. 따라서 센서 네트워크의 특성을 고려하여 안전한 USN 플랫폼 설계가 필요하다. 또한 센서 네트워크의 보안 통신 및 관리 기술을 포함하여 USN 서비스를 구성해야 한다.

센서 네트워크에서 많은 센서 노드들이 무선 네트워크로 전송하는 정보를 안전하게 보호하기 위해서 내부적으로는 센서 노드의 보안 기능을 강화하고, 전체 네트워크를 보호하기 위해 계층적으로 보안 요구 사항을 만족 시켜야 한다[8, 9, 10].

제 2 절 USN 환경에서의 키 관리 기술

1. 키 관리 범위

키 관리 기술은 센서 네트워크 환경에서 제한된 자원으로 효율적이고 안전한 키 설립 방법을 설계하는 것이다. USN 환경에서 센서 노드들 사이의 안전한 통신을 위해서는 키가 반드시 필요하다. 키는 암호 기술을 기반으로 하여 키의 생성, 분배, 활용까지 모든 부분에서 신뢰성이 있어야 하며, 모든 과정이 안전하게 이루어 져야 한다.

키의 생성은 통신을 하기 위해 키를 안전하게 생성 할 수 있는 절차를 말한다. 암호 시스템에서 생성되는 키는 이용 형태에 따라 기본적으로 마스터 키(Master key)와 세션 키(Session key)로 구분된다. 세션 키는 종단 시스템(End System) 사이의 통신에서 임시로 사용하는 키를 말하며 대개 가상회로나 트랜스포트 연결과 같은 논리적 연결이 이루어지는 동안만 사용한 후에 폐기된다. 따라서 세션 키는 키의 수명이 짧고, 키 분배 센터가 종단 시스템이나 사용자와 공유하고 있는 마스터 키를 사용하여 안전하게 암호화되어 센서 노드에게 전송된다. 마스터 키는 시스템이나 사용자가 키 분배 센터와 공유하는 유일한 키이다. 센서 네트워크에서 마스터 키를 사용할 경우 전체 센서 네트워크가 가지고 있는 키는 마스터 키 하나뿐인 것이다. 따라서 USN에서 키의 노출은 전체 네트워크가 위험해 질 수 있으므로 키의 생성에 특별한 주의가 요구된다.

키 분배는 키가 생성된 위치로부터 암호 알고리즘에서 사용된 위치로 암호화 키를 전송해 주는 과정이다. 이는 통신을 위해 센서 노드들에게 생성된 키를 분배해야한다. 키를 분배하는 방법은 키의 방식에 따라 대칭 기술을 이용하는 방법과 비대칭 기술을 이용하는 방법으로 나뉜다. 또한 노드에 저장되는 데이터에 따라 크게 Pairwise 키 방식과 마스터 키 방식, 랜덤 키 방식 등으로 나눌 수 있다.

키 저장은 나중에 사용할 키를 안전하게 저장하는 것이고, 키 보관은 키를

사용한 후에 키들의 유효 기간이 끝나거나 취소될 경우 키들의 안전한 저장을 위한 절차를 제공하는 것이다[11, 26].

2. 키 관리 기술 및 센서 네트워크 보안 프로토콜

USN에서 키를 구성하기 위해 가장 먼저 고려해야 할 것은 암호학적인 키를 설정하는 문제이다. 이러한 키는 센서 노드 사이에서 정보를 교환하거나 교환된 정보를 보호 하는데 사용된다.

가장 고전적인 키 설정 방법으로 공개키 방법이 있다. 이 방법은 노드가 네트워크 내에서 다른 노드와 안전하게 키를 설정 할 수 있다는 장점이 있다. 하지만 현재 센서 노드들은 자원 제약성 때문에 공개키를 이용하기에 어려운 실정이다[58]. 그래서 초기 센서 네트워크 보안은 대칭키를 기반으로 하는 연구가 진행 되어 왔으나 현재 공개키 시스템을 적용하려는 시도가 다시 활발히 진행 중이다[66].

키 관리 기술에는 싱글 네트워크 와이드 키(Single network-wide key), Pairwise 키 설립(Pairwise key establishment), 신뢰된 베이스 스테이션(Trusted base station)을 이용하여 키를 설립하는 방법이 있다. 그리고 공개키 기법(Public key schemes), 키 사전 분배 기법(Key pre-distribution schemes), 동적 키 관리(Dynamic Key management)를 이용하여 키를 관리하는 방법 등이 있다.

Single network-wide key는 키 설립 기법 중 가장 단순한 방법으로 하나의 단일 키(Single key)가 모든 노드들에게 미리 설치된다. 모든 노드들은 이 키를 사용하여 메시지를 암호화, 복호화 하게 된다. 이 방법은 메모리의 공간을 적게 사용한다는 장점이 있지만 공격자의 공격을 받기 쉽다는 단점이 있다.

Pairwise key establishment는 WSN(Wireless sensor network)에서 가장 효율적인 키 설립 방법으로 모든 노드가 유일한 키를 가진다. 센서 네트워크의 노드가 n개 있을 때 각 노드는 n-1 개 키를 가진다. 각 노드는 다른 모든 노드들의 신원을 확인할 수 있다. 예를 들어 센서 네트워크의 모든 노드의 개수가 10,000개라면 각 노드는 9,999개 키를 저장하기 위한 메모리가 필요하다.

센서 노드의 자원은 제한되어 있기 때문에 Pairwise key establishment는 센서 노드가 적은 규모의 네트워크에 적합하다. 다시 말하면, Pairwise key establishment는 네트워크의 노드들의 수를 n이라고 하면, 모든 노드들이 n-1 개 키를 가지기 때문에 노드의 수가 많은 네트워크에서는 센서 노드의 자원 제약성으로 인해 적합하지 않다.

이 문제를 해결하기 위해 통신하고 있는 두 노드 사이의 세션 키는 신뢰할 수 있는 베이스 스테이션(Trusted Base station)을 통해 두 노드에게 보내는 방법을 사용한다. 이 방법을 중앙 집중 키 분배 센터(KDC : Key distribution center)라고 부르기도 한다. 신뢰할 수 있는 베이스 스테이션은 요구하는 메모리의 크기가 작고, 노드의 응답을 완벽하게 제어한다. 그러나 베이스 스테이션이 공격자의 목표가 될 수 있다는 단점이 있다.

키 관리 기법 중 공개키 관리(Public key management)는 RSA(Ron Rivest, Al shamir, Len Adleman)와 ECC(Elliptic Curve Cryptography)라는 알고리즘을 이용하여 키를 관리한다. ECC는 타원 곡선을 이용하여 키를 암호화하는 방법으로 최근 WSN에서 많이 사용되고 있는 알고리즘이다. ECC를 이용한 키 관리는 서로 통신하는 이웃 노드들에 대해 하나의 공유키를 설립한다.

키 사전 분배 기법(Key pre-distribution schemes)은 센서 노드가 배치되기 전에 각 센서 노드에 몇 개 키를 미리 설치하는 방법이다. 노드가 배치되고 난 후 센서 노드는 안전한 통신을 위한 공유키를 설립하기 위해 서로의 노드를 발견하는 과정을 거친다. 이 방법은 어떤 두 센서 노드가 Pairwise key를 사용하여 통신을 하는 확률을 보장하지만 안전한 통신을 위해 사용하는 Pairwise key를 계산할 수 있다는 것은 보장하지는 않는다. 이 방법에는 랜덤 키 사전 분배(Random key pre-distribution schemes), q-합성수 랜덤 키 분배(q-Composite random key distribution), 다중 경로 키 강화(Multi-path key reinforcement) 방법, Random Pairwise 키 방법, Polynomial pool-based 키 분배, Random subset(RS)[168] 키 사전분배, Grid-based 키 사전분배 방법 등 다양한 방법들이 있다.

동적 키 관리(Dynamic key management)는 안전하고 효율적인 동적 키 관리 시스템(Dynamic key management system)을 생성하는 것을 주요 문제로

생각한다. 이 방법은 EBS(Exclusion based system)라고 불리기도 한다. EBS는 K+m개 키를 가지는 Key pool에서 각 노드에게 K개 키를 할당한다. 만약 노드가 캡쳐 당하면 전체 네트워크는 키를 갱신한다. 이 방법은 네트워크의 생존가능성(Survivability)을 향상시킨다는 장점이 있으나 적은 수의 네트워크일 경우 공격자에 의해 전체 네트워크가 노출될 수 있다는 단점도 있다.

그리고 RS(Random subset) 키 사전 분배와 관련되어 센서 네트워크의 키 관리 기법 중 Polynomial을 이용하는 키 관리 기법이 있다. Grid 기반과 Location 기반으로 나뉘며 D.Liu, P.Ning이 제안한 센서 노드 사이의 Pairwise key를 설정하는 프로토콜이다[168, 172]. 첫 번째로 Grid 기반 키 관리 기법은 일반적인 랜덤 키와 다른데, 이 기법은 일반 랜덤 키처럼 실제 키 값을 센서 노드에게 할당 하는 것이 아니라 Polynomial을 생성하여 노드에서 Polynomial을 분배하는 것이다. 이 Polynomial을 이용하여 노드가 키를 생성한다. 임의의 두 센서 노드가 동일한 t-degree Polynomial을 공유하여 두 노드는 그 Polynomial을 통해 공통키를 생성한다. 그리고 두 번째로 Location 기반에서는 Polynomial을 이용하는 것은 Grid 기반과 같지만 이 Polynomial을 이용하여 센서 필드를 셀 단위로 나누고 각 셀과 고유한 Polynomial을 연관시킨다. 그리고 특정 셀에 위치하고자 하는 센서가 있으면 그 위치에 해당하는 Polynomial과 그 특정 셀 주위에 가장 인접한 4개 셀에 해당하는 4개의 Polynomial을 할당한다. 그러면 이웃의 4개 셀에 배치된 센서와 Pairwise key를 생성하는 것이다.

센서 네트워크 보안 프로토콜(Sensor Network security protocol)이란 사용 가능한 자원이 제한적인 USN 환경에서 센서 노드들 사이에 안전한 통신 서비스를 제공하는 프로토콜을 말한다[59]. 센서 네트워크 보안 프로토콜의 연구 분야로는 센서 노드들 사이에 안전한 통신을 위한 키 관리 연구 분야가 있다. SPINS는 기존에 제안된 프로토콜로 신뢰 가능한 베이스 스테이션을 경유한 이웃 센서 노드와 키를 교환하는 방식을 사용하고 있다. 또한 LEAP는 이웃 노드의 노출을 최소화하기 위한 In-network processing을 하는 프로토콜이다.

센서 네트워크에서 사용되는 키 관리 기술은 목표에 따른 어플리케이션의 요구사항과 각 센서 네트워크의 자원(Resource)에 따라 다르게 사용된다.

제 3 절 USN 환경에서의 보안

1. USN 보안 개요

가. USN 보안 개요

USN(Ubiquitous Sensor Network)기술은 유비쿼터스 사회의 기반이 되는 주요한 기술로서 사회 구조에 전반적인 변화를 가져올 것으로 주목되고 있다. 최근 유비쿼터스 환경을 실현하는 기술로 사물 및 환경 정보를 센싱(Sensing)하여 무선 통신으로 정보 수집 및 처리하는 센서 네트워크 기술에 대한 관심이 높아지고 있기 때문이다. 센서 네트워크 기술은 상황정보 인지 능력을 다수의 센서 노드들이 무선 통신 네트워크를 구성하여 환경 정보 모니터링 및 홈, 자동화 등 다양한 분야에서 사용할 수 있는 기술이다.

USN 기술에 사용되는 센서 노드들은 도청에 취약한 무선 환경으로 연결이 되기 때문에 인증된 노드만이 통신에 참여하도록 해야 하며 노드 간에 전송되는 데이터의 내용이 외부에 노출되지 않도록 하는 등의 데이터 보안이 요구된다. 그러나 센서 노드들의 저전력(Low-power)과 낮은 연산력(Low-computing) 등의 제한된 능력으로 인해 보안에는 취약하다는 문제점이 여전히 존재하고 있다. 또한 무선 통신 환경의 특성 상 라디오주파수(RF : Radio Frequency) 잡음과 다중 경로 페이딩(Multi-path Fading)으로 인한 패킷 손실, 센서의 이동으로 인한 토폴로지의 잦은 변경 등과 같은 특성들 때문에 안전한 통신을 보장하는 것은 더욱 어려워지게 된다.

무선 네트워크로 구성된 센서 네트워크상에서 많은 센서 노드들을 통하여 전송되는 정보를 보호하기 위한 기법은 내부적으로 센서 노드의 보안 기능을 추가하는 것을 넘어 전체 네트워크를 보호하기 위한 보안 요구사항을 만족하여야 한다.

나. USN 보안의 필요성

센서 네트워크는 다양한 환경에서 환경 정보를 모니터링하고 필요한 정보를 센싱(Sensing)하여 처리하는 용도로 사용되기 때문에 정보의 신뢰성이 매우 중요하다. 그러나 다수의 센서 노드들이 센싱 된 정보를 베이스 스테이션(Base Station)으로 전송하는데 있어서 각 센서 노드들의 제한된 자원 능력은 네트워크상에서 센서 노드의 삽입과 탈퇴를 발생시켜 토폴로지가 자주 변하게 된다. 이것은 수집되는 정보의 신뢰성을 저하시키는 요인이 된다. 이러한 가운데 악의적인 노드가 센서 노드로 위장하여 네트워크에 참여하게 되면 잘못된 정보를 전송하거나 라우팅 정보에 혼란을 가져와 센서 네트워크의 보안에 악영향을 끼칠 수 있다. 특히 노드들이 배치되어 있는 환경이 공격에 그대로 노출되어, 전송되는 정보가 변조 또는 유출됨으로서 기밀성뿐만 아니라 무결성까지도 위협할 수 있다. 또한 이러한 공격의 효과는 단순히 센서 노드의 문제뿐만 아니라 USN 서비스를 이용하는 사용자 영역까지 미칠 수 있기 때문에 이를 방지하기 위해 보안을 강화해야 한다.

다. USN 보안 현황

센서 네트워크 보안 기술 개발 현황을 살펴보면 현재 국내 산업계의 기술 수준은 초기 단계에서 머물고 있다[66]. 아직까지 센서 네트워크 자체가 완전히 성숙하지 못한 단계에 있기 때문에 현재 단계에서 USN 환경에서의 공격의 형태나 공격자에 대한 정의를 명확히 내리기는 어렵다. 하지만 현재의 공격보다는 광범위한 대상을 목표로 점점 더 지능적인 공격 형태가 나올 것으로 예상이 되고 있다. USN 환경에서의 공격대상은 기존 환경의 컴퓨터에 저장된 정보 또는 통신 정보 뿐만 아니라 개인의 정보가 될 수도 있으며 공격 범위는 개인의 컴퓨터를 벗어나 개인의 사적인 공간으로 확대될 수도 있다. 따라서 공격에 대한 피해 범위는 공격 범위 확대 및 공격의 용이함에 따라 확대될 것으로 예상된다[8].

2. USN 보안 요구 사항

유비쿼터스 보안은 적법하지 않은 노드가 공유된 정보에 접근하거나 공유 정보를 노출 및 변경하지 못하도록 하는 것이다. 이를 위해 보안의 요구사항을 만족시켜야 한다. [표 1-1]은 유비쿼터스 네트워크 환경에서의 보안 요구사항을 나타낸 것이다.

[표 1-1] 유비쿼터스 네트워크 환경의 보안 요구사항[67]

보안 요구사항		추가 요구사항
기존 보안 요구 사항	인증	노드 간 상호인증 동적인 키 사용 무선 구간 키 교환 기법 제공 장치 독립적인 노드 인증 PKI 오버헤드 감소 집중형 인증/과금 기법 안전 전이 협약
	비밀성	키 관리 기반 이동형/서버 장치 내 데이터 암호화 서버 장치에 저장된 정보 암호화 저 전력 암호 알고리즘
	무결성	유비쿼터스 장치의 특성에 맞는 무결성 보장을 위한 암호학적 기법
추가적인 보안 요구사항	가용성	DoS 공격 서비스 액세스 우선순위 대가 지불 서비스
	권한 관리	개체 식별과 검증 노드 정보 접근 제어
	익명성	익명성에 대한 노드의 전달 권한
	안전한 로밍	동일한 서비스 네트워크 내의 안전한 핸드오프 글로벌 로밍 서비스 핸드오프 과정에서 보안 접속 유지와 보안 컨텍스트 정의 및 관리 분산 인증 및 실시간 패킷 과금에 대한 문제

센서 네트워크는 센서를 통해 주변의 정보를 수집하여 정보를 처리하는데 유용하게 쓰인다. 따라서 기존의 다른 네트워크와는 달리 센서 네트워크만의 독특한 특성에 맞는 위협요소나 공격 기법 그리고 이를 대응하기 위한 새로운 연구가 필요하다. 이에 대해 센서 네트워크에서의 보안 위협에 대응하기 위해서 현재 센서 네트워크 환경에서는 기밀성, 무결성, 가용성, 익명성, 인증성 등의 보안 서비스가 제공되고 있다.

가. 기밀성(Confidentiality)

기밀성은 수동적 공격으로부터 데이터를 보호하는 것으로 정당한 권한이 부여된 노드만이 데이터의 내용을 파악할 수 있도록 하는 것이다. 장치의 분실 및 도난, IP 스니핑, 장치간의 동기화에 의해 위협당할 수 있으며 이를 유지하기 위해서는 다음과 같은 기능이 요구된다[68].

- o 트래픽 데이터 암호화
- o 키 관리 기법 제공
- o 이동형 장치와 서버장치의 정보 암호화
- o 저전력 암호 알고리즘

USN에서는 이동하는 정보의 기밀 유지가 필요하다. 그렇기 때문에 근접한 다른 네트워크에 센서가 노출되지 않도록 해야 한다. 그리고 센서 노드들은 다양한 어플리케이션을 통해서 정보를 교환하므로 정보 또한 암호화하여 교환하는 기법을 이용한다. 따라서 기밀성을 유지하기 위한 가장 효율적인 기법은 암호화이다. 암호화 키는 데이터를 수신하는 노드만이 알 수 있도록 함으로써 기밀성을 유지한다. 그러므로 저전력과 낮은 연산력을 가지는 센서 노드의 특성에 맞는 경량 암호 알고리즘이 필요하다.

나. 무결성(Integrity)

무결성은 한 노드에서 보낸 데이터가 다른 노드에게 가는 도중 공격자에 의해 공격 받지 않도록 하는 것을 말한다. 센서 노드 간에 메시지를 주고받을 때 메시지의 내용이 변경되지 않은 메시지를 전달하는 것을 보장하는 것이다[68].

무결성은 장치의 분실 및 절도, 악의적인 소프트웨어 등에 의해 침해될 수도 있다. 메시지 무결성을 유지하기 위해서는 암호학적인 기법을 이용한다. USN 환경에 적합하도록 연산량이나 전력 소모량이 적으면서 메시지 무결성을 보장할 수 있는 암호학적 메커니즘의 연구가 필요하다.

또한 USN에서 송수신 되는 정보의 위조 또는 변조를 막을 수 있도록 데이터 무결성 보호를 위한 기술 역시 필요하다. 무선 통신에서 데이터의 무결성은 수신자가 수신한 데이터가 전송과정 도중에 위변조 되지 않았음을 보장하는데 이 때 데이터의 무결성은 인증을 통해 확인할 수 있다.

다. 가용성(Availability)

가용성은 서비스 거부 공격(DoS : Denial of Service), 악의적인 소프트웨어, 신호 방해 공격, 배터리 소진 공격, 멀티 홉 라우팅 프로토콜(Multi hop routing protocol)에 의존하며 노드들 중 하나가 협력을 거부하는 등의 행동에 의해 침해당할 수 있다. USN에서의 서비스는 가용성을 확보해야한다. 센서 네트워크는 불필요한 연산을 최대한 줄임으로써 전력 소모를 최소화하여 센서 네트워크의 수명을 연장해야 한다. 전체 네트워크의 가용성 유지를 위해 중앙에서 키를 관리 하는 노드를 배치하여 이 노드가 장애를 일으키지 않도록 관리하는 것이 중요하다. 따라서 센서 네트워크의 가용성을 침해하지 않는 수준의 보안 요구사항이 필요하다[70].

라. 익명성(Anonymity)

암호화는 메시지의 내용에 대한 기밀성 유지를 보장하지만 통신 사실 자체를 비밀로 유지할 수는 없다. 따라서 노드의 통신 사실 및 위치 등에 대한 프라이버시를 완전히 보호하지는 못한다. 익명성은 이러한 노드의 프라이버시 보호 측면에서 필요한 기능이다.[68].

익명성은 정보를 이용한 사물 및 개인에 대한 위치를 추적하거나 감시가 이루어지지 않도록 인증된 노드가 제어할 수 있다. 그러나 익명성이 보장될 경우 공격자의 위치를 추적하는데 어렵기 때문에, 노드의 위치를 알아야 하는 위급 상황 시 익명성으로 인해 노드의 위치 추적이 어려움을 겪을 수 있다. 이렇기 때문에 USN 환경에서는 노드의 익명성을 보장하면서 동시에 익명성을 선택적으로 제공받을 수 있는 방안이 함께 연구되어야 한다.

마. 인증성(Authentication)

USN에서 센서 노드의 통신은 상호 인증이 선행되어야 하는 것을 인증성이라고 한다. USN에서는 일시적이고 불확실한 연결을 제공하므로 인증을 위해 통신을 시도하는 과정에서 통신의 불확실성 때문에 적법하지 않은 노드를 적법한 노드로 인증할 가능성이 발생한다. 따라서 불확실한 통신 상태에서도 인증이 정상적으로 이루어질 수 있는 기법이 필요하다.

USN 환경에서 필요한 인증 기법의 예는 다음과 같다[68].

- o 노드 간 상호 인증
- o 무선 구간 키 교환 기법 제공
- o 장치 독립적인 노드 인증
- o 안전 협약

USN 환경에서는 전달되는 메시지가 원래의 정상적인 것임을 확인하기 위한 인증이 필요하다. USN 환경에서 공격자가 무선 환경의 취약성을 활용하여

메시지를 삽입할 수 있으므로 수신자는 데이터가 어디서부터 오는 것인지를 확인할 필요가 있다. 이 때 메시지의 인증은 목적지의 노드에게 수신한 데이터가 제대로 찾아왔는지를 확인하는 역할을 한다.

바. DoS 방지(Denial of Service Prevent)

USN에서 센서 노드들은 응용 서비스에 따라 열악한 환경에 배치될 수 있으며 공격을 받지 않아도 배터리 소실이나 홍수 등과 같은 물리적 공격에 의해 노드가 유실될 수 있다. 즉 센서 네트워크의 기반 구조가 취약하기 때문에 다양한 형태의 서비스 거부(DoS) 공격이 일어날 가능성이 높다. 열악한 환경에서 동작하는 센서 네트워크는 일부 노드에 문제가 생기더라도 다시 라우팅 경로를 재설정하는 결함 감내(Fault Tolerance) 기능을 지니고 있지만 공격자들에 지능적인 공격에 대해서는 제 기능을 발휘하지 못할 수도 있다. 이를 방지하기 위해 다양한 계층에서 이루어질 수 있는 서비스 거부 공격의 가능성을 고려해야 한다[71].

제 4 절 USN 환경에서의 공격 분류

USN 환경은 유비쿼터스 컴퓨팅 구현을 위한 센서 네트워크로, 기존에 이미 연구되어온 무선 인터넷, 무선 랜, 홈 네트워크 등의 센서를 사용하는 분야를 통합한 환경이라 할 수 있다. 이러한 USN의 특성으로 인해 데이터의 보안이 일반 컴퓨터 환경이나 일반 네트워크 환경보다 더 심각한 상황을 발생시킬 수 있다. 따라서 이러한 심각한 상황을 방어하기 위한 사전 작업으로 USN 환경에 가해질 수 있는 공격 형태를 다양한 관점에서 분류할 하였다.

본 절에서는 침해유형과 계층별 공격, 수동적/능동적 공격과 외부자/내부자 공격으로 공격 형태를 분류하였다.

1. 침해 유형에 따른 분류

침해 유형에 따른 분류는 센서 네트워크의 기본적인 보안 요구사항인 비밀성, 기밀성, 무결성, 인증, 가용성 중 침해하는 유형에 따라 공격 방식을 분류할 수 있다. 그리고 분류에 따라 각각의 보안 위협에 맞는 대응 기법을 이용하여 침해당한 보안 요구사항을 다시 확보해야 한다.

USN 환경에서는 무선통신을 기본으로 장치들 간에 통신을 하게 되는데 이때 발생할 수 있는 위협으로는 DoS, 바이러스 공격, 신호 방해 공격, 배터리 소진 공격 등이 있다. 이러한 위협들은 침해 유형에 따라 분류할 수 있으며 [표 1-2]는 침해 유형에 따른 공격 형태를 나타내고 각 위협에 따른 현황과 문제점 그리고 대책들 표로 정리한 것이다.

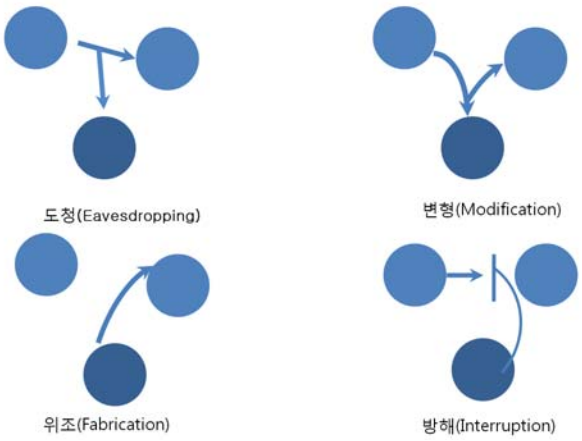
2. 수동적 공격과 능동적 공격에 따른 분류

USN에서의 공격은 공격자의 네트워크의 접근 권한에 따라 수동적인 공격과 능동적인 공격으로 분류할 수 있다. 네트워크에 직접적인 위협을 가하는 공격들이 능동적인 공격에 속하며 이와는 반대로 손쉽게 방어가 가능한 특징이 있는 공격을 수동적인 공격으로 분류한다. 수동적인 공격은 방어하기는 쉽지만 단지 무선 상의 패킷만을 도청하기 때문에 공격 여부를 판별하는 것이 어렵다. 수동적인 공격은 공격자가 공격하고자 하는 네트워크에 대한 접근 권한을 획득하지 않았을 경우에 사용하는 공격기법으로 수동적 공격을 통해 얻어낸 정보를 이용하여 네트워크의 접근 권한을 획득하여 능동적인 공격을 할 수 있다. (그림 1-3)은 수동적 공격을 크게 네 가지로 분류한 것을 나타낸다 [73].

수동적 공격에는 데이터를 도청하거나 가로챈 데이터를 위변조하는 기법과 다른 노드로 데이터 전송을 방해하는 공격 등이 있다.

능동적인 공격은 수동적인 공격과는 반대로 공격자가 공격하고자하는 네트워크에 대한 접근 권한을 획득한 후 이를 통해 네트워크의 일원인 것처럼 가장하여 네트워크를 공격하는 기법으로 수동적인 공격에 비해 종류가 다양하고

공격의 효과가 강력하다. 능동적인 공격에는 물리적으로 드러나 있는 노드를 획득하여 중요 정보를 획득하는 노드 획득과 필요 없는 데이터를 계속 전송함으로써 노드의 작동을 유도하여 전력을 소비시키는 자원 고갈공격이 있다. 그리고 라우팅 정보를 위변조하거나 재전송 공격(Replay Attack)으로 공격하는 라우팅 공격이 있다.



(그림 1-3) 수동적 공격유형

3. 외부자 공격과 내부자 공격에 따른 분류

외부자 공격은 네트워크에 참여할 권한이 없는 공격자의 공격으로 도청이나 데이터 위변조가 주요 목적이다. 그러나 외부자 공격이 그 자체로서 공격의 목표를 이룰 수 없다면 기본적으로 내부자 공격을 위한 정보를 획득하기도 한다.

내부자 공격은 어떤 방식으로든 네트워크에 참여할 수 있는 권한을 취득하여 네트워크 공격을 시도하는 것을 말한다. 내부자 공격에는 적법한 노드로부터 네트워크에 참여하기 위한 보안키, 인증 데이터를 획득하는 공격이 있다. 내부자 공격은 네트워크의 적법한 노드의 권한을 획득하기 때문에 보안 기법을 적용하더라도 원천적으로 공격을 봉쇄할 수는 없다. 따라서 공격자가 처음부터 네트워크에 참여하고 있다고 보기는 어렵기 때문에 공격 초기에는 외부

자 공격만 있다고 생각할 수 있다. 그리고 외부 공격자가 획득한 정보를 이용하여 내부 공격자인 것처럼 공격이 이루어 질수 있기 때문에 공격의 피해를 최소화할 수 있는 보안 기법의 연구가 필요하다[6].

[표 1-2] 유비쿼터스 환경에서의 보안위협 유형[72]

침해유형	보안 위협	현황 및 문제점	대책
가용성	DoS	가용성 침해	가용성 확보
	트로이목마, 웜 바이러스	가용성 침해	백신 프로그램 적용
	신호 방해 공격	통신 채널 혼선	확산대역 주파수 호핑
	배터리 소진 공격	짧은 시간 내에 배터리 소진	가용성 확보
비밀성	IP Spoofing	무선 신호가 원하지 않은 노드에게 전달	암호화
	트로이목마, 웜 바이러스	비밀성 침해	백신 프로그램 적용
	장치의 분실 및 도난	장치 소유자가 인증 정보 소유	암호화
	신원 정보 및 위치 정보 노출	프라이버시 침해	익명성 보장
무결성	트로이 목마, 웜 바이러스	무결성 침해	백신 프로그램 적용
인증	Rouge 액세스 포인트	단방향 인증환경에서 공격자의 액세스 포인트가 인증 없이 네트워크에 접근	양방향 인증 체계 구축 필요
	장치의 분실 및 도난	장치 소유자가 인증 정보 소유	장치 독립적인 노드 인증

제 2 장 USN 키 관리 기술과 관련된 키 분배 기법

본 장에서는 USN에서 사용할 수 있는 키 관리 기술을 살펴보고 각 키 관리 기술의 키 분배 방법을 자세히 다루며 장단점을 분석 하였다. USN의 키 분배 기법은 사전키 기반의 분배 기법, 공개키 기반의 분배기법, 센서 네트워크 보안 프로토콜로 크게 세 가지로 구분한다. 1절에서는 사전키 기반의 분배 기법을 설명하며, 이 기법은 마스터 키(Master key) 기반 키 분배 기법, Pairwise 키 기반 분배 기법, 확률론적 기반 키 분배 기법, 그룹 기반 키 분배 기법으로 구분 할 수 있다. Pairwise 키 분배 기법으로 All Pairwise, Random pairwise, Closest pairwise가 있으며, 확률론적 키 분배 기법으로 Blom의 대칭 행렬과 D.Liu, P.Ning의 Polynomial기반 분배 기법, EG 기법, q-합성수, Multi-path 기법이 있다. 그룹 기반 키 분배 기법으로 위치 기반 Pairwise 그룹과 클러스터 기반 그룹이 있다. 2절에서는 공개키 기반의 분배 기법으로, ECC와 ECDH, 3절에서는 센서 네트워크 보안 프로토콜로 LEAP와 SPINS가 있다. 이처럼 USN 환경에서 사용할 수 있는 다양한 키 관리 기법들을 본 장에서 자세히 설명한다.

제 1 절 사전키 기반의 분배 기법

1. 마스터 키 기반 키 분배 기법

가. Broadcast Session Key Negotiation (BROSK)

(1) BROSK 개요

Broadcast Session key Negotiation(BROSK)[5, 19]은 마스터 키 기반 사전 분배 방식으로, 각 센서 노드들이 하나의 마스터 키를 이용해서 Pairwise 키를

설정한다. 즉, 센서 네트워크의 공통 단일 세션 키가 갖는 보안 취약점을 개선하여 센서 네트워크에 있는 모든 센서 노드들에게 공통의 비밀키(Secret key, 마스터 키)를 부여한다. 그러면 각 센서 노드는 마스터 키로 암호화된 키 협상 메시지를 브로드 캐스팅하여 이웃 센서 노드와 세션 키를 형성한다.

(2) 분배 방법

네트워크에 존재하는 모든 센서 노드들에게 공통의 마스터 키가 할당되면, 모든 센서 노드들은 동일한 마스터 키 K_m를 공유하게 된다. 노드 S_i, S_j는 세션 키를 생성하기 위해 난수를 생성한 후 마스터 키로 암호화하여 키 협상 메시지를 브로드캐스팅 한다. 그러면 각 센서 노드들이 랜덤 수를 주고받으며 이웃 노드와 세션 키를 형성한다. 이때, 노드 사이에 설정된 세션 키는 $K_{i,j} = PRF(K_m || RN_i || RN_j)$이다.
(PRF()는 Pseudo Random Function)

(3) 장점

BROSK 방식은 각 노드들이 마스터 키만 저장하므로 요구되는 메모리양이 매우 적다. 또한 이 기법은 통신량이 매우 적고 각 센서 노드 쌍에게 유일한 세션 키를 형성 할 수 있다.

(4) 단점

BROSK 방식은 굉장히 낮은 저항성을 제공한다. 그 이유는 마스터 키가 모든 센서 노드들에게 공통으로 사용하므로 마스터 키가 노출되는 경우에 모든 링크의 키가 계산될 수 있다. 이것은 전체 네트워크의 세션 키가 노출되는 문제점을 지닌다.

나. Lightweight key management system

(1) 개요

Lightweight key management system[5]은 저항성을 향상시키기 위해 하나의 마스터 키를 사용하는 방식을 개선한 것이다. 센서 노드의 저전력 및 메모리 제한 등의 제한 조건을 만족시키기 위한 필수적인 기술이다.

(2) 분배 방법

센서 네트워크에서 각각의 노드들은 n개씩 그룹화 되어 연속적으로 있다고 가정한다.

키 셋업 단계에서 각 센서 노드에게 그룹 인증을 위한 키g(roup authentication key) bk_1과 키 생성 키(key generation key) bk_2를 저장하도록 한다.

만약 같은 시간에 만들어진 센서 노드 S_A와 S_B가 있다면, 그룹 인증키 bk_1을 사용해서 상대방을 확인한다. 확인 후에 각각 랜덤 수 RN_A와 RN_B를 교환하여 세션 키를 생성한다.

$$K_{A,B} = PRF(bk_1 || RN_A || RN_B)$$

만약 다른 시간에 만들어진 센서 노드라면, i 단계에 전개된 노드 S_A는 랜덤 수 RN_A와 비밀 정보 $S_{A,j}$를 저장한다. $S_{A,j}$는 새로운 j 단계에 전개된 노드를 인증하기 위해 사용하는 비밀 정보이다.

j 단계에서 노드 S_B는 노드 S_A로부터 랜덤 수 RN_A를 받아서, j 단계에 전개된 노드들만 아는 비밀 정보 gk_j와 함께 계산하여 인증을 수행한다.

$$S_{A,j} = PRF(gk_j || RN_A)$$

인증을 마치면, $S_{A,j}$는 두 노드 사이에 Pairwise 키를 생성하기 위해 키 생성 키로 사용한다.

(3) 장점

노드들의 전개 단계에서 단계가 m개인 경우 메모리는 최대한 4+2m을 필요로 한다. 따라서 Lightweight key management system에서는 메모리를 많이 사용하지 않으므로, 센서 노드의 제한 사항 중 하나인 메모리 문제를 해결 할 수 있다.

(4) 단점

만약 공격자에게 bk_1, bk_2, gk_i가 노출되면, j 단계에 전개된 모든 센서 노드들의 링크의 안전적인 면에 큰 영향을 끼치게 된다. 이것은 상당히 낮은 연결 지향성을 제공한다.

2. Pairwise 키 분배 기법

가. All pairwise scheme

(1) All pairwise scheme 개요

All Pairwise scheme[5]는 센서 노드가 센서 네트워크에 존재하는 다른 노드들과 각각 Pairwise 비밀키를 저장하는 방식이다.

(2) 분배 방법

네트워크의 크기를 N이라고 한다면, 센서 노드 $S_i\ (1 \le i \le N)$는 다른 센서 노드들과 통신을 위해서 자신을 제외한 $N-1$개 키가 필요하다. 따라서 네트워크 전체는 $N(N-1)/2$개의 서로 다른 키가 필요하다.

(3) 장점

All pairwise scheme 방식은 키 연결성이 매우 좋다. 한 노드에서 저장된 키들이 노출되더라도 다른 노드들 사이의 연결에 영향을 끼치지 않고 통신이 가능하다. 이것은 매우 좋은 저항성을 갖는 다는 것이다.

(4) 단점

All pairwise scheme 방식은 하나의 센서 노드가 저장하는 키의 개수가 많고, 네트워크 전체에서 필요로 하는 키의 개수 역시 많다는 단점을 지닌다.

나. Random pairwise key scheme

(1) Random pairwise key scheme 개요

Random pairwise key scheme는 Pairwise scheme의 단점을 보안하여 센서 노드 사이의 상호인증을 제공 하였고, 이 방법이 안전성도 높였다. 이 방식에서 각 센서 노드들은 두 노드들이 연결되어 있을 확률이 p가 되도록 랜덤하게 선택한 N_p 개의 Pairwise 키를 저장한다.

이 방식은 노드 사이의 상호 인증과 노드 캡처에 대해 완벽한 회복력을 가진다. 그리고 베이스 스테이션(Base station)이 없어도 노드가 손상 되었는지를 감지하고 취소 할 수 있는 기능이 있다[1, 5, 7, 16, 20].

(2) 분배 방법

Random pairwise key scheme는 배치 전의 초기화 과정인 사전 키 셋업(Key setup prior to deployment) 단계와 배치 후의 키 설정 과정인 공유키 탐색(Shared-key discovery after deployment) 단계로 나뉜다.

(가) 키 셋업 (key setup prior to deployment) 단계

센서 네트워크를 구성하는 센서 노드의 수를 n이라고 하면, 유일한 노드 ID를 n개 생성한다. 각 센서 노드들은 랜덤하게 선택된 m개의 노드 ID를 갖는다. 생성된 각각의 노드 쌍에 대해서 Pairwise key를 생성하고 각각의 노드 키링에 저장한다. 센서 네트워크의 크기가 N인 경우, 각 노드는 N_p개 키와 대응하는 다른 노드의 ID를 저장하므로, 키 체인을 저장하기 위해 2개의 기억장치를 필요로 한다.

(나) 공유키 탐색 (Shared-key discovery after deployment) 단계

각 센서 노드들이 자신의 ID를 브로드캐스팅(Broadcasting) 한다. 그러면 라디오 범위(Radio range) 안에 존재하는 인접한 이웃 노드들에게 브로드캐스팅된다. 이것을 통해 인접한 이웃 노드들은 자신의 키링과 비교하여 같은 ID를 찾는다. 만약 같은 ID를 가졌다면, 암호화된 응답(Cryptographic handshake)을 통해 공통의 Pairwise 키를 가지게 된다. 반면에 같은 ID를 가지지 못했다면, 센서 노드 사이의 링크를 생성하지 않는다. 또한 Random pairwise 키 사전 분배는 노드 취소를 제공하고 취소 공격과 노드 복제와 생성 공격에 대해서도 회복력을 가진다.

(3) 장점

Random pairwise key scheme에서는 베이스 스테이션(Base station)없이도 안전성을 가지며 노드 사이의 상호 인증을 제공한다. 또한 이 방식은 메모리 사용 양이 적고 저항성도 좋다.

Random pairwise key scheme으로 Path를 설정할 때 키 정보는 암호화 되어 전송 된다. 그래서 센서 노드의 수가 많더라도 기존의 Pairwise key와 동일하게 안정성을 제공한다[10].

(4) 단점

새로 들어오려는 노드의 키링에 인접한 노드와 Pairwise 키가 존재 하지 않으면, 이 노드와 경로 키 설정이 불가능 하므로 두 노드 사이에 링크 생성을 할 수 없다. 즉, 인접한 노드와 Pairwise 키가 없으면 새로운 노드가 들어 올 수도 없다. 이것은 키 연결성이 낮다는 것을 뜻한다.

따라서 Random pairwise key scheme는 위와 같은 키 연결성이 낮다는 단점을 해결 위하여 방법으로 전체 센서 네트워크의 연결성을 증가시키기 위해 범위를 확장하게 된다. 하지만 이것은 공격자에게 서비스 거부 공격(DoS) 기회를 증가 시키는 꼴이 된다. 더욱이 범위 확장은 오버 헤드도 같이 증가 시키게 된다[1].

다. Closest Pairwise Key pre-distribution scheme

(1) Closest Pairwise key pre-distribution scheme 개요

Closest(Location-based) pairwise key pre-distribution scheme은 Random Pairwise key scheme에서 키 연결성이 낮은 점을 개선하기 위해 제안된 방식이다.

이 방식은 각 센서 노드들이 전개될 위치를 예측 가능한 경우에 각 노드와 가장 가까운 n개의 이웃 노드들 사이에 Pairwise 키를 공유하도록 한다[4, 5].

(2) 분배 방법

키 셋업 단계에서 노드 S_A는 자신의 Unique key와 가장 가까운 n 개의 이웃 노드 S_{B_1}, S_{B_2}, … , S_{B_n}를 선택한다.

센서 노드 S_A와 S_B의 Pairwise 키는 Pseudo random function으로 생성한다.

$$K_{A,B} = PRF(K_{B_1} || ID_A)$$

(3) 장점

노드 S_A는 모든 Pairwise 키들을 저장하고, S_{Bi}는 K_{Bi}와 PRF를 저장한다. 따라서 한 센서 노드가 키 체인을 저장하기 위해 2n+1개의 메모리 유닛을 필요로 한다. 그렇기 때문에 노드들이 전개되는 위치가 예측 가능하다면 키 연결성은 높아지면서 메모리의 양을 감소시킬 수 있다.

(4) 단점

이 방식은 Pairwise 키 검색과 PRF 함수 계산을 위해 CPU를 사용해야 한다.

3. 확률론적 분배 기법

가. Blom's 기법

(1) Blom's 기법 개요

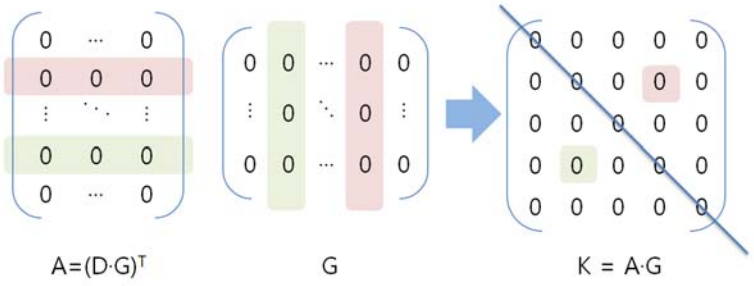
Blom에 의하여 제안된 키 사전 분배 방법으로 키 분배 센터에서 두 노드에게 임의의 함수 값을 전송하면 두 노드는 전송 받은 정보로부터 두 노드 사이의 통신에 필요한 세션 키를 생성한다. 즉 센서 노드는 신뢰할 수 있는 키 분배 센터로부터 전송 받은 정보를 이용하여 센서 노드들 사이에 안전한 통신을 하기 위해 필요한 세션 키를 계산할 수 있다 [12, 21, 24].

Blom's 기법을 이용하여 대칭키를 생성하는 방법으로 Blom의 대칭행렬[22]과 Blom의 기법을 응용하여 센서 네트워크에 맞게 수정하고 다중 키를 사용하여 노드 캡쳐에 대한 네트워크 회복력을 향상 시킨 D. Liu, P. Ning이 제안한 Polynomial[21]을 사용하는 기법이 있다.

(2) 분배 방법

가) Blom 스킴 - 행렬

Blom은 네트워크상의 어떤 노드 사이에도 Pairwise 비밀 키를 찾을 수 있도록 키 사전분배 방법을 제안하였다[22]. 이 기법은 랜덤한 대칭 행렬을 이용하여 행렬 계산을 통해 두 노드 사이에 Pairwise 키를 찾고자 하는 것이다[7].



(그림 2-1) Blom 스킴의 행렬

o T는 $k \times n$ 크기를 갖는 행렬 G를 생성하여 공개한다.

o $k \times k$의 대칭 행렬 D를 생성한다. 이 때 D는 비밀행렬로 공개하지 않는다.

o T는 각 사용자 i에게 $(DG)^T$의 i번째 행만 나눠준다.

대칭키는 행렬 $K = (DG)^T G$의 각 항이다. 즉 i번째 사용자와 j번째 사용자는 행렬 K의 값 $K[i][j]$을 대칭키로 사용한다. (K는 대칭행렬이므로 $K[j][i]$의 값과 $K[i][j]$는 동일한 값을 가진다.)

만약 각 사용자 i가 j와 공유할 대칭키를 계산하고 싶으면 G의 j열과 내적을 구하여 $K[i][j]$을 계산한다.

$$K = (DG)^T G = G^T D^T G = G^T D G = K^T$$

나) D. Liu, P. Ning의 Polynomial

Polynomial 기법은 Blom의 키 사전 분배 기법과 비슷하지만 Blom 기법이 벡터를 사용하는 것에 비해 Polynomial은 t-degree bivariate Polynomial(degree가 t인 이변 다항식)을 사용한다. 즉, 키를 설정하는 서버가 임의로 대칭변수 t차(t-degree) Polynomial을 생성한다. 생성된 Polynomial을 센서 노드에게 할당하여 통신을 하는 두 노드 사이에 공통된 키 값을 유도한다. 한마디로, 이 Polynomial은 f(x, y) = f(y, x)를 만족해야 하며, 통신을 하고자 하는 두 센서 노드에게 이 대칭 Polynomial이 공유 및 분배된다.

대칭키를 얻기 위해 Polynomial을 이용하는 과정은 다음과 같다[21].

여기서 TA란 Trusted authority로써 관련된 사용자들과 키 값이 신뢰할 수 있는 키 관리 기관을 말한다.

- o 1단계 : 소수 p와 각각의 사용자 A의 공개키인 $r_A \in Z_p$ 를 공개한다. (r_A는 사용자 A에 따라 모두 다르다.)
- o 2단계 : TA는 적당한 계수 a, b, c $\in Z_p$ 를 가진 Polynomial을 선택.

$$f(x, y) = a + b(x + y) + cxy (\mathrm{mod}\ p)$$

- o 3단계 : TA는 Polynomial $a_A(x)$를 다음과 같이 계산하여 안전한 채널로 사용자 A에게 전송한다.

$$a_A(x) = f(x, r_A) \bmod p$$

여기서 α_A는 x에 관한 선형 Polynomial $(x)=\alpha_A+b_A{}^x$ 로 표현할 수 있다.

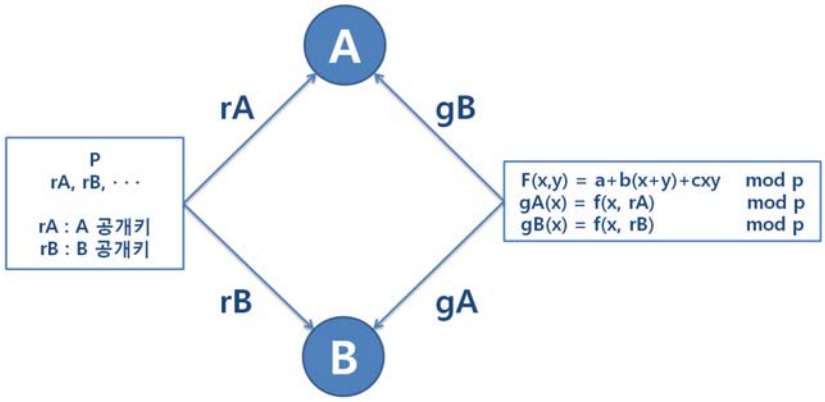
$$a_A = a + br_A (\mathrm{mod}\ p),\ \ b_A = a + cr_A (\mathrm{mod}\ p)$$

- o 4단계 : A와 B가 서로 정보를 교환하기를 원할 때는 공통키를 사용한다. A와 B는 각각 공개되어 있는 r_A, r_B를 각자의 Polynomial에 x대신 다음 (식1)을 대입한다. 그 후 다음 (식2)와 같이 계산하여 A, B 사이의 공통 대칭키를 얻는다.

$$f(r_B, r_A) = \alpha_A(r_B), \quad f(r_A, r_B) = \alpha_B(r_A) \qquad \text{(식1)}$$

$$K_{AB} = K_{BA} = a + b(r_A + r_B) + cr_A r_B (\mathrm{mod}\, p) \quad \text{(식2)}$$

(그림 2-1)은 위의 과정을 그림으로 표현한 것이다. 즉,TA에서 공개키(Public key)를 사용자 A에게는 rA를, 사용자 B에게는 rB를 준다. 그 후 사용자 A와 B가 통신을 하기 위한 공통키를 생성하는데 위의 수식을 이용하여 사용자 A는 gB 키를, 사용자 B는 gA 키를 얻는다.



(그림 2-2) Blom 키 분배

Polynomial 기법을 예시를 통해 설명하고자 한다. 키를 분배해야 할 세 명의 사용자 A, B, C가 있다고 하자. 이 때, p=17이고, 공개키 rA=12, rB=7, rC=1이며, TA가 a=8, b=7, c=2를 선택하면,

Polynomial f(x, y) = 8 + 7(x+y) + 2xy(mod 17)

이 된다. 그리고

gA(x) = 7 + 14x, gB(x) = 6 + 4x, gC(x) = 15 + 9x

가 된다. 따라서 사용자 A, B, C 세 사람 사이의 공통키는 각각

k_{AB}=3, k_{AC}=4, k_{BC}=10

이 되는 것이다[171].

(3) 장점

Blom 방식의 좋은 점은 열과 행 벡터가 선택되기 때문에 두 노드안의 두 벡터의 중식이 같아져서 결국 공유키가 된다는 것이다. 또한 각 노드들은 적은 양의 정보만을 저장하고 각 노드 간에 필요한 링크키를 계산할 수 있다. 그래서 Blom의 키 사전 분배방법은 두 노드간의 대칭키를 만들어 내는데 편리하고 효과적이라고 할 수 있다. 또한 공격자에 의한 노드 캡쳐에 대해서도 이전의 방법보다 더 나은 저항력을 가진다. Blom 기법은 λ-security 특성을 갖는데 Polynomial에서는 λ 노드보다 많은 수의 노드가 캡쳐 되지 않는 이상 Polynomial의 계수를 모두 계산할 수 없고, 대칭 행렬에서는 노출되는 열의 수가 λ 이하이면 행렬 D를 기반으로 생성된 다른 키들의 안전이 보장되는 것을 의미한다.

(4) 단점

Blom을 이용하여 대칭키를 만들어서 그 결과를 각자에게 안전한 채널로 제공할 수 있지만 일정 수 이상의 노드가 캡쳐당하면 다른 노드의 키를 알아낼 수 있는 단점이 있다. 또한 두 노드 간의 대칭키를 계산하기 위해 적지 않은 연산을 요구하여 메모리와 배터리 사용에 대한 소모가 크다.

나. Eschenauer-Gligor (EG) 기법

(1) EG 개요

Eschenauer-Gligor(EG) 기법은 2002년 Laurent Eschenauer와 Virgil D. Gligor에 의해 "A Key-management scheme for distribute sensor networks"에서 제안 되었다[16].

이 기법은 랜덤 키 사전 분배(Random key predistribution) 기법으로, 센서

네트워크에서 공개키 암호화 방식을 적용하여 발생하는 문제점과 단일키 암호화 방식을 사용하여 발생하는 문제점을 해결하기 위해 연구되었다[20, 24].

Eschenauer-Gligor기법은 무선 센서 네트워크(WSN)의 초기 키 선분배 기법이며 최초의 개체 간 키 설정(Pairwise key Establishment) 기법이다[4, 7, 23].

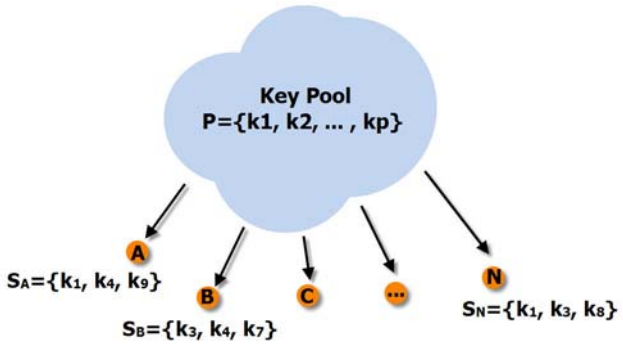
Eschenauer-Gligor 기법은 3단계로 구성된다.

o 1단계 : 키 분배(Key predistribution)
o 2단계 : 공유키 찾기(Shard key discovery)
o 3단계 : 패스키 확립(Path-key establishment)

(2) 분배 방법

1단계 키 분배(Key predistribution) 단계에서 센서 네트워크 전체에서 사용할 대규모 키들의 공간 Key Pool P를 생성한다. 각각의 센서 노드는 Key Pool P에서 랜덤하게 k개 키를 선택하여 메모리에 저장한다.

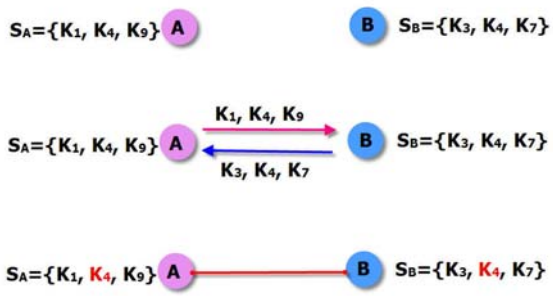
여기서 키 k들의 집합을 그 센서 노드의 키 링(S_k)이라고 한다. Key Pool P에 있는 모든 키들은 유일한 ID를 가지고 있으며, 키와 함께 키에 대한 ID도 센서 노드의 키링에 저장된다.



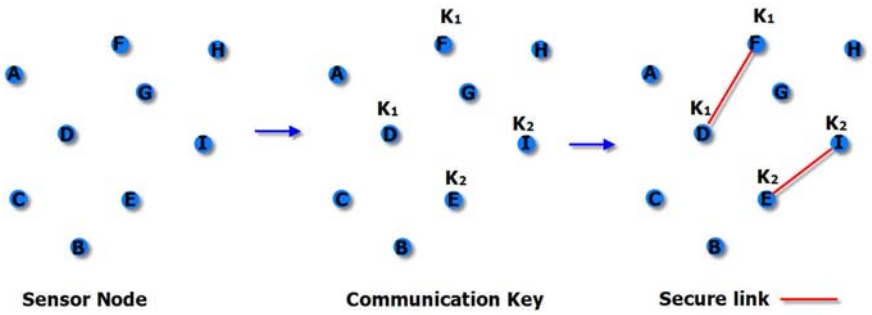
(그림 2-3) Key Pool로부터 랜덤하게 Key 할당

이렇게 센서 노드들에게 키를 배치한 후에 2단계 공유키 찾기(Shard Key discovery) 단계가 수행된다. 이 단계에서는 이웃 센서 노드와 공통된 키를 찾는다. 각각의 센서 노드는 자신의 키링에 있는 키의 ID를 브로드캐스트 한다. 그러면 이웃 노드는 브로드캐스트 된 ID와 자신의 키링에 있는 키의 ID를 비교한다.

만약 같은 키를 가지고 있으면 공통키가 존재하는 것이므로, 두 노드는 안전한 링크(link)로 연결되고 상호 인증 및 공통의 키로 암호화 통신을 할 수 있다.



(그림 2-4) 공유키 찾기



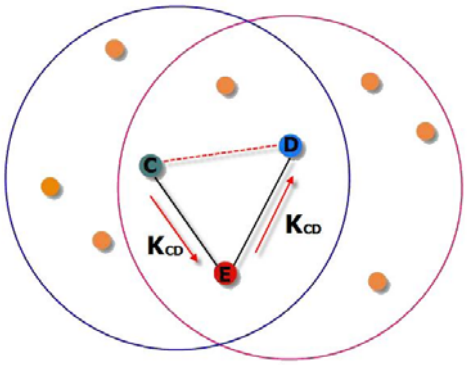
(그림 2-5) 링크 연결

여기서 두 센서 노드 간에 키를 공유할 확률 p_c가 주어진다. 이 p_c는 확률적 연결성 값(Probabilistic connectivity value)으로, 센서 노드 S_A(센서 노드 A의 키 링)와 S_B(센서 노드 B의 키 링)가 키를 만들 때 공유키 $k \in S_A \cap S_B$를

사용한다.

만약 같은 키를 가지고 있지 않으면 안전한 링크(link)를 생성할 수 없으므로, 3단계 패스키 확립(Path-key establishment)을 통해서 패스를 확립한 후 두 노드간의 상호 인증 및 통신이 가능하도록 한다. 즉 패스키 확립 방법은 두 노드가 공통된 키가 없을 때 다른 노드를 통하여 공통된 키를 찾는 것이다.

패스키 확립 과정은 다음과 같다. 통신 범위 안에 있는 공통키를 찾지 못한 두 센서 노드 C와 D가 있다. 이들은 공통 통신 범위 내에서 두 센서 노드 모두와 공통키를 찾는 제 3의 센서 노드 E를 찾는다. 그러면 두 센서 노드 중 하나 C가 자신의 키링(key ring)에 있는 키를 노드 E에게 전달하면 노드 E는 그 키를 노드 D에게 전달한다. 그래서 두 센서 노드 C와 D는 공통된 키를 가지게 되어 안전한 링크를 생성 할 수 있다.



(그림 2-6) 패스 키 확립 과정

(3) 장점

센서 노드는 메모리가 적고 에너지 효율성이 좋지 않기 때문에 연산량이 많은 공개키 암호 방식을 사용하기에 제약이 따른다. 이를 보안하기 위해 센서 네트워크에서 대칭키 방식을 이용하였다. 기존의 대칭키 방식에서는 센서 네트워크를 구성하고 있는 모든 센서 노드가 단일키를 사용한다. 단일키 사용은 하나의 노드에서 단일키가 노출될 경우 전체 센서 네트워크의 정보가 노출되

는 문제점을 가진다. 하지만 랜덤 키 사전 분배 기법을 사용함으로써 외부 노드나 네트워크 전체의 키 체인과 노드 정보가 노출되는 것을 방지 할 수 있다. 대규모 네트워크에서 키 설정 확률이 충분히 크다면 각 노드들은 더욱 많은 노드와 공통키를 공유 할 수 있다. 이러한 방법은 신뢰하는 베이스 스테이션(base station)을 지정할 필요 없이 키 설정을 할 수 있다.

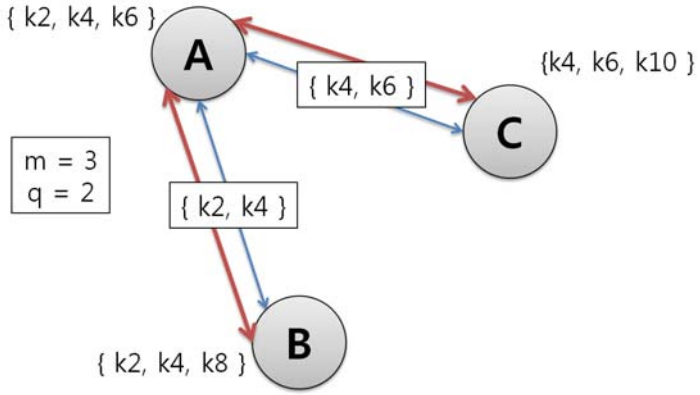
(4) 단점

Eschenauer-Gligor(EG) 기법에서 센서 노드는 자신이 가진 자원에 비해서 많은 키를 저장해야 한다. 또한 Key pool P에서 랜덤하게 임의의 개수의 키를 선택할 때 두 노드가 공통키로 사용하려는 키를 다른 노드가 가지고 있을 수 있다. 이럴 경우 공격자가 이 키를 가진 노드를 캡처하여 정보를 얻을 수 있다. 또한 센서 노드 공격자가 많은 센서 노드들을 포획해서 그 센서 노드의 키링을 획득하면 전체 키 Key Pool P를 예측 하여 Key Pool을 완전히 재구성할 가능성이 있다.

다. q-합성수(q-composite) 랜덤 키

(1) q-합성수 랜덤 키 개요

랜덤 키 분배 기법에는 랜덤-키 사전 분배와 랜덤 Pairwise 키 사전 분배가 있다. 랜덤 Pairwise 키 사전 분배는 랜덤-키 사전 분배기법의 안전성을 강화시킨 기법으로 q-합성수 랜덤 키 사전 분배 방법이 있다. q-합성수 랜덤 키 사전분배 기법은 공통키를 q개 사용한다는 점을 제외하면 랜덤 키 사전 분배 기법과 동일하다. 해쉬 함수나 XOR 방식을 이용한 새로운 키 생성 방식으로 노드간의 통신을 위한 기본 키 분배 방식보다 노드가 공격을 당했을 때의 보안성을 강화했다[1, 2, 7, 12, 20, 22].



(그림 2-7) q-합성수 랜덤 키

(2) 분배 방법

q-합성수 랜덤 키 사전 분배 방법은 키 공간에서 s개 키가 임의로 선택되어 키 풀을 이루고 각각의 노드는 키 풀에서 m개 키를 선택하여 키링을 이룬다. 그런 다음 다른 노드와의 통신을 위하여 필요한 키를 설정하기 위하여 이웃 노드와는 적어도 q개 이상의 키를 공유 한다는 가정 하에 hash함수를 이용하여 새로운 세션 키를 형성한다.

$$K = \text{hash}(k1 \| k2 \| \ldots \| kq)$$

(3) 장점

q-합성수 랜덤 키 사전 분배기법은 센서 네트워크에서 키를 설정하는 데 있어서 보안성을 강화할 수 있다. 공격자는 두 노드 사이에 사용된 공통키 q개를 알아야만 도청을 할 수 있다. 그렇기 때문에 적은 수의 노드가 공격을 당하더라도 전체 네트워크에 미치는 영향은 작다.

(4) 단점

q-합성수 랜덤 사전키 분배방법에서 두 노드 사이의 링크를 생성하기 위해서는 q개 이상의 키가 있을 때만 가능하다. 따라서 공통키를 가지고 있을 확률을 높이기 위해서는 키 풀의 크기를 줄이거나 노드마다 가지고 있어야 하는 키의 개수를 늘려야 한다. 그러므로 하나의 노드가 저장하고 있어야 하는 정보의 양이 늘어나게 되고 많은 수의 노드가 공격자에게 노출이 된다면 기존의 사전 분배 방식보다 더 많은 정보가 노출될 수 있다. 또한 만약에 두 노드 사이에 q개 키가 모두 저장되어 있는 노드가 공격자에 의해 캡쳐 당한다면 노드 간 통신의 안전성이 보장받지 못하는 문제점이 발생할 수가 있다.

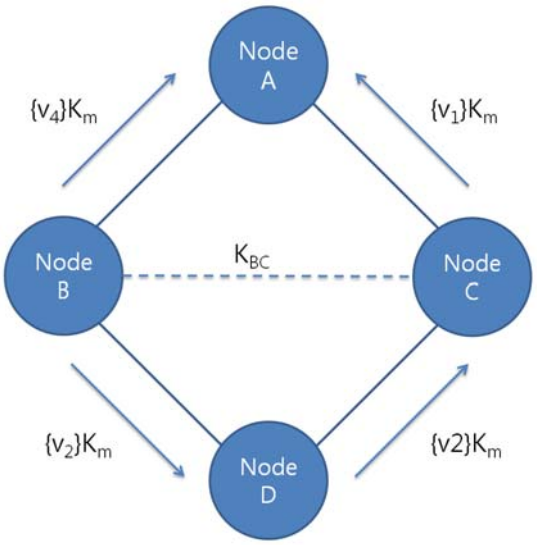
라. Multi-Path

(1) Multi-Path 개요

다중 경로 키 기법 또한 q-합성수 랜덤 사전키 분배 기법과 마찬가지로 랜덤 키 사전 분배 프로토콜의 결점을 보안하기 위해 제안되었다. 노드는 세션 키를 설정한 후 독립적인 경로를 통하여 세션 키를 강화한다[1, 7, 20].

(2) 분배 방법

다중 경로 키 강화 기법은 두 노드 사이의 보안성을 강화하기 위하여 두 노드 사이의 다양한 경로를 통해 새로운 경로키를 설정한다. (그림2-8)에서 노드 B와 C는 세션 키 K_{BC}를 강화하기 위하여 독립적인 두 경로, 노드 A를 통한 경로와 노드 D를 통한 경로를 이용한다. 노드 B는 키와 같은 길이를 갖는 v1과 v2를 임의로 선택한다. 그런 다음 두 경로를 통해 노드 C에게 보낸다. 노드 C는 두 임의의 값을 받으면 새로운 세션 키 k' 가 생성이 된다.



(그림 2-8) 다중경로 키 강화

즉 노드 A와 B사이에 p개의 경로가 존재한다면 A는 B에게 p개의 값을 생성하여 다양한 경로를 통하여 전달을 한다. 이를 전달받은 B는 이 값들과 기존의 A와 B 사이의 키를 이용하여 새로운 키 k′을 형성한다. 세션 키를 형성하는 방법은 다음 식과 같다. (j: 독립적인 경로의 수)

$$k' = k \oplus v_1 \oplus v_2 \oplus \cdots \oplus v_j$$

(3) 장점

기존의 랜덤 키 사전 분배 기법보다 안전성을 강화함으로써 한 노드가 공격을 당할 때 전체 네트워크에 영향을 끼칠 수 있는 손실을 줄인다. 즉, 많은 경로를 통하여 데이터를 분산시킴으로 인해 한 노드에 데이터가 몰리는 혼잡이나 병목 현상을 줄일 수 있다. 또한 다중 경로를 사용하기 때문에 하나의 경로에 문제가 발생하여 전송에 실패하더라고 다른 경로를 통해 무사히 정보를 전달할 수 있다. 따라서 센서 네트워크에서 서비스를 제공할 때도 지연 없이 정보 전달이 가능하다.

(4) 단점

다중 경로 기법은 랜덤 키 사전 분배기법의 안전성 문제를 해결하였다. 하지만 인접한 노드와의 Pairwise키가 키링에 존재 하지 않는다면 두 노드 간의 링크를 생성할 수 없다. 뿐만 아니라 새로 추가되는 노드와 인접한 노드 사이에 Pairwise 키가 없는 경우에 새로운 노드를 추가할 수 없다. 또한 경로에 있는 중간 노드들에 대한 신뢰성이 있어야 한다. 만약 경로에 있는 어떤 한 노드가 공격자에 의해 손상된다면 노드들 간의 통신이 안전하지 않을 수도 있다. 그리고 세션 키를 강화하기 위한 독립적인 경로를 찾는 과정에서 오버헤드가 발생할 가능성이 있다.

4. 그룹 기반 분배 기법

가. 위치 기반 Pairwise 그룹

(1) 위치 기반 Pairwise 그룹 개요

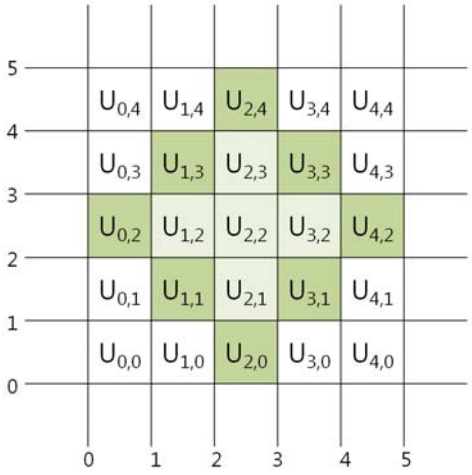
D.Liu, P.Ning이 제안한 방법으로 Pairwise 키 설정 프로토콜이다. Grid 기반처럼 Polynomial을 이용하여 센서 필드를 셀 단위로 나누고 그 셀과 고유한 Polynomial을 연관키는 방식을 이용한다. 특정 셀에 위치하고자 하는 센서는 그 위치에 해당하는 Polynomial과 그 셀과 인접하는 4개의 셀에 각각 4개의 Polynomial이 할당된다. 그런 다음 이웃한 4개의 셀에 배치된 센서와 Pairwise key를 생성한다[5, 7].

(2) 분배 방법

위치 기반 키 분배 방식은 그리드 기반 키 분배 구조에서 사용하였던 방식처럼 f(x,y)=f(y,x)을 만족하는 Polynomial을 분배하는 방식을 이용한다. 그리드 기반 키 분배 구조와는 달리 센서 필드를 직사각형 구조로 나누고 각 셀의 좌

표를 (i,j)로 표시한다. 그리고 그 셀과 고유한 Polynomial을 연관시킨다. 즉 특정 노드 U_{ij}에 Polynomial $f_{ij}(x, y)$를 할당한다. 특정 셀에 위치하는 센서가 그 위치에 해당하는 Polynomial과 인접한 4개의 셀에 해당하는 4개의 Polynomial을 할당 받아 이웃 셀에 배치된 센서와 Pairwise 키를 설정하는 방식이다.

예를 들어 (그림 2-9)와 같은 센서 필드에서 셋업 서버는 좌표 (1, 2)에 있는 센서 $u_{2,3}$에게 노드 u가 위치한 셀과 인접한 4개의 셀에 해당하는 Polynomial share $f_{2,2}(u_{2,2},y), f_{2,1}(u_{2,2},y), f_{1,2}(u_{2,2},y), f_{2,3}(u_{2,2},y), f_{3,2}(u_{2,2},y)$를 배분한다. 센서 배치 후 특정한 두 센서가 Pairwise key를 설정하려고 하면, 우선 공통의 Polynomial이 있는지 확인한다. 만약 공통의 Polynomial이 있으면 Polynomial based key distribution방법으로 키를 설정한다.



(그림 2-9) 위치 기반 키 분배 구조

(3) 장점

노드들은 센서의 위치 정보를 이용하여 직접적으로 인접한 노드들과 Pairwise key를 얻을 수 있다. 그렇기 때문에 Pairwise key predistribution의 퍼포먼스를 향상시킬 수 있다.

또는 센서 노드들의 위치를 정확히 알 수 있다면 공통키를 설정할 노드들을 예측하여 키 분배를 쉽게 해결 할 수 있다는 장점이 있다. 위치기반 Pairwise 그룹 기법에서 센서 노드는 메시지를 통하여 전송 범위 내에 위치한 노드들의 그룹 식별자를 알아낸다. 대부분의 통신이 전송 범위 내에서 이루어지기 때문에 이웃 노드들의 배치 정보는 키 분배 시 유용하게 사용될 수 있다.

센서 배치 방법을 고려하여 배치된 센서 노드의 위치에 따라 필요한 키를 집중적으로 분배하여 공통 키 설정 확률을 높이고, 메모리 소모량을 줄일 수 있다.

(4) 단점

위치 기반 사전 키 분배 방식은 셀을 추가하면서 각각의 셀에 위치한 노드들이 노출된 센서의 ID들을 기억하고 있으므로 Polynomial이 노출 될 수 있는 위험이 있다. 또한 센서 노드들의 배치가 임의적으로 이루어지기 때문에 키 설정 확률을 높이는데 제한적이다.

나. 클러스터 기반 그룹

(1) 개요

센서 노드들끼리 그룹을 형성하고, 그룹 안에서 보안을 위해 그룹 키를 사용하는 기법을 그룹 키 관리 기법이라고 한다.

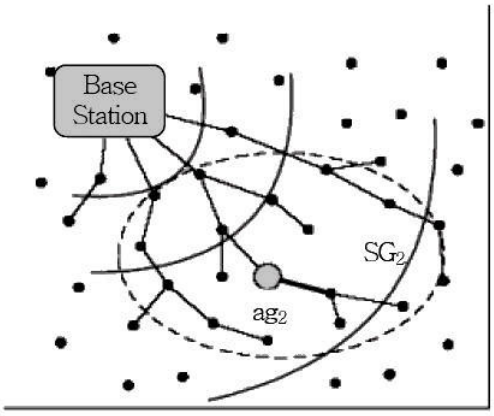
그룹 키의 기본 구조는 베이스 스테이션(base station)과 클러스터(cluster) 구조를 중심으로 베이스 스테이션과 클러스터마다 중간에 aggregator를 두는 형태이다.

기본 방법은 우선 각 클러스터가 하나의 그룹을 형성한다. 그 다음에 각 그룹에서 보안 유지를 위해 필요한 그룹 키를 베이스 스테이션의 aggregator에게 전달하고, aggregator가 다시 그룹 내 센서 노드들에게 전달한다[4, 5, 10, 17].

(2) 분배 방법

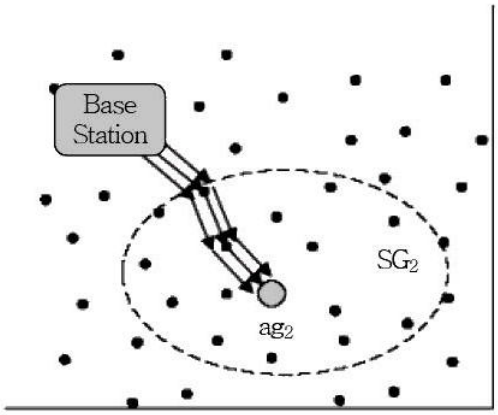
아래의 그림은 그룹 키 기반 보안 기법을 각 단계마다 표현한 것이다. 여기서 베이스 스테이션이 각 센서 노드들에게 그룹 키를 분배 할 때, 모든 센서 노드는 미리 베이스 스테이션과 비밀 키를 공유한다고 가정한다.

(그림 2-10)은 그룹 선언(group announcement) 단계이다. 이 단계에서는 미리 그룹을 나누고 aggregator를 정한다. 그리고 베이스 스테이션이 모든 센서 그룹의 정보와 각 그룹의 aggregator의 정보를 모든 센서 노드들에게 브로드캐스트 한다.



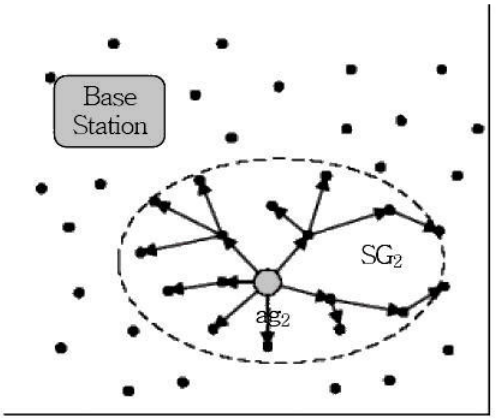
(그림 2-10) 그룹 선언

두 번째 단계인 (그림 2-11)은 베이스 스테이션이 해당 센서 그룹에 포함되는 모든 센서 노드와 각 그룹에게 사용할 그룹 키를 각 그룹의 aggregator에게 유니캐스트(Unicast)로 전달하는 단계이다. 이때 전송되는 키는 베이스 스테이션과 해당 aggregator 사이의 비밀 키로 암호화된다. 그리고 베이스 스테이션과 해당 aggregator 사이의 공유키로 생성한 MAC 값을 같이 보낸다.



(그림 2-11) 베이스 스테이션이 aggregator에게 키 전달

(그림 2-12) 단계는 각 그룹의 aggregator가 자신이 속한 그룹 안의 모든 센서 노드들에게 정보를 유니캐스트로 전달하는 단계이다. 이때 전달되는 정보는 그룹의 그룹 분별 아이디와 그룹 키, 그리고 MAC 값이다.

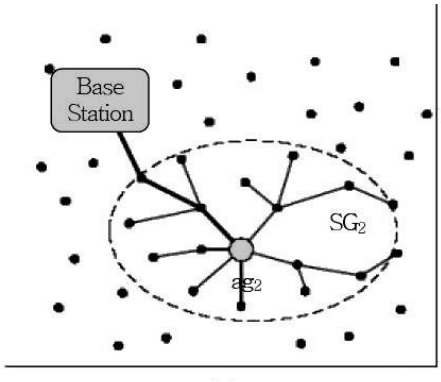


(그림 2-12) aggregator가 그룹 내에 정보 전달

마지막 단계로 (그림 2-13)는 그룹 내의 각 센서 노드들이 자신이 속한 그룹을 인식하게 되고, 그룹 키를 안전하게 수신하는 단계이다. (그림 2-13) 단계에서 각 그룹의 aggregator로부터 정보를 받으면 각 센서 노드는 자신이 어느

그룹에 속하는지 알게 된다.

그리고 자신이 사용할 그룹 키를 계산 할 수 있고 이 키를 이용하여 생성한 MAC 값을 확인한다. MAC 값을 확인함으로써 메시지가 변조 되지 않았는지 확인할 수 있다. 즉, aggregator로부터 정당하게 온 메시지인지 확인 가능하다.



(그림 2-13) 그룹 키 인식 및 수신

이처럼 각 aggregator를 통해서 베이스 스테이션으로부터 효율적인 키 분배가 되는 것이다.

(3) 장점

그룹 키 관리 기법에서는 공유 키 탐색을 위해 센서 노드들이 주고받는 메시지의 양이 감소한다. 그리고 각 그룹 키는 자신만의 그룹 영역을 담당함으로 해당 그룹의 센서 노드가 이동하더라도 그 영향이 그룹 내로 한정된다.

(4) 단점

그룹 키 관리 기법은 임의의 센서 노드에 관한 개별 인증을 할 수 없고 단지 그룹에 대해서 멤버 여부의 인증만 가능하다. 그리고 그룹 키를 안전하게 전송하기 위해서 미리 비밀 키를 가지고 있어야 한다. 만약 미리 비밀 키를

가지고 있지 않으면 센서 노드가 네트워크에 들어 왔을 때 안전하게 그룹 키를 받을 수 없다. 또한 그룹 키가 알려지면 전체적으로 시스템 보안에 큰 영향을 끼치게 된다.

5. 키의 사전 분배 종류 및 특징 비교

아래의 [표 2-1]은 키의 사전 분배 방식의 장점과 단점을 표로 정리하여 비교한 것이고, [표 2-2]는 키의 개수 및 메모리 크기를 표로 간략히 정리하여 비교한 것이다[1]. 여기에서 비교한 키의 종류로는 마스터 키, Pairwise 키, 랜덤 키, q-합성수 랜덤 키, Multi-Path 키, 랜덤 Pairwise 키가 있다.

마스터 키는 모드 노드가 하나의 키만 저장하므로 키 하나만 메모리에 저장하면 된다. 하지만 이 키 하나가 깨지면 네트워크 전체가 위험해 진다.

이 중에서 Pairwise 키와 랜덤 Pairwise는 베이스 스테이션 없이 안전성을 제공한다. 센서 노드들은 베이스 스테이션을 매우 신뢰하며, 베이스 스테이션은 센서 노드들 보다 메모리와 컴퓨팅 파워 등이 강해서 센서 노드들이 자원 제약성 때문에 하지 못하는 일을 할 수 있다. Pairwise는 센서 네트워크를 구성하는 센서 노드의 수에서 자신의 노드를 제외한 수(n-1)만큼 키를 가지고 있으며, 랜덤 Pairwise는 전체 네트워크 센서 노드의 키링에 저장된 만큼 가지고 있다.

랜덤 키는 인접한 노드와 링크를 생성할 수 있지만, 이때 서로 인접한 노드끼리 키가 겹칠 수 있다.

랜덤 키에 비해서 q-합성수 랜덤 키는 안정적이라고 할 수 있다. 노드가 캡쳐 당해도 전체 네트워크에 미치는 영향이 작기 때문이다. 하지만 q-합성수 랜덤 키 역시 인접한 노드끼리 키가 겹칠 수 있으며, 반면에 인접한 노드라도 q를 만족하지 못하면 링크가 생기지 않는다.

이러한 랜덤 키 분배 문제를 해결하기 위해서 Multi-Path 키를 만들었다. 하지만 이 분배 기법은 경로를 찾을 때 오버헤드가 발생한다.

[표 2-1] 키의 사전 분배 종류의 장단점

키의 사전 분배	장점/단점	
마스터 키	장점	모든 노드가 단일키 하나만 저장
	단점	단일키가 깨지면 전체 네트워크 깨짐. 새 노드 추가 불가.
Pairwise 키	장점	베이스 스테이션 없이 안전성을 제공. 노드 사이의 고유한 키 사용.
	단점	키 생성 비용과 센서 노드 메모리 사용 증가. 새 노드 추가 불가.
랜덤 키	장점	인접한 노드와 링크 생성 가능.
	단점	어떤 두 노드 사이의 키를 다른 인접한 노드가 가질 수 있음 .
q-합성수 랜덤 키	장점	랜덤 키 사전 분배에 비해 안전성 증가. 적은 수의 노드가 캡쳐 당했을 때 전체 네트워크에 미치는 영향 적음.
	단점	인접한 노드라도 q를 만족하지 않으면 링크 생성 불가능. 두 노드 사이의 키를 인접한 다른 노드가 가질 수 있음.
Multi-path 키	장점	랜덤 키 사전 분배 문제 해결.
	단점	경로 찾기 위한 오버 헤드. 중간 노드의 신뢰가 있어야 함.
랜덤 Pairwise 키	장점	불필요한 메모리 공간 문제 해결 베이스 스테이션 없이 안전성을 제공. 노드 사이의 고유한 키 사용.
	단점	인접한 노드와 Pairwise 키가 키링에 없으면 링크 생성과 새 노드 추가 불가능

[표 2-2]는 키의 사전 분배 종류별로 키의 개수와 메모리의 크기를 계산한 것이다.

[표 2-2] 키의 사전 분배 키 개수와 메모리 크기

키의 사전 분배	특징	
마스터 키	키의 개수	1
	메모리 크기	x
Pairwise 키	키의 개수	$n-1$
	메모리 크기	$(n-1)\times x$
랜덤 키	키의 개수	m
	메모리 크기	$(m+path)\times x$
q-합성수 랜덤 키	키의 개수	m
	메모리 크기	$(m+path+d)\times x$
Multi-path 키	키의 개수	m
	메모리 크기	$(m+path+d)\times x+ran$
랜덤 Pairwise 키	키의 개수	$m=np$
	메모리 크기	$m\times x$

- o n : 센서 네트워크를 구성하는 센서 노드의 수
- o x : 키 하나의 크기
- o m : 노드의 키 링(key ring)에 저장되어 있는 키의 수 $(m<n)$
- o $path$: 키 설정 이후 경로 키(path key)의 수
- o d : 인접한 노드와 생성한 링크의 수
- o ran : 다중 경로 키(multi-path)를 위한 랜덤한 값을 저장할 메모리의 크기

제 2 절 공개키 기반의 분배 기법

1. ECC (Elliptic Curve Cryptography)

가. ECC 개요

ECC(Elliptic Curve Cryptography)는 1985년 Neal Koblitz와 Victor Miler가 각각 독립적으로 제안한 알고리즘으로 타원곡선 이산 로그 문제(ECDLP : Elliptic Curve Discrete Logarithm Problem)를 기본으로 한다. ECDLP는 타원곡선 상의 임의의 한 점 P에 정수 K를 곱한 값이 $Q = kP$일 때, 점 Q와 P를 알더라도 정수 K를 계산하기가 어렵다[61, 62].

나. 분배 방법

ECC를 이용한 키 교환 과정은 다음과 같다.

선택된 타원곡선상의 임의의 점 P를 선택한다. 그리고 사용자 A, B는 자신의 개인키로 점 P를 계산하여 각각의 공개키를 생성한다.

$$P_A = k_A B, \quad P_B = k_B B$$

생성된 공개키를 A, B가 서로 교환하고, 전달 받은 상대방의 공개키와 자신의 개인키를 계산하면, 아래의 형태로 나타나며 서로 동일한 키를 생성하게 된다[63].

$$P_S = k_A(k_B B) = k_B(k_A B)$$

다. 장점

ECC는 ElGamal과 RSA(Ron Rivest, Adi Shanmir, Leonard Adleman)에 비해 작은 키 사이즈를 가지며, 빠른 속도와 높은 안전성을 갖는다. 이러한 장점 때문에 최근 무선 환경과 같이 전송량과 계산량이 적은 환경에 적합하다는 것

이 일반적인 의견이다. 그래서 그 활용도가 점차 증가하고 있다.

라. 단점

ECC는 유한체 이론 및 정수론을 기반으로 한 배경 이론을 가지므로 상대적으로 연산이 복잡하다. 그러므로 해당분야의 전문 지식이 있어야 하기 때문에 구현하는데 어려움이 많다.

2. ECDH (Elliptic Curve Diffie-Hellman)

가. ECDH 개요

ECDH(Elliptic Curve Diffie-Hellman)는 타원 곡선을 이용한 암호시스템에서 기존의 디피-헬만(Diffe-Hellman)에 해당하는 방법이다. 이것은 임의의 두 사용자가 안전한 랜덤 키를 사용할 수 있도록 한다. 이 프로토콜은 타원곡선 상의 이산대수 문제에 기반 한다.

노스캐롤라이나 주립 대학에서는 ECC를 TinyOS 상에서 구현하여 키를 안전하게 분배하고 있다. 실제 사용을 위해 타원곡선 기반 암호화 프로토콜인 ECIES와 키 분배 프로토콜인 ECDH, 서명 기법인 ECDSA 프로토콜을 구현하였다.[64] 본 보고서에는 키 분배 프로토콜인 ECDH를 설명하였다.

나. 분배 방법

ECDH는 DH(Diffie-Hellman) 알고리즘을 타원곡선으로 변환한 것으로 X9.63(미국 표준 협회의 X9 시리즈 프로토콜 중의 하나)로 표준화 되고 있는 중이다. 다음은 타원 곡선 이산로그를 이용한 Diffie-Hellman 키 교환 방식이다[65].

두 센서 노드는 서로 동일한 타원 곡선 $E(F_q)$, 생성원 $G \in E(F_q)$와

생성원의 위수 n을 미리 알고 있다고 가정한다.

이 때 각 센서 노드는 자신들의 개인키 $x_a, x_b \in [2, \ldots, n-2]$를 선택하고, 공개키 $Q_a = x_a G$, $Q_b = x_b G$ 를 계산한다.(이것은 타원 곡선 이산대수 문제이다.) 그래서 서로 공개키를 교환한 뒤에 상대 센서 노드의 공개키와 자신의 개인키를 이용하여 공유키 $K = x_a x_b G = (x_k, y_k)$를 공유할 수 있는 것이다.

다음은 ECDH 알고리즘 과정을 나타낸 것이다.

- o 타원 곡선 $E(F_q)$와 $G \in E(F_q)$를 선택하여 공개한다.
- o 각 센서 노드는 정수 $x_a, x_b \in [2, \ldots, n-2]$ 를 선택하여 비밀 키로 가진다.
- o 센서 노드는 각각 $Q_a = x_a G$, $Q_b = x_b G$를 계산하여 서로 나누어 가진다.
- o 센서 노드는 각각 $K = x_a(x_b G)$와 $K = x_b(x_a G)$를 계산하여 K를 공유한다.

다. 장점

ECDH(Elliptic Curve Diffie-Hellman) 키 분배 기법은 실제로 비밀 키를 전송하는 것이 아니기 때문에 기밀성과 인증성을 제공한다. 한 방향 함수의 특성을 이용하여 공격자가 비밀 키를 알기 위해 더 많은 시간이 걸리도록 이산수학을 기반으로 계산적으로 어렵게 만들었다. 그리고 대칭키 암호 알고리즘 기반의 키 분배 기법보다 다소 긴 시간이 소요되지만, 실제 응용에 사용되는 경우에도 충분히 실제 사용 할 수 있다[65].

라. 단점

ECDH(Elliptic Curve Diffie-Hellman) 키 분배 기법의 문제점은 비밀 교환 방식에 바탕을 두고 있기 때문에 중간자 공격(Main-in-the-Middle)에 취약한 점이다. 중간자 공격이란 A와 B 사이에 중간자가 침입을 하여 잘못된 공개 값을 주고받는 것이다. 즉 A가 B에게 보내는 공개 값을 중간자 Z가 가로채어 B를 가장하여 자신이 생성한 공개 값을 A에게 전송한다. 또한 중간자 Z는 A를 가장하여 공개 값을 생성하여 B에게 전송한다. 이 결과 Z는 A뿐만 아니라 B와 공유하는 키들을 사용할 수 있게 된다. 따라서 A와 B사이의 통신 내용을 모두 도청하거나 변조할 수 있게 된다.

ECDH 키 분배 기법은 상대방에 대한 인증 기능이 없기 때문에 실제 키 분배 방식에서는 디지털 서명과 같은 별도의 메시지 인증 절차를 추가로 수행해야 한다.

제 3 절 센서 네트워크 보안 프로토콜(Protocol)

1. LEAP (Localized Encryption and Authentication Protocol)

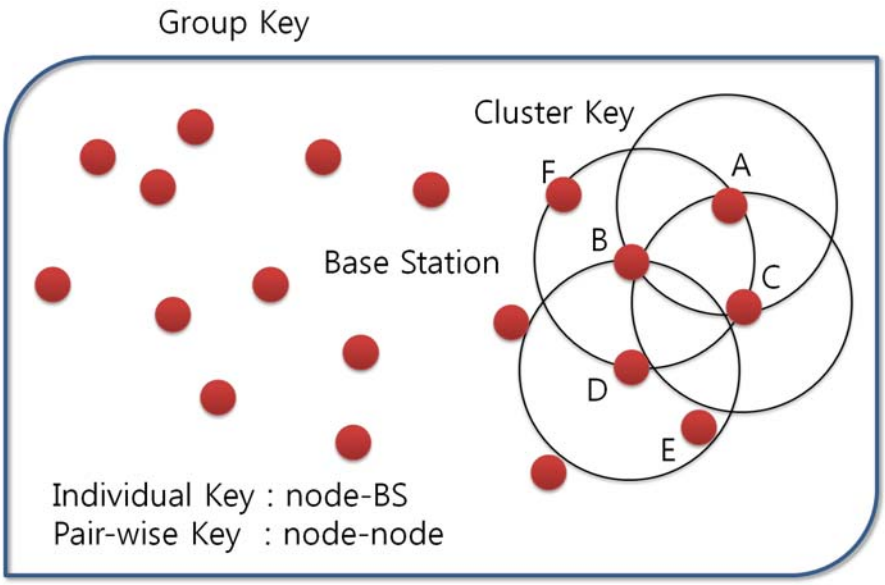
가. LEAP 개요

2003년 Sencun Zhu, Sanjeev Setia, Sushil Jajodia이 제안한 로컬 암호화와 인증 프로토콜 LEAP(Localized Encryption and Authentication Protocol)는 프로세싱을 제공하는 센서 네트워크를 위한 키 관리 프로토콜이다.

LEAP는 마스터 키 기반의 방식으로, 같은 시간 동안 어떤 센서 노드의 정보가 노출 되었을 때, 이웃 센서 노드까지 노출 되는 피해를 줄이기 위해서 제안 되었다. 이 기법은 노드 식별자를 이용하여 이웃 센서 노드와 공유키를 생성한 다음 마스터 키를 제거한다. 그러면 노드의 정보가 노출 되더라도 이

웃 센서 노드와 공유한 키를 공격자에게 노출 되지 않을 수 있다.

LEAP에서 모든 센서 노드는 4개 키를 가지고 있다. 4개의 키는 개인키, Pairwise 키, 클러스터 키, 그룹 키로 구성되어 있다[2, 3, 46, 10, 16, 23, 29].



(그림 2-14) LEAP 구조

나. 분배 방법

모든 센서 노드는 개인키, Pairwise 키, 클러스터(Cluster) 키, 그룹(Group) 키를 가지고 있다.

다음은 LEAP 구조 분배 방법을 설명하기 위한 표기이다.

o u, v : 센서 노드
o $\{f_K\}$: Pseudo Random 함수
o $\{s\}_K$: 키 K로의 암호화
o MAC(k, s) : 대칭키 k를 사용한 MAC 값

(1) 개인키 설정

개인키는 베이스 스테이션과 공유하는 개인키를 가진다. 이 키를 통해 센싱(Sensing)한 이벤트 보고용 MAC(Message Authentication Code)를 생성하는데 사용되며, 노드가 배치되기 전에 미리 로드 되어야 한다.

노드 u를 위한 개인키는 Pseudo Random 함수 $\{f_K()\}$와 베이스 스테이션의 마스터 키 K_u^m를 사용해 베이스 스테이션이 아래와 같이 생성 된다.

$$K_u^m = f_{K_u^m}(u)$$

(2) Pairwise 키 설정

Pairwise 키는 센서 노드가 이웃한 다른 센서 노드들과 공유하는 키이다. 이 키를 통해서 다른 노드들과 프라이버시와 소스 인증 같은 안전한 통신이 가능하다.

(가) 키 사전 분배

노드는 배치되기 전에 동일한 초기의 키 K_I를 메모리에 저장시킨다. 그리고 각 노드는 그 K_I로부터 Pseudo Random 함수를 이용해서 자신의 마스터 키를 생성한다. 예를 들면 노드 u와 v 사이의 키를 설정하기 위해서 베이스 스테이션(Base station)은 노드 u에게 초기키를 사전에 할당한다. 그다음에 u는 이 키를 이용하여 마스터 키를 생성하게 된다.

$$K_u = f_{K_I}(u)$$

(나) 이웃 노드 발견

노드가 배치 된 후에 노드 u는 T_{min} 타이머를 작동 시키고 자신의 아이디(ID)와 랜덤 수 N_u를 브로드캐스트 한다. 이를 받은 이웃 노드 v는 마스터 키

K_v로 MAC를 만든다. 그리고 자신의 아이디와 마스터 키 K_v가 사용된 인증 코드를 포함하여 MAC를 전송한다. 노드 u는 K_v를 계산하여 노드 v의 ID와 메시지를 인증한다.

$$u \rightarrow *: u, N_u$$
$$v \rightarrow u: v, MAC(k_v, N_u | v)$$

(다) Pairwise 키 확립

두 노드 u와 v는 주고받은 데이터를 기반으로 Pseudo Random 함수를 사용하여 두 노드 간의 동일한 Pairwise 키를 생성한다. 노드 u가 자신의 이웃 노드 v를 찾는 Pairwise 키 K_{uv}는 다음과 같이 계산된다. 이때 아이디 u가 아이디 v보다 작은 아이디일 경우 아래와 같다.

$$K_{uv} = f_{K_v}(u) \quad (u < v)$$

(라) 키 제거

타이머가 끝나서 초기 키 설정이 끝나면 저장된 초기키와 중간 Pairwise 키 생성 할 때 사용한 마스터 키를 메모리에서 완전히 삭제한다.

(3) 클러스터 키 설정

클러스터 키는 클러스터 헤더가 랜덤하게 만들었으며, Pairwise 키를 이용해 암호화하여 이웃 센서 노드에게 전달한다. 그래서 같은 클러스터에 속한 센서 노드들은 그 노드들 사이의 데이터 통합과 안전한 통신이 가능하다.

센서 노드 u가 이웃 노드 v_m과 통신을 원하는 경우에 클러스터 키를 확립한다. 우선 노드 u는 랜덤 키 K를 생성하고, 생성된 키를 각각의 이웃 센서 노드와의 Pairwise 키로 암호화하여 전달한다.

$$u \rightarrow v_i : (K_u^c)_{k_{ui}}$$

(4) 그룹 키 설정

그룹 키는 베이스 스테이션과 센서 네트워크의 모든 센서 노드들이 공유하는 키이다. 이 키를 사용하여 센서 네트워크의 모든 노드들에게 브로드캐스트 할 경우 메시지(쿼리 메시지, 이벤트 등록 및 삭제, 탈취된 노드 알림 등등)를 암호화하여 전송하기 위해 사용한다. 이 키는 노드가 배치되기 전에 각각의 센서 노드들에게 할당 된다.

다. 장점

USN 환경에서 노드들의 에너지 사용 제한과 노드들의 계산 능력이 떨어지는 것을 위해 LEAP에서 대칭키를 사용하여 초경량으로 메시지를 암호화하거나 복호화 한다.

노드는 위의 제약 사항을 만족하면서 대량의 센서가 흩어져 있는 센서 네트워크에서 4개의 암호화 키를 사용하는 영역 암호화 및 인증 프로토콜로, 안전하고 효율적인 네트워크를 구성하기 위해서 노드는 노드 사이에 MAC 확인을 통해 인증(authentication)을 한 후에, 받은 메시지를 포워딩(forwarding)하거나 프로세싱(processing)한다. 이렇게 함으로써 DoS 같은 공격을 막아 에너지 소모를 줄이며, 이웃 센서 노드의 피해를 줄일 수 있다.

이러한 키 관리 메커니즘을 통해서 in-network 프로세싱이 가능하게 된다. 동시에 이웃 노드가 보안 위협에 노출되더라도 노드의 보안을 유지 할 수 있다.

라. 단점

LEAP 기법은 센서 노드가 배치되기 전에 개인키와 그룹 키를 탑재 된다.

그렇기 때문에 악의적인 공격자가 센서 노드의 정보를 획득 할 수 있다. 만약 이때, 초기화 과정이 끝나기 전에 센서 노드가 탈취된다면, 이 악의적인 공격자는 1분 이내에 센서 노드에 저장된 모든 정보를 획득하게 된다. 그러면 센서 네트워크에서 사용하고 있는 모든 키들을 생성 할 수 있는 것이다.

2. SPINS(Security Protocol for Sensor network)

가. SPINS 개요

SPINS(Security Protocol for Sensor networks)는 A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar가 센서 네트워크 보안을 위해 초기에 제안한 인증 메커니즘이다. 믿을 수 있는 베이스 스테이션을 통하여 통신 가능한 이웃 센서 노드와 키를 교환하는 방식이다.

센서 네트워크 환경을 위한 보안 프로토콜 집합인 SPINS는 SNEP와 μTESLA로 구성되어 있다[2, 9, 10, 20, 25, 30].

SNEP(Secure Network Encryption Protocol)은 노드 사이의 통신에서 데이터 기밀성을 제공하기 위한 대칭키 암호 프로토콜이다. 그리고 nonce 값과 MAC(Massage Authentication Code)를 이용하여 데이터 기밀성뿐만 아니라 무결성 및 데이터 인증을 제공한다. 그리고 종단 간 통신의 보안과 적시성(freshness)을 제공하며, 시멘틱 보안에 대한 안전성(semantic secureness)을 보장한다.

센서 노드 A가 센서 노드 B에게 메시지 D를 보내기 위해서 A는 D를 마스터 키로 유도된 암호화 키 K_{encr}와 카운터 C를 이용하여 데이터를 암호화 한다. 그리고 암호문에 C를 붙여서 MAC 키로 MAC 값을 만들어 전송 한다.

이 식은 SNEP 프로토콜에서 센서 노드 A와 B의 통신을 나타낸다.

- o MAC(Key, Message) : 메시지 인증 코드 함수
- o {M}<Key, IV> : 메시지 M이 대칭키 Key와 초기벡터 IV를 이용하여 암호화 됨

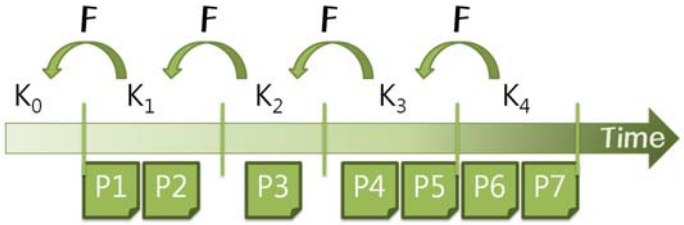
$$A \rightarrow B:\ N_A\ ,\ D_A$$
$$B \rightarrow A:\ \{D_B\}_{(K_{encr}, C)},\ MAC(K_{mac},\ N_A \mid C \mid \{D_B\}_{(K_{encr}, C)})$$

μTESLA는 A. Perrig 교수의 이전 연구 결과인 EMSS와 TESLA 프로토콜의 경량화 버전으로, 브로드캐스팅 되는 데이터에 대한 인증을 제공한다. 즉, 대칭키를 사용한 메시지 인증 프로토콜이다.

μTESLA는 단방향 함수(one-way function)를 통해 생성된 단방향 키 체인(one-way key chain) 기법을 사용한다. 그래서 동기화된 클럭을 기반으로 인증키의 지연 노출을 통한 비밀 키 암호로 공개키 암호와 같은 비대칭 키를 생성한다.

아래 (그림 2-15)는 μTESLA 프로토콜에 대한 도식도이다.

왼쪽에서 오른쪽으로 시간의 흐름을 나타낸다. k_{n-1}은 단방향 해쉬 함수 $F(k_n)$을 통해 얻어진 값이다. 각각의 패킷 Pi은 메시지와 MAC 그리고 Ki+k 값으로 구성되어 있다. 메시지를 받는 노드가 특정 시간 t에서 패킷 Pi를 받았다고 한다면, t+k 시간에서 얻어진 패킷 안의 Ki+k 값을 k번 해싱(hashing)해서 얻어진 Ki 값으로 MAC을 확인한다.



(그림 2-15) μTESLA 도식도

나. 분배 방법

(1) SNEP(Secure Network Encryption Protocol)

SNEP 프로토콜은 데이터의 기밀성, 완전성, 적시성, 인증, 재전송 보호와 시멘틱 보안에 대한 안전함을 제공한다. 특히 대칭키를 가지고 있지 않은 제 3

자가 노드들 간의 통신 도중에 데이터를 가로채도 데이터에 대한 어떠한 정보를 얻을 수 없고, 암호화를 해도 데이터를 알 수 없도록 하는 것이 시멘틱 보안의 목표이다. 즉, 도청자가 암호화된 데이터를 추측 하는 것으로부터 보호하는 것이다.

SNEP는 신뢰 할 수 있는 베이스 스테이션에서 센서 노드들이 설치되기 전에 베이스 스테이션과 공유하는 하나의 마스터 암호 키 K를 미리 분배 받는다. 이것을 기반으로 하여 Pseudo Random 함수를 통해 각 센서 노드의 독립적인 키가 생성된다.

$$\begin{array}{ll} \text{Encryption keys} & K_{AB} = F_X(1) \text{ and } K_{BA} = F_X(3) \\ \text{MAC key} & K'_{AB} = F_X(2) \text{ and } K'_{BA} = F_X(4) \\ \text{PNG key} & K_{rand} = F_X(5) \end{array}$$

각 노드는 생성된 키 K_{AB}, K_{BA}를 통해 서로 암호화와 복호화를 수행한다. 그리고 K'_{AB}, K'_{BA}를 통해서 MAC를 생성하고 검증한다.

MAC(Message Authentication Code)은 데이터의 인증과 무결성을 인증하는데 사용된다. 이러한 경우에 MAC은 CBC-MAC(Cipher Block Chaining)이 된다. CBC-MAC은 블록 암호의 CBD 모드를 사용하는 것이다. 이 방법은 CBC 모드를 사용하여 선택된 블록 암호로 데이터를 암호화 시킨 후에 암호문 블록을 가지고 MAC 값을 구하는 것이다. 즉, 평문의 각각의 블록을 암호화하기 이전의 평문 블록으로 XOR 시킨 것이 아래의 CBC-MAC이다. 암호화 메시지는 MAC을 포함할 것이다.

이와 같은 암호화 방식은 적시성, 비밀성, 재전송 보호를 제공한다.

$$A \rightarrow B : \{D\}K_{AB}, C_A, MAC(K'_{AB}, C_A || \{D\}K_{AB}, C_A)$$

- o D : 암호화된 데이터(카운터 모드에서)
- o K : 암호화 키
- o K′ : mac 암호화 키
- o C : 카운터

다음은 인증된 메시지 형식이다.

$$A \rightarrow B: D, MAC(K'_{AB}, D)$$

수식 과 같이 임시로 한번 사용할 숫자를 얻어 요구 메시지에 포함한다. 즉 데이터를 받는 쪽의 응답과 MAC의를 임시로 포함하고 있다.

$$A \rightarrow B: N_A, R_A \quad where\, N\, is\, a\, nonce \text{ and R the request}$$
$$B \rightarrow A: \{R_B\}(K_{BA,} C_B), MAC(K'_{BA}, N_A || C_B || \{R_B\}(K_{BA}, C_B))$$

만약 MAC이 올바르게 검증된다면 센서 노드 A는 센서 노드 B가 요구를 보낸 뒤 그 응답을 생성시켰다는 것을 알 수 있게 된다.

만약 카운터 교환 프로토콜이 필요하다면 읽혀진 메시지의 종류와 그 공유된 카운터의 일치하지 않는 상태인 것이다. 즉, 아래의 식은 카운터 값의 회득과 동기화를 위해 메시지를 보내는 것이다.

$$A \rightarrow B: C_A \; B \rightarrow A: C_{B,} MAC(K'_{BA,} C_A || C_B)$$
$$A \rightarrow B: MAC(K'_{AB,} C_A || C_B)$$
$$A \rightarrow B: N_A \; B \rightarrow A: C_{B,} MAC(K'_{BA,} N_A || C_B)$$

(2) μTESLA(micro timed efficient stream loss-tolerant authentication)

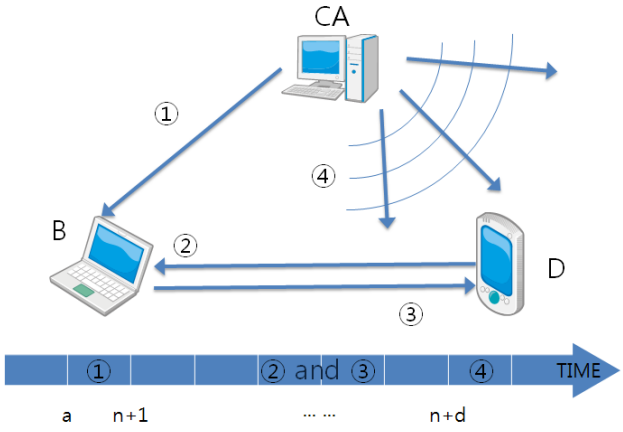
TESLA 방식은 스트림 데이터의 무결성을 보장하기 위한 멀티캐스팅 보안 프로토콜이다. TESLA 기법은 초기 패킷을 인증하기 위해서 디지털 서명을 사용하기 때문에 센서 네트워크에 적용하는데 무리가 있다. 따라서 μTESLA는 TESLA 방식을 확장하여 센서 네트워크에 적용 할 수 있도록 응용한 것이다. 그렇기 때문에 μTESLA의 인증 키 체인 생성이나 브로드캐스트 데이터 생성 방식은 TESLA와 비슷하다. 단, 베이스스테이션만 센서 노드에게 브로드캐스팅 할 수 있으며, 센서 노드끼리 브로트캐스팅 할 수 없다. 베이스스테이션만 패킷 인증을 위한 키 체인을 생성하고 유지한다. μTESLA는 TESLA와 다르게 초기 패킷 인증을 위한 전자 서명을 하지 않는다.

이 구조는 3계층의 Ad-hoc 네트워크 프로토콜을 가진다. 고전력의 AP(Access Point), 중전력의 이동성 전달 노드, 저전력의 이동성 센서 노드 구

조로 설정하고, TESLA를 사용한 효율적인 인증 방식을 가진다. 센서 노드 사이에 직접적인 통신은 없고, 중간에 위치한 이동성 전달 노드는 단순하게 전달 기능만을 갖는 노드이다. 그리고 모든 노드와 AP(Access Point)는 RSA(Ron Rivest, Al shamir, Len Adleman) 키 쌍과 TTP(Trusted Third Party)의 공개키를 가지고 있다고 가정한다.

TESLA 인증서 발급 방식은 다음과 같다.

- o CA(Certificate Authority)는 주기적으로 B에 대한 TESLA 인증서를 발급한다.
- o B는 발급 받은 TESLA 인증서를 보관하고 있다. 이때 말단 센서 D가 서비스를 요청한다.
- o 이에 대해 자신을 인증하기 위해서 인증 패킷을 발급한다. 발급한 패킷에는 B의 인증서와 TESLA 키를 이용한 MAC 값을 포함한다.
- o n+d 주기에 CA가 TESLA 키를 공개하면 D는 이 키를 사용하여 B에게 받은 인증 패킷을 검증하고, 패킷에 포함된 B의 인증키와 MAC 값도 검증한다.



(그림 2-16) TESLA 인증서 사용 단계

이 인증서를 사용하는 인증 프레임워크는 AP를 통해 검증된 센서로부터 왔는지 데이터가 도착했는지, 도착한 데이터가 변조되지 않았는지 확인한다.

μTESLA에는 다섯 가지 상태가 존재한다. 다섯 가지 상태는 보내는 측의 설정, 브로드캐스팅 된 패킷의 인증, 새 수락자의 Bootstrapping, 브로드캐스팅 된 패킷의 인증, 노드들의 브로드캐스팅 되어 인증된 데이터이다.

(가) 보내는 측의 설정

보내는 측은 F 함수인 단방향 키 체인을 이용하여 보안키를 생성한다. 여기서 F는 단방향 함수(one-way function)로 K_0~K_n까지 알게 되더라도 그 다음 k_{n+1}에 해당하는 수를 추측할 수 없다. 아래 식은 키 체인 수행결과이다.

$$K_i = F(K_{i+1})$$

또한 시간을 각 interval로 나누어 그 키 값 K_i를 각 interval i에 할당한다.

(나) 브로드캐스팅 된 패킷의 인증

각각의 키는 시간 간격을 두고 interval i에게 전송된다. 송신자는 현재 나누어진 패킷의 각 interval 키 값 Ki를 이용하여 MAC 값을 계산하고, MAC 값과 패킷을 XOR 시켜 전체 노드에 뿌려진다.

(다) 새 수락가의 Bootstrapping

데이터를 받은 측은 임시 수락 메시지를 데이터를 보낸 측에게 보낸다. 데이터를 보내는 측에서는 보내는 측의 현재 시간, 키 체인의 만료 시간 키, 시간 간격의 시작 시간 i, 시간 가격과 지연의 알림 지속시간을 포함한다.

(라) 브로드캐스팅 된 패킷의 인증

데이터를 받은 측에서는 패킷이 변경되지 않고 안전하다는 것을 확인할 필요가 있다. 안전하지 않은 패킷은 버려질 것이고, 안전한 패킷은 첫 번째로 새롭게 주어진 키와 그 패킷은 인증된다.

(마) 노드들의 브로드캐스팅 되어 인증된 데이터

모든 설정을 마친 노드들은 인증된 데이터를 브로드캐스팅 하게 된다.

다. 장점

SPINS의 장점은 마스터 키와 Pseudo Random 생성 함수를 통해 키를 만들어 냄으로써 키의 교환이 필요 없다. 이는 키 생성과 분배에서 직접적인 키 이동이 없어서 안전한 방법이라고 할 수 있다.

또한 생성된 키를 바탕으로 암호화를 통해 데이터 기밀성과 MAC을 통한 두 노드 사이의 데이터 인증, 무결성을 제공해 주며, 신뢰 가능한 베이스 스테이션을 통하여 이웃 센서 노드와 키를 교환한다.

라. 단점

각 노드들은 키 교환을 위해 베이스 스테이션과 통신을 한다. 그렇기 때문에 베이스 스테이션 주위의 노드들의 급격한 에너지 소모가 발생하게 된다. 그러므로 대규모 센서 네트워크 환경에서는 비효율적인 방법이 될 수 있다.

SPINS는 정보가 유출되거나 센서 노드가 물리적인 위협을 받을 때 이러한 위협으로부터 복원할 수 있는 방법, 즉 노드의 폐기, 추가, 키 갱신을 제공해 주지 않는다.

이 기법의 키 생성이 단순하기 때문에 마스터 키가 유출 되면 통신에 사용되는 키들이 쉽게 노출 될 수 있다.

μTESLA는 모든 센서 노드들이 시간적으로 동기화 되어 있어야 한다. 또한 네트워크로 전송 지연이 발생 할 수 있으므로 키 노출 지연 시간이 필요하며 패킷을 위한 저장 공간도 필요하다.

제 3 장 USN 환경에서의 공격기법

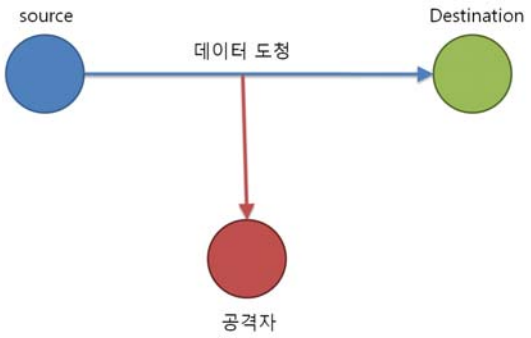
본 장에서는 USN 환경에서 발생 할 수 있는 공격 기법과 USN 보안 기술을 분석하였다. 1절에서는 도청, 데이터 위변조, 서비스거부, 라우팅 공격, 물리적 공격을 자세히 분석하였다. 2절에서는 키 관리 기술뿐만 아니라 경량 암호 및 인증 기술, 물리적 공격 및 부채널 방지 기술, 라우팅 공격 방지 기술, DoS 방지 기술, 프라이버시 보호 기술을 전반적으로 알아보았다.

제 1 절 공격 유형 분석

1. 도청(Eavesdropping)

가. 도청 개요

도청(Eavesdropping)이란 USN에서 정보의 흐름이나 내용을 변경하지 않고 몰래 수신만 하는 것을 말한다. 도청은 USN에서 소극적 공격의 한 종류로 보안의 기밀성을 해친다.



(그림 3-1) 도청(Eavesdropping)

USN을 구성하는 각 센서 노드들은 일반적으로 IEEE 802.15.4와 같은 무선 통신으로 구성되기 때문에 무선 통신상에서 주고받는 데이터에 대한 기밀성이 제공되지 않을 경우 외부 공격자에 의해 손쉽게 도청 당할 수 있다[6].

예를 들어 RFID 시스템에서 태그와 리더 사이의 통신은 높은 효율성을 나타내기 위해 수 미터의 범위 안에서도 가능하다. 그리고 태그와 리더 사이의 통신은 라디오 방식이기 때문에 누구든지 태그에 접근하여 태그의 출력 값을 얻을 수 있다[8].

이러한 특성을 이용하여 개인의 상세 정보, 기업의 비밀 등의 데이터를 빼낼 수 있으며, 만약 USN 센서노드들이 누구나 접근 가능한 공공장소에 설치되어 있으면 이러한 도청 위협이 더욱 커질 수 있다.

나. 도청 공격 종류 및 기법

센서 노드들 사이의 통신 범위 안에 도청 공격자가 있으면 도청이 이루어질 수 있다. 도청에는 도청자가 자신을 숨기고 센서 노드간의 중간 통신만 수신하는 소극적인 도청이 있고, 도청자가 센서나 데이터를 통합하는 시스템에 직접 신호를 보내어 적극적으로 정보를 알아내려는 적극적 도청이 있다. RFID로 예를 들면 도청자가 리더기와 태그 사이에서 통신을 라디오주파수(RF)로 수신하는 것은 소극적 도청이고, 도청자가 리더를 가지고 태그를 스캐닝(Scanning) 하는 것은 적극적 도청에 해당 된다[8].

[표 3-1]은 도청 공격의 종류를 정리한 것이다.

도청 공격의 대표적인 예로 스니핑 공격이 있다. 이 절에서는 스니핑 공격이 어떻게 이루어지는지를 통해 도청의 원리를 설명하고자 한다.

(1) 스니핑(Sniffing) 공격

스니퍼(Sniffier)는 네트워크에서 송수신되는 트래픽(Traffic)을 도청하는 장치를 의미하며, 스니핑(Sniffing)은 스니퍼를 사용해서 데이터를 도청하는 행위를 의미한다[81].

[표 3-1] 도청의 유형

도청 종류	내용
데이터 내용 도청	개인 사생활, 기업 기밀 등의 문제로 기밀성 저해
센서 노드 ID 도청	노드의 ID는 노드의 인증이나 서비스에 이용되는 중요한 정보로, 신분위장 공격이나 서비스 거부 공격을 수행 할 수 있는 정보 유출
단말 시스템의 인증 데이터 도청	불법적인 접속을 시도 할 수 있는 정보 유출
센서 노드 인증 데이터 도청	불법적인 접속을 통한 신분위장 등의 공격을 수행 할 수 있는 정보 유출

다시 말하면, 도청이란 네트워크에서 전달되는 정보를 엿보고 가로채는 공격 행위로, 컴퓨터 네트워크 상에 흘러 다니는 트래픽을 엿듣는 도청 장치인 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 스니핑이라고 한다.

스니퍼는 다음과 같은 동작으로 공격을 시도한다. 네트워크 디바이스를 열어서 “promiscuous mode(혼잡모드 : 자신이 목적지가 아님에도 모든 정보를 받아들이는 모드)"로 만들어 지나가는 모든 트래픽을 볼 수 있다. 이렇게 트래픽을 필터링함으로써 발신 및 수신주소, 서비스, 계정과 패스워드가 포함된 데이터를 구분해서 출력하는 동작을 실행한다. 따라서 USN 네트워크에 흐르는 트래픽을 스니핑 함으로써 암호화되지 않은 정보가 쉽게 모니터링 당하는 USN 센서 노드 혹은 네트워크의 도청이 이루어진다.

다. 도청 대응 기법

(1) 일반적인 도청 대응 기법

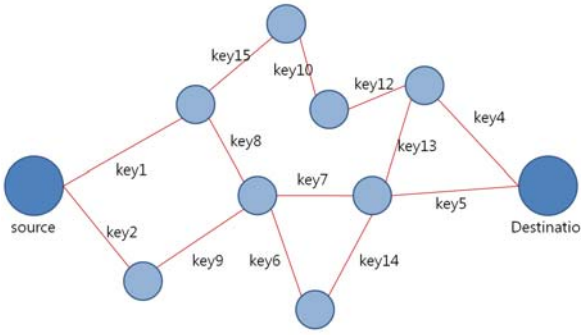
USN에서 전달되는 정보는 제 3자에게 전달되지 않아야하고, 만약 전달된다 하더라도 그 정보가 정확히 어떤 정보인지 알 수 없는 무의미한 정보가 되어야 한다. 따라서 기밀성을 위해 무선 통신 상에서 주고받는 데이터에 암호화를 적용하거나 통신 채널에 암호화를 적용하여 해결 가능하다. 위의 도청 기법인 스니핑 공격에 대한 대응 방법 역시 암호화를 사용하는 것이며, 보편적으로 사용되는 암호기법으로 공개키 암호 기법이 있다.

(가) 데이터 전송 경로에 암호화 하는 기법 [58]

첫 번째로 통신 채널에 대해 암호화(기밀성)를 제공함으로써 해결 하는 기법이 있다. 하지만 이 기법은 센서 노드의 자원 제약성 때문에 암호화 기능을 제공하는 것이 쉽지 않아서 키 분배 및 관리에 문제가 발생한다.

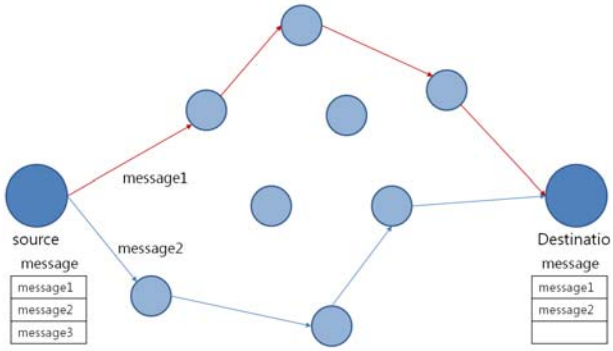
(그림 3-2) 통신 채널 암호화

두 번째로 인접 노드 사이의 암호화 기능을 제공함으로써 인접 노드 간에만 키를 공유 하는 기법이 있다. 하지만 위·변조 노드가 존재하는 경우에는 노드 사이에 형성된 보안의 의미를 잃게 된다.



(그림 3-3) 인접 노드 사이의 암호화

세 번째로 다중 경로 라우팅 기법을 사용하는 기법이 있다. 이 기법은 독립적인 여러 경로를 통해서 메시지를 분할 전송 한다. 그리고 목적지 센서 노드에서 다시 합하여 정보를 얻는다. 이렇게 함으로써 중간 경로에서 도청을 당할 위험을 방지하게 된다.



(그림 3-4) 다중 경로 라우팅

(나) 알고리즘 기반 도청 방지 기법

도청을 방지하기 위헌 알고리즘 기반 암호화 방법으로 트리워킹 알고리즘이 있다. 트리워킹(Tree-walking) 알고리즘은 ID의 첫 번째 비트부터 시작하여 비트 단위로 노드를 구분하여 노드를 분류해 가면서 하나의 노드를 선별하는 기법이다[82].

RFID 시스템을 예로 들면, 리더는 자신과 통신 할 수 있는 전파 범위 안의 태그들에게 ID를 요청한다. 만약 이 신호에 응답하는 태그가 복수 개인 경우는 전파 충돌로 인해 태그를 인식하지 못하게 된다. 복수개의 태그가 응답 한 경우 ID의 첫 번째 비트가 0인 태그에 대한 ID만 응답할 것을 다시 요청한다. 만약 또 충돌이 발생한다면 ID의 다음 비트들을 차례로 명시하여 충돌을 방지한다.

이와 같은 트리워킹 알고리즘을 이용하여 도청을 막는 방법으로 고요한 트리워킹(Silent Tree-walking)과 랜덤 트리워킹(Randomized Tree-walking)이 있다.

1) 고요한 트리워킹(Silent Tree-walking)

일반적으로 바이너리 트리워킹 방식으로 통신을 할 경우 리더가 태그의 각 ID를 브로드캐스트하기 때문에 도청자에게 태그의 정보를 주게 된다. 그래서 태그가 리더에게 보내는 데이터는 도청자가 도청 할 수 없다는 것에 착안하여 만들어진 고요한 트리워킹 방식은 리더가 태그의 정보를 부르지만 태그가 리더에게 보낸 마지막 데이터와 리더가 태그에게 보내고 싶은 데이터를 XOR 하는 방식으로 이루어진다.

2) 랜덤 트리워킹(Randomized Tree-walking)

랜덤 트리워킹 방식은 자신의 실제 ID와 랜덤하게 생성한 다른 ID를 가진 태그가 랜덤 ID를 리더에게 보내고 리더는 태그의 ID를 찾기 위해 트리워킹을 시도하는 것이다. 만약 도청자가 도청을 한다면 이때 수집 되는 ID는 태그의 실제 ID가 아닌 랜덤하게 생성된 쓸모없는 ID가 된다. 이 기법은 태그가 자신이 생성한 랜덤 ID를 반드시 기억하고 있어야 한다는 제약 사항이 있다.

3) 재 암호화(Re-Encryption)

재 암호화 기법은 공개키 암호화 시스템을 사용하여 암호화한 고유 번호를 태그에 덮어 쓰는 방식이다[80]. 이 기법은 태그의 제안된 컴퓨팅 리소스를 가지기 때문에 공개키 암호화 시스템을 믿을 수 있는 외부 계산기에 의해 암호 연산한다. 이 기술에서 공개키에 의해 암호화된 암호문은 주어진 태그의 연결성(link-ability)을 감소시키기 위해 주기적으로 재 암호화(re-encryption) 된다[9].

(2) 도청 방지를 위한 키 관리

도청은 센서 노드들 간에 전송되는 정보의 흐름이나 내용을 변경하기보다는 수신만 하는 소극적 공격에 속한다. 도청 공격을 막기 위해서는 전송되는 정보는 도청하는 공격자에게 노출 되지 않도록 하여 송신자와 수신자만 알고 있어야 한다. 따라서 센서 노드 하나에 대한 암호키 공격의 효과가 전체 네트워크로 확산되지 않도록 키를 제어하는 관리 기법을 이용해야 한다.

도청 공격을 방어하기 위한 키 관리 기법에는 센서 노드와 노드 사이에 키를 설립하는 Pairwise 키 기법이 있다. 인접한 두 노드 사이에만 암호화가 되어 있기 때문에 다른 노드가 암호화된 데이터를 알 수 없게 되므로 도청을 막을 수 있다.

그리고 다른 방법으로 Multi-path 기법을 이용 할 수 있다. Multi-path는 하나의 데이터를 여러 패킷 단위로 분할하여 다양한 경로를 보냄으로써 도청자가 전송되는 중간에 데이터를 수신한다 하더라도 전체 데이터의 정보를 알아차릴 수 없기 때문에 전체 네트워크에 미치는 영향이 적다.

또한 소규모의 네트워크의 경우 마스터 키를 이용하여 전체 통신 채널 구조를 보안하는 방법도 사용될 수 있다. 도청이 이루어지고 있다고 판단되면 빠르게 마스터 키를 빠르게 재분배 하도록 한다.

2. 데이터 위변조 공격 (Data Fabrication&Modification)

가. 데이터 위변조 개요

USN의 각 센서 노드들은 무선 통신을 하기 때문에, 물리적인 제약 없이 통신 범위 안에 있는 공격자가 데이터 위변조 공격을 시도하는 것이 상대적으로 매우 쉽게 이루어진다. 다시 말하면 USN 네트워크에서 센서 노드들은 주변의 상황 정보를 인지하여 싱크 노드 혹은 게이트웨이 노드 등을 통하여 응용 시스템으로 정확히 전달하는 것이 목적인데 특별히 상황 정보의 정확성이 매우 중요한 응용 서비스에서 그 정확성이 크게 왜곡될 수 있다[6].

데이터 위변조 공격으로 전달되는 정보를 변조(Modification)하여 왜곡된 정보가 전달되도록 하거나 차단(Interruption)하여 인가된 노드가 읽지 못하도록 하거나 자신이 아닌 타임이 정보를 보낸 것처럼 위조(Fabrication)하는 것이 있다[71].

센서 노드의 메모리에 존재하는 데이터는 항상 공격자의 대상이 되며, 공격자는 이 데이터를 삭제하거나 수정하는 등 잘못된 데이터를 다른 센서 노드에게 보내어 공격자의 의도대로 동작하게 한다. 이렇게 잘못된 데이터를 통해 통신하게 하므로 치명적인 위험이 생기며 USN의 보안 요구사항인 가용성(Availability)을 침해하게 된다.

데이터 위변조 공격을 통해서 공격자가 미리 지정한 명령이 작동되도록 함으로써 노드의 권한을 획득 하여 노드의 센서 노드의 정보를 속여 정보를 변경 할 수 있다. 예를 들어, 어떤 물건에 부착된 센서 노드가 데이터 위변조 공격에 당해서 비싼 가격의 물건을 싼 가격의 물건으로 바꾸는 일들이 발생하게 될 수 있으며, 이러한 일은 기업의 입장에서 엄청난 손해이고, 신용카드나 현금카드에 사용되는 센서 노드가 공격당해서 복제되는 경우 개인이 막대한 피해를 입을 수 있다[80].

나. 데이터 위변조 공격 종류 및 기법

공격자에 의한 데이터 위변조 공격으로는 Terminal ID의 변조, 호 설정 메시지의 변조, 라우팅 정ㅂ의 변조, 노드 인증데이터의 변조, 등록 시 메시지의 변조, 통신내용의 변조 등이 있다. 이에 대한 자세한 사항은 [표 3-2]에서 정리하였다.

[표 3-2] 데이터 위변조의 유형

종류	내용
Terminal ID의 변조	RSA 메시지에서 Terminal ID는 단말 시스템을 확인하는데 꼭 필요한 메시지 요소이다. 이러한 점을 이용하여 공격자가 RSA의 메시지를 캡쳐하여 ID를 변경 한 후 전송하는 공격법
호 설정 메시지의 변조	calling ID, called ID 등을 변경하여 호 설정 메시지를 전송함으로써 서비스가 불가능하게 하거나 원하지 않은 과금을 받도록 하는 공격법
라우팅 정보의 변조	라우팅 정보를 변경하게 되면 메시지가 원하는 목적지로 도달 할 수 없게 하는 공격법
노드 인증 데이터의 변조	노드의 인증 데이터를 변경함으로써 인증 실패를 유발하여 서비스를 받을 수 없게 하는 공격법
등록 시 메시지의 변조	공격자가 노드의 게이트키퍼 등록 시 RRQ 메시지를 수정하여 게이트 키퍼로 하여금 과금 정산 등의 서비스를 노드의 설정과 다르게 만드는 공격법
통신 내용의 변조	실시간으로 전송되는 패킷에 대한 공격을 실시하여 통신이 불가능하게 하는 공격법
게이트키퍼 ID의 변조	게이트키퍼 ID를 변조하여 RAS 메시지를 공격자에게 전송하도록 하는 공격법

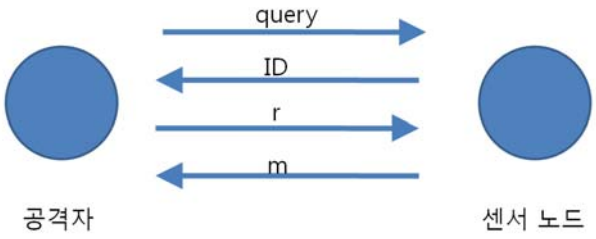
이 절에서는 데이터 위변조 공격의 일반적 기법인 스푸핑 공격에 대해 설명한다.

(1) 스푸핑(Spoofing) 공격

스푸핑 공격은 공격자가 IP 주소, 하드웨어주소(MAC address) 등의 정보를 속여서 중요한 정보의 권한이나 정보를 가로채고 서비스를 방해하는 공격을 말한다. 스푸핑 공격으로 센서 노드를 속여서 공격자의 연결이 정당한 것이고 통신 안에서 사용이 허락된 노드라고 여기도록 할 수 있다.

다음은 센서 노드가 스푸핑 공격을 당하는 과정이다[83].

- o 공격자가 센서 노드에게 query를 전송한다.
- o 공격자로부터 query를 수신한 센서 노드는 자신의 ID를 공격자에게 전송하게 된다.
- o 공격자는 백-엔드 데이터베이스와 인증 과정을 무시하고 랜덤 값을 생성하여 센서 노드에게 전송한다. 물론 랜덤 값은 이전 세션에서 도청한 랜덤 값 r을 이용하여 재전송 공격을 수행하여도 된다.
- o 센서 노드는 수신한 랜덤 값과 자신의 비밀 키를 이용하여 메시지 m을 계산하고 공격자에게 전송하게 된다.
- o 공격자는 이 메시지를 수신한 후 세션을 종료 한다.



(그림 3-5) 스푸핑 공격

다. 데이터 위변조 대응 기법

(1) 일반적인 데이터 위변조 대응 기법

USN 네트워크에서 데이터 위변조 공격에 대처하기 위한 기본적인 대응 조치로 공격자가 아닌 정상 노드만이 네트워크에 참여할 수 있도록 해야 한다. 다시 말하면 센서 노드에게 위변조 되지 않은 메시지를 보냈다고 확인 할 수 있는 신뢰할 수 있는 인증 기법이 필요하다는 것이다[67]. 즉, 이런 형태의 공격을 막을 수 있는 기법은 USN 네트워크에 추가적인 외부 인증 시스템을 도입하여 비 공인된 노드가 자원을 사용하는 것을 막는 것이다.

(2) 데이터 위변조 방지를 위한 키 관리

데이터 위변조 공격의 목표는 노드가 환경 정보를 센싱 하여 싱크 노드를 통하여 응용 시스템으로 전달하는 정보를 변경함으로써 센서 네트워크 보안요구 사항인 정확성을 침해하는 것이다. 따라서 노드에게 잘못된 데이터가 전송되고 보안이 깨지게 된다.

따라서 위와 같은 데이터 위변조 공격에 대응하기 위해서는 데이터를 전송하는 노드와 받는 노드 모두 정당한 노드임을 인증해야 하며, 노드 간에 전달되는 정보가 정당한 정보임을 인증해야 한다. 이와 같은 경우 두 노드 사이에 공개키를 이용하여 데이터를 암호화/복호화 하는 공개키 방식을 이용 할 수 있다.

또한 Pairwise 키 관리 기법을 이용하여 센서 네트워크 전체에서 두 노드 사이의 공유키를 사용함으로써 수신자가 수신한 정보가 정확한 정보임을 확인할 수 있다. Pairwise 키 관리 기법으로 Random pairwise, q-합성수와 같이 여러 가지가 있으며 상황에 따라서 적합한 Pairwise 키 관리 기법을 사용한다.

3. 서비스 거부 공격(Denial of Service)

가. 서비스 거부 공격 개요

서비스 거부 공격(Denial of Service)은 공격자가 호스트나 네트워크의 사용 가능한 자원을 독점하여 서비스를 제공하는 센서 네트워크 혹은 센서 노드에 대하여 서비스의 기능과 성능이 원활하게 이루어지지 못하도록 하는 모든 종류의 공격을 포괄한다[6]. USN 네트워크에서 서비스 거부 공격으로 센서 노드들의 하드웨어적인 문제, 소프트웨어 상의 문제 혹은 네트워크상의 전파 방해나 통신 장애등의 서비스 거부 공격이 있다. 다시 말하자면 공격자가 네트워크상에서 센서 노드를 공격하여 생기는 문제뿐만 아니라, 센서 노드의 배터리가 방전되거나 홍수 등과 같은 자연 혹은 인공 재해로 노드가 분실되거나 공격자에 의해 노드가 파괴 되는 등의 하드웨어적 문제도 있다. 그리고 센서 노드 자체의 버그가 생기거나 USN 네트워크에서 노드가 탈퇴하여 생기는 문제도 서비스 거부의 일종이다. 특히, RFID 시스템에서 자원에 대한 정상서비스를 방해하기 위한 공격으로 RF 신호 채널을 방해하거나, 임의의 다른 수단으로 태그를 무력화시키는 것도 포함된다[79].

이러한 DoS(Denial of Service) 공격으로 USN 센서 네트워크의 성능이 저하 될 뿐만 아니라 USN 센서 네트워크를 통해 서비스 받는 노드들은 정상적인 서비스를 받을 수 없는 일이 발생한다.

나. 서비스 거부 공격 종류 및 기법

DoS의 공격 형태 중 가장 단순한 공격은 공격자가 높은 에너지 신호를 브로드 캐스팅하여 네트워크의 동작과 기능을 혼란이나 마비시키는 것이다. 이보다 더 강력하게 공격하는 기법으로는 공격자가 802.11 매체 접근 제어(MAC : Medium Access Control) 프로토콜을 방해하여 통신을 못하게 하는 기법이 있다[7].

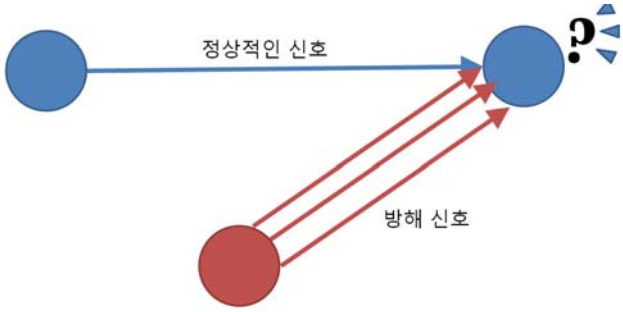
다음은 센서 네트워크 계층별로 서비스 거부 공격을 분석 한 것이다.

(1) 물리 계층(Physical Layer)

(가) Jamming

Jamming은 한 노드에 과다한 접속 요청으로 정상적인 요청을 처리할 수 없게 하는 공격이다[84]. 일반적으로 재밍이라고 하는 전파방해 공격은 지속적으로 의미 없는 전파를 계속 보내어 노드 정상적인 정보를 얻을 수 없도록 하는 것을 말한다. USN 네트워크는 무선 환경으로 센서 노드들이 밀집해 있는 경우 주파수 대역 자체가 복잡하기 때문에 고의적인 공격뿐만 아니라 전파 신호가 교란 되는 경우도 생길 수 있다.

예를 들어 (그림 3-6)과 같이 한 노드로 정상적인 신호뿐만 아니라 공격자가 고의적으로 보내는 신호들이 전송된다. 이 노드는 어떤 신호에 대해 정보 처리를 해야 하는지 혼란이 생겨 정상적인 서비스를 할 수 없게 된다.



(그림 3-6) Jamming

(나) Tampering

Tampering은 센서의 위치를 바꾸거나 손상을 입혀 상위 계층으로 접근하는 공격이다.

(2) 링크 계층(Link Layer)

(가) Collision

Collision은 전체 패킷을 고쳐 전송 시 체크섬(Checksum) 오류로 충돌을 일으키는 공격이다.

(나) Exhaustion

Exhaustion은 잦은 충돌 발생으로 계속된 패킷 전송을 통해 에너지 등의 자원을 고갈시키는 공격이다.

(다) Unfairness

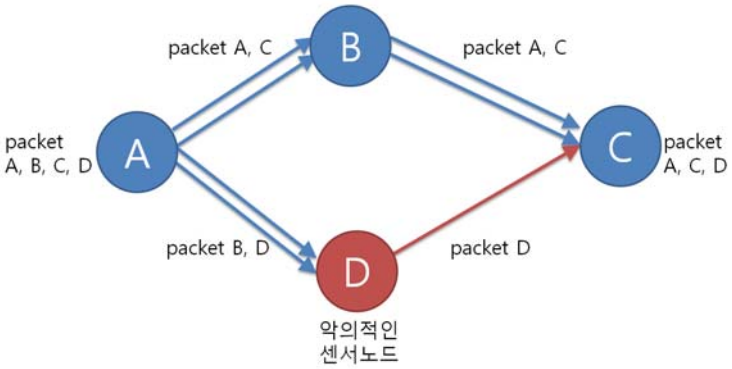
Unfairness는 MAC 프로토콜의 우선순위 등으로 데드라인(Dead Line)을 맞추지 못해 서비스를 적절한 시간에 제공받지 못하게 하는 공격이다.

(3) 네트워크와 라우팅 계층(Network and Routing Layer)

(가) Neglect and greed

Neglect and greed는 센서 노드로 오는 임의의 패킷을 다른 노드로 포워딩(forwarding)하지 않음으로써 데이터 전송을 막는 공격이다[84].

(그림3-7)과 같이 센서 노드 A가 센서노드 C에게 packet A, B, C, D를 보내고자 할 때 악의적인 센서 노드 D는 packet B, D를 받았지만 packet D만 보내고 packet B는 보내지 않는다. 결국 센서 노드 C는 packet B를 받지 못하고 packet A, C, D만 가지게 된다. 즉 실제 받아야 하는 양보다 적은 양의 정보를 받게 된 것이다.



(그림 3-7) Neglect and greed 공격

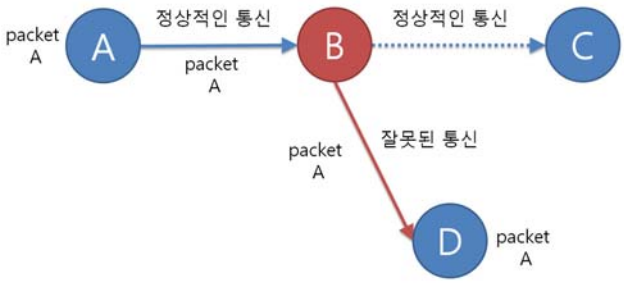
(나) Homing

Homing은 자동적으로 표적을 따라 가도록 만들어진 미사일의 유도 방식으로, USN 환경에서는 중요한 데이터를 가지고 있는 노드를 찾아내어 이 노드로 전송되는 패킷의 내용을 가로채는 공격을 뜻한다.

(다) Misdirection

Misdirection은 전송되는 패킷을 공격자가 중간에 가로채어 목적지가 아닌 다른 곳으로 포워딩(Forwarding)하여 데이터 전송을 방해하는 공격이다[84].

아래 (그림 3-8)과 같이 센서노드 A가 센서 노드 C에게 packet을 전송하고자 한다. 하지만 센서 노드 B가 Packet A를 중간에 가로채어 센서 노드 C에게 보내는 것이 아니라 임의의 다른 센서 노드 D에게 보낸다.

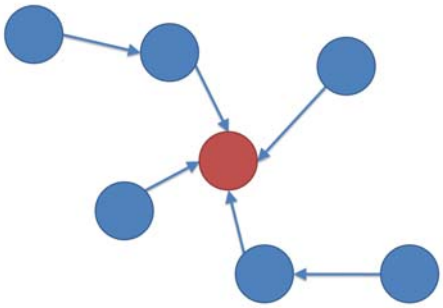


(그림 3-8) Misdirection 공격

이와 같이 Misdirection 공격은 네트워크의 정보를 외부로 유출 시킬 수 있고, 한 노드에 데이터를 집중적으로 보내 특정 노드의 활동을 방해 할 수 있다.

(라) Black holes

Black holes는 라우팅 정보를 조작하여 모든 노드로부터 패킷을 받고, 전송받은 패킷을 다른 노드로 포워딩(Forwarding)하지 않는 공격이다[84]. 공격 노드는 자신이 베이스 스테이션(Base Station)인 것처럼 모든 노드에게 신호를 보낸다. 이렇게 함으로써 다른 노드들로부터 패킷을 수집하여 또 다른 노드에게 포워딩 하지 않는다.

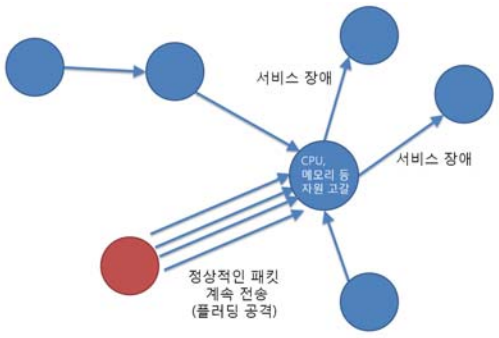


(그림 3-9) Black holes 공격

(4) 전송 계층(Transport Layer)

(가) Flooding

통신 규약을 이용한 공격으로 계속된 패킷 전송으로 해당 노드를 마비시키는 공격인 플러딩(Flooding) 공격은 정상 패킷과 동일한 패킷을 무작위로 전송하여 해당 센서 노드의 CPU, 메모리 등을 고갈 시키고 네트워크의 병목을 야기 시켜 정상적인 서비스 제공을 받지 못하도록 방해하는 공격이다.



(그림 3-10) Flooding 공격

(나) Desynchronization

Desynchronization은 두 노드 사이의 동기화를 방해하여 연결을 막는다.

다. 서비스 거부 공격 대응 기법

(1) 일반적인 서비스거부 공격 대응 기법

이러한 공격을 방어하는 표준 중 하나는 스펙트럼 확산 통신(spread-spectrum communication)이다. 하지만 이는 암호학적으로 안전하기는 하나 상용 가능한 것은 아니며, 공격자가 노드를 직접 포획하여 암호학적인

키를 얻어낼 경우에는 안전하지 않다.

스펙트럼 확산 통신 이외에 센서 네트워크의 속성으로 인해 새로운 방어가 가능하다. 전파 방해가 단지 네트워크의 어떤 한 부분에만 영향을 미칠 경우, 전파 방해에 저항력이 있는 네트워크는 전파 방해와 영향 받은 지역을 탐지하여 그 지역의 주변을 라우팅 함으로써 방어가 가능하다[7].

또한 DoS 공격을 막기 위해서 센서 노드가 공격에 대해서 충분히 견딜 수 있도록 공격 트래픽을 분산시켜, 네트워크 설계 시 정상적인 데이터 처리와 비정상적인 데이터 처리를 구분할 수 있는 기술이 필요하다. 이렇게 함으로써 자체적인 USN 네트워크 보호뿐만 아니라 DoS 공격의 영향을 줄 수 있는 취약성을 원천적으로 차단하여 USN 네트워크를 지키는 방식을 사용한다[80].

결함 감내(Fault tolerance)는 특정 노드들이 USN 네트워크에서 탈퇴하더라도 자동적으로 라우팅 경로가 재설정되는 것을 말한다[75]. 이러한 기능을 제대로 설계하기 위해서 다양한 계층에서 이루어 질 수 있는 서비스거부 공격의 가능성을 고려해야 한다.

다음 [표 3-3]은 Anthony D. Wood et al[84]이 만든 표로, 센서 네트워크에서 일어날 수 있는 서비스 거부 공격과 방어를 네트워크 계층으로 정리한 것이다.

(2) 서비스 거부 공격 방지를 위한 키 관리

DoS는 전파 방해와 같은 공격으로 USN 통신을 제한할 수 있다. 또 다른 유형의 DoS 공격에는 센서 노드의 에너지를 고갈시키는 방법도 있다. 이러한 공격으로 인해 노드는 정당한 서비스를 받을 수 없게 된다. DoS 공격에 대응하기 위해서는 센서 노드의 에너지를 적게 사용하는 LEAP 프로토콜을 이용하는 방법이 있다. 또한 네트워크상에서 트래픽을 많이 발생 시켜 센서 노드 같은 통신이나 서비스를 방해 하는 공격에 대한 방어 기법으로 Multi-path 기법을 이용 할 수 있다. 이 기법을 사용하여 네트워크상이나 센서 노드에 몰려드는 트래픽을 분산 시킬 수 있다.

[표 3-3] 센서 네트워크 계층과 DoS 공격 기법[6]

네트워크 계층	공격	방어
물리적	Jamming	Spread-spectrum, Priority messages, Lower duty cycle, Region mapping, Mode change
	Tampering	Tamper-proofing, Hiding
링크	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
네트워크와 라우팅	Neglect and greed	Redundancy, Probing
	Homing	Encryption
	Misdirection	Egress filtering, Authorization, Monitoring
	Black holes	Authorization, Monitoring, Redundancy
전송	Flooding	Client puzzles
	Desynchronization	Authentication

4. 라우팅 공격(Routing Attack)

가. 라우팅 공격 개요

라우팅(Routing)이란 네트워크에서 데이터를 전송할 경로를 선택하는 과정으로 소스 노드로부터 최종 목적지 노드까지 데이터가 전송되는 경로를 관리한다.[85] USN에서 라우팅 공격은 메시지가 정상적인 경로를 거쳐 싱크 노드로 전달되는 과정을 방해하는 것을 말한다. 공격자는 라우팅 공격을 이용하여 서비스가 정상적으로 이루어지지 않도록 할 수 있으며 또한 다른 공격을 시도하기 위한 준비 단계로 라우팅 공격을 이용할 수 있다[6].

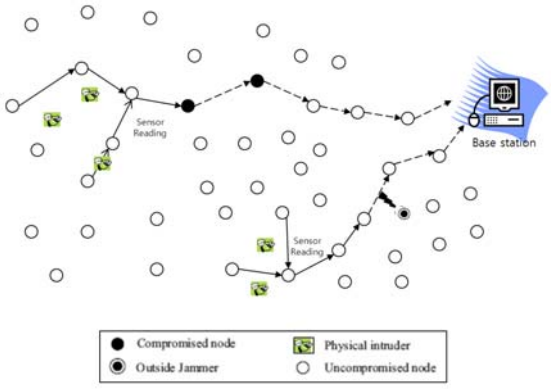
이를 방지하기 위해 USN은 적절한 라우팅 기법을 제공해야 한다. 일반적인 라우팅 기법들은 보안보다는 센서 노드들이 센싱 된 데이터를 얼마나 효율적으로 보내는지에 중점을 두고 있기 때문에 다양한 종류의 라우팅 공격에 취약하다. 라우팅 공격에 대항하기 위해서는 우선 공격자가 네트워크에 접근하는 것을 차단하고, 비정상적인 라우팅 정보를 감지하여 공격자를 찾아서 차단해야 한다.

나. 라우팅 공격 종류 및 기법

라우팅은 외부 공격과 내부 손상 노드로 인한 공격을 받을 수 있다.

라우팅 공격의 종류에는 선택적 포워딩(Selective Forwarding)공격, 라우팅 정보의 위변조 공격, 싱크홀(Sinkhole)/웜홀(Wormhole) 공격, Hello Flood공격, Sybil 공격, ACK 조작 공격 등 다양한 공격이 있다.[39]

(1) 선택적 포워딩(Selective Forwarding)



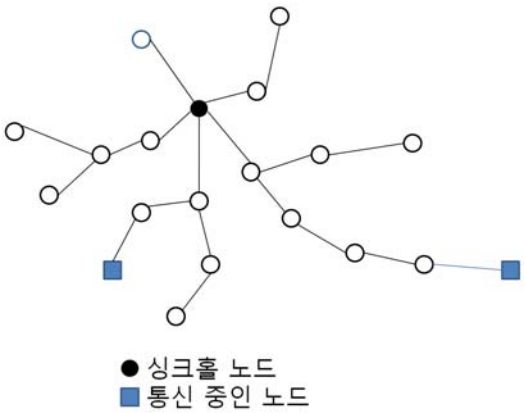
(그림 3-11) Selective Forwarding

선택적 포워딩(Selective Forwarding)은 (그림 3-11)처럼 공격자가 네트워크의 센서 노드를 직접 포획하여 이 노드를 거쳐 전송되는 데이터에 대한 전달을 거부 혹은 데이터를 중간에서 가로채거나 삭제하는 공격을 말한다[86].

(2) 라우팅 정보의 위변조 공격

USN네트워크에서는 노드들 간에 무선으로 통신하기 때문에 공격자가 네트워크에 참여하기 위한 물리적인 제약이 없다. 따라서 공격자가 라우팅 정보를 위변조 하는 것이 상대적으로 쉽다. 위변조 공격은 센서 노드들 사이에 전달되는 데이터를 직접 공격하는 기법으로 공격자가 네트워크 외부에서 무선 장비를 이용하여 센서 노드들 사이에 전달되는 데이터를 위변조 하는 공격을 말한다.

(3) 싱크홀(Sinkhole) 공격



(그림 3-12) Sinkhole 공격

싱크홀(Sinkhole)공격은 Selective Attack과 같이 사용하여 라우팅 정보를 변경한다. 이 때 변경한 정보를 이용하여 공격자가 포획한 노드를 네트워크의 중심에 배치시켜 센서 노드들이 이 노드를 지나가도록 유도하고 특정 지역 내의 모든 통신 트래픽을 자신이 심어놓은 노드로 유도하는 공격을 말한다[87]. 싱크홀 공격은 자신이 베이스 스테이션(base station)과 같은 중요한 노드 또는 목적지 노드로 향하는 가장 효율적인 경로인 것처럼 위장하기 때문에 하나

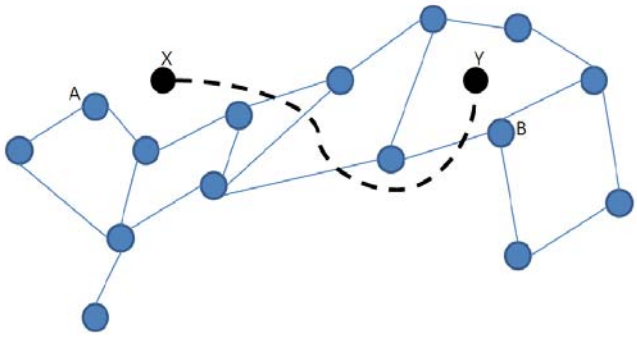
의 싱크홀 노드가 존재하는 것만으로도 네트워크에 큰 악영향을 미칠 수 있다 [87].

(그림 3-12)는 싱크홀 공격이 발생했을 경우의 네트워크 상태를 나타낸 그림이다. 주변 노드의 데이터 전송 경로가 싱크홀 노드를 거치기 때문에 싱크홀 노드가 다른 공격들을 수행할 경우 더욱 넓은 범위의 노드들이 공격에 노출이 된다.

(4) 웜홀(Wormholes) 공격

웜홀(Wormholes) 공격은 공격자가 자신의 노드들을 터널과 같은 특정 장치를 이용하여 연결하여 다른 노드들이 자신의 위치를 혼돈하게 만드는 공격이다. 실제로는 존재하지 않는 노드의 연결이 있는 것처럼 인식하여 도청이나 선택적 포워딩(Selective forwarding)에 활용이 되기도 한다.

(그림 3-13)은 기본적인 웜홀(Wormhole)을 나타낸 그림이다.



(그림 3-13) 기본적인 Wormhole 공격

A가 B에게 데이터를 보내려고 할 때 A로부터 데이터를 받은 X는 데이터를 X와 Y 사이에 형성된 웜홀 터널을 통하여 Y로 보내게 된다. Y는 데이터를 받아서 B에게 전송한다. 웜홀이 없을 경우에는 A와 B사이의 정상적인 경로를 따라 여러 홉을 거쳐 데이터가 이동이 되어야 하지만 이 경우에는 웜홀을 통해 데이터가 빠른 속도로 전송된다. 따라서 공격자가 네트워크의 매우 위협적

인 위치에 웜홀을 생성하고 이를 악용할 경우 경로 설정 과정에서 웜홀이 경로에 포함되게 하거나 포착되기 어렵게 특정 메시지를 선택적으로 차단하거나 변경이 가능하다[88].

(5) Hello Flood 공격

센서 노드들은 자신을 알리기 위한 기법으로 HELLO 패킷을 브로드캐스팅한다. 패킷을 받은 노드는 이를 이용하여 이웃 노드의 리스트를 얻을 수 있다. Hello Flood 공격은 경로 설정 단계에서 한 노드의 이웃에 위치하고 있는 것처럼 위장하여 강한 강도의 신호로 HELLO 패킷을 전송한다. 이렇게 함으로써 일반 노드들의 경로 설정 시 공격 노드가 라우팅에 참여하는 방식의 공격을 시도한다.

이 공격은 이웃 노드뿐만 아니라 원거리에 있는 일반 노드들의 이웃 노드로 설정되어 불필요한 라우팅 테이블의 크기를 증가시킬 수 있을 뿐만 아니라 일반 노드들이 경로를 재설정하기 이전까지 센서 노드들의 라우팅의 혼란을 일으킬 수 있다. 또한 이웃 노드로 가장하여 공격 노드로 전달되는 패킷을 삭제하거나 변조함으로써 불필요한 패킷을 발생시킬 수 있다.

(6) Sybil 공격

공격자가 센서 노드를 포획하여 얻은 정보를 바탕으로 네트워크 내의 다른 노드들에게 많은 수의 노드 ID를 노출시켜 주변에 여러 센서 노드가 있는 것처럼 가장하는 공격으로 Geographic routing에 치명적인 공격이다.

공격자 노드가 ID를 생성하는 방식은 크게 두 가지로 나눌 수 있다. 하나는 ID를 단순히 만들어 사용하는 것이고 다른 하나는 정상 노드의 ID를 가져와서 사용하는 것이다. Sybil 공격으로 정상적인 노드가 공격 노드인 것처럼 혹은 그 반대를 유도할 수 있으며 다른 경로로 라우팅 되어야 하는 일반 경로의 정보를 여러 ID를 통해 공격 노드를 거치도록 유도할 수 있다.

다. 라우팅 공격 대응 기법

(1) 일반적인 라우팅 공격 대응 기법

센서 네트워크에 대한 공격은 외부공격(Outsider attack)과 내부 공격(Insider Attack)으로 나눌 수 있다. 라우팅에 대한 외부 공격은 링크 계층에서의 암호화 및 인증 기법을 이용하면 막을 수 있다. 공격자는 정당한 방법으로 네트워크 토폴로지에 참여하여 라우팅에 관여하는 것이 불가능하므로 라우팅 정보의 조작, 선택적 메시지 전달(Selective Forwarding), Sybil Attack, 싱크홀(Sinkhole) 공격 등은 불가능하다. 그러나 링크 계층 보안 기법으로 웜홀(Wormhole)이나 Hello Flooding을 막는 것은 어렵다.

노드들사이의 상호 협력을 기반으로 하는 라우팅에서 문제가 되는 것은 공격자에 의해 포획된 노드나 이기적인 노드를 포함한 비정상적인 노드들이다. 암호기술을 이용한 보안만으로는 모든 공격을 막는 것은 어려우므로 비정상적인 노드들을 감지하여 라우팅 경로에서 배재시키거나 불이익을 당하게 하는 방안을 연구해야 한다[71].

(가) 선택적 포워딩(Selective Forwarding) 공격 대응 기법

선택적 포워딩(Selective Forwarding) 공격은 선택적으로 특정 정보의 전송을 차단하는 공격으로 이를 막기 위해서는 다중 경로 라우팅(Multi Path routing)을 적용하는 기법이 있다. 다중 경로 라우팅은 메시지를 분할해서 전송하고 목적지 센서 노드에서 이를 다시 취합해 중간 경로에 대한 도청을 차단하는 기법을 말한다. 노드들이 동적으로 패킷을 전송할 다음 Hop을 확률적으로 선택함으로써 공격자가 데이터의 흐름을 제어하는 위험을 줄일 수 있다[39].

(나) 라우팅 정보 위변조 공격 대응 기법

데이터 위변조 공격에 대처하기 위해서는 기본적으로 공격자가 아닌 정상 노드만이 네트워크에 참여할 수 있는 기법을 제공함과 함께 특정 노드로부터의 메시지가 그 노드로부터 변조되지 않은 채 전달되었음을 확인할 수 있는 메시지 인증 기법이 필요하다.

(다) 싱크홀(Sinkhole) 공격 대응 기법

싱크홀(Sinkhole) 공격은 사전에 막기는 힘들기 때문에 현재 공격이 일어나고 있는 지점을 확인한 후 공격에 방어하는 기법을 사용한다. 공격 지점을 확인하기 위해서 베이스 스테이션은 네트워크의 트래픽을 분석하는데 이를 위해 공격 패턴을 분석하고 공격지점을 확인하는 기법이 필요하다. 또한 다수의 노드가 상호 협조하여 싱크홀 공격을 수행하는 경우에 대한 감지도 필요하다.

(라) 웜홀(Wormholes) 공격 대응 기법

웜홀(Wormholes) 공격과 싱크홀(Sinkhole) 공격은 기존의 기밀성이나 무결성 또는 인증 기능을 제공하는 기법으로는 막을 수 없다. 이 경우 가장 효율적인 기법은 라우팅 프로토콜 자체가 공격을 당하더라도 견고하게 유지할 수 있게 만드는 기법과 공격이 일어난 이후에 공격사실을 확인하는 기법이 있다.

웜홀 공격은 네트워크에 있는 드러나지 않는 사적인 채널을 통해 통신하기 때문에 감지하기 어렵다. 이를 위해 웜홀을 탐지하는 다양한 기법이 연구되었다. 예를 들면 네트워크에 중앙 인증기관을 두어 각 노드들의 위치 정보를 기반으로 하여 라우팅이 끝난 후 선택된 경로에 대한 정당성 여부를 판단 한다. 이때 노드들 사이의 거리 중 이상이 발견되면 그 경로 상에 웜홀이 있는 것으로 간주하고 웜홀을 탐지하는 기법이 있다[88].

(마) Hello Flood 공격 대응 기법

Hello Flood 공격도 Sybil 공격 대응 기법처럼 키 프로토콜을 공유하는 방식을 이용하여 양방향 링크의 인증을 받는 기법이 있다.

Leap 프로토콜에서는 Hello Flood공격을 막기 위해 어떤 노드는 Hello 메시지를 브로드캐스팅하고 이웃 노드에게 응답이 오기를 기다린다. Mac에 의해 인증된 이웃 노드로부터 오는 응답 값을 통해 Hello 메시지를 보낸 노드는 응답 신호를 신뢰할 수 있게 된다.

Hello Flood 공격을 막는 또 다른 기법은 TTP(Trusted Third Party)를 이용하는 기법이다. 어떤 두 개의 센서 노드 x와 y가 서로의 인증을 위해 TTP를 이용하는데 각 센서노드는 멀리 떨어져 있는 베이스 스테이션과 유일한 대칭키를 공유한다. x와 y는 각자의 ID를 검증할 수 있고 베이스 스테이션으로부터 공유키를 얻을 수 있다.

(바) Sybil 공격 대응 기법

Sybil공격은 공격 노드가 노드의 주변 노드들인 것처럼 위장하여 행동하면서 발생한다. 이 공격을 막기 위해서는 ID 인증을 해야 한다. 센서 노드들은 베이스 스테이션(Base Station)과 대칭키를 공유한다. 노드들은 이 키를 사용하여 암호화된 키를 생성함으로써 인증을 할 수 있다. 또한 노드들이 가질 수 있는 이웃 노드의 수를 제한하는 기법을 통해 너무 많은 링크가 생기는 것을 막음으로써 Sybil 공격에 대응할 수 있다. 이럴 경우 공격자에 의해 메시지가 수정되거나 도청 당하는 것을 막을 수는 있지만 웜홀(Wormhole)공격을 받을 수도 있는 문제점이 있다.

(2) 라우팅 공격 방지를 위한 키 관리

센서 네트워크의 라우팅은 기존의 유선 라우팅 프로토콜에 비해 도청, 위장 공격과 같은 능동적인 공격에 쉽게 노출된다. 따라서 센서 네트워크가 가지는

센서 노드, 전송 메커니즘, 센서 OS, 응용 서비스의 제원들을 파악하여 개발 초기단계부터 보안 기능을 고려하여 키 관리 기법을 이용하여 공격에 대응해야 한다. 따라서 라우팅 공격에 대응하기 위해서는 Multi path를 이용하여 한 노드가 공격을 당하더라도 전체 네트워크에 영향을 적게 미치도록 하는 방법이 있다. 그리고 q-합성수 역시 노드가 공격당해서 라우팅 정보가 노출 되더라도 전제 네트워크에 미치는 영향을 적게 하는 방법이다.

5. 물리적 공격(Physical Attack)

가. 물리적 공격 개요

물리적 공격(Physical Attack)은 센서 노드에 물리적인 손상을 입히거나 노드를 파괴하여 네트워크 내부의 일부 노드가 동작하지 못하도록 만드는 공격을 말한다. USN에서의 센서 네트워크는 외부에 설치되어 환경 정보를 센싱하여 이를 처리하는 목적으로 많이 사용되기 때문에 외부로부터의 물리적인 공격을 받기 쉽다.

하지만 일반적으로 USN 네트워크에서는 노드의 유실, 전력 소진 등 다양한 이유로 특정 노드의 사용이 불가능할 경우 라우팅 경로를 재설정할 수 있는 결함 감내 기능을 포함하기 때문에 물리적인 공격은 네트워크에 치명적인 영향을 끼치지 않는다.

그러나 센서 노드를 탈취하여 노드가 가지고 있는 중요한 정보를 획득할 경우에는 심각한 위협이 될 수도 있다. 또한 하나의 노드를 획득하는 것만으로도 전체 네트워크를 도청할 수 있으며 공격용 코드를 삽입하여 내부자 공격에 이용할 수도 있다[6].

센서 네트워크에서의 물리적인 공격으로는 노드에 물리적인 손상을 입히거나 노드를 절취하는 등의 공격이 있다. 이럴 경우 전류 센서 등을 사용하여 노드가 공격을 당했음을 확인하고 이에 대응할 필요가 있다.

또 다른 물리적 공격으로는 부채널공격이 있다. 부채널공격이란 노드가 동작하고 있을 때 사용하는 전력 혹은 반사하는 전자파 정보 등을 이용하여 노

드 내부에 있는 암호키와 같은 중요한 정보를 알아내는 공격이다. 부채널 공격의 종류로는 단순 전력분석(SPA, Simple Power Analysis) 및 차분전력분석(DPA, Differential Power Analysis), EM(Electro-Magnetic)등이 있다.

나. 물리적 공격 종류 및 기법

(1) 부채널 공격 기법

부채널 공격이란 RFID 태그나 센서 노드에서 소비되는 소비 전력 혹은 발산 되는 전자파 특성을 분석하여, 태그 내부와 센서 노드에서 중요한 정보를 분석하거나 추출하는 기술로서, 매우 강력한 보안 공격 기술이다.

부채널 공격법은 표본 자료의 분석 과정에서 사용된 기법에 따라 단순 부채널 공격법 (SSCA : Simple Side Channel Attack) 과 차분 부채널 공격법 (DSCA : Differential Side Channel Attacks) 으로 나눌 수 있다[89].

단순 부채널 공격법 SSCA는 연산과정에서 발생하는 추정 정보를 이용하여 비밀 정보를 유추하는 기법이며, 차분 부채널 공격법 DSCA는 연산 결과와 연산 과정에서 발생하는 부채널 정보의 상관성을 이용하여 비밀 정보를 알아내는 기법이다.

다. 물리적 공격 대응 기법

(1) 일반적인 물리적 공격 대응 기법

(가) 부채널 공격 대응 기법

부채널 공격의 대응 기법 중 일반적인 기법은 Goubin에 의해 제안되었다[8]. Goubin이 제안한 기법 중 가장 효과적인 기법은 알고리즘을 수정하는 대응 법으로 자료나 키가 사용될 때 마다 다른 값을 갖도록 사용되는 암호의 알고리즘을 수정하는 기법이다. 이 밖에도 무작위성 기법과 블라인딩 기법, 마스킹 기법 등 다양한 공격 대응 기법이 있다. 무작위성 기법은 다양한 부채널을 통해 누출될 수

있는 자료를 임의로 많은 양을 만드는 것이다. 공격자는 난수성을 띤 정보만을 얻을 수 있기 때문에 연산 과정 중 포함된 초기 값이나 중간 값을 알 수 없다. 블라인딩 기법은 입력 a에 대해 수학적 함수 f를 이용하여 b를 얻을 때 a와 b를 모르면서 값을 연산하는 암호 기법을 말한다. 마스킹 기법은 알고리즘의 연산 과정 중에 나타난 중간 값을 감추는 것을 의미한다.

또한 DPA는 샘플데이터에 대한 전력 소비 곡선에서 나타나는 통계적인 특성을 이용하여 이루어진다. 따라서 이를 막기 위해서는 비밀 키에 의존하는 전력의 소비량을 통계적으로 나타나지 않게 해야 하며 이를 위해서 알고리즘의 과정을 마스킹 기법에 의해 랜덤 화하여 연산을 수행하는 방법이 있다.

(나) 물리적 공격 방어를 위한 키 관리

물리적 공격에는 자연 재해 또는 인위적으로 센서 노드에 물리적 손상을 입히는 공격과 부채널 공격이 대표적이다. 하지만 센서 노드를 탈취하거나 손상을 입히는 공격은 키 관리를 이용해서 대응하기는 어렵다. 또한 센서 노드의 전파를 이용하여 노드 내부에 있는 암호키와 같은 중요한 정보를 알아내는 부채널 공격의 경우 키 관리 기법을 이용하여 원천적으로 방어를 하는 것은 어렵다. 따라서 공격자가 부채널 공격을 이용하여 노드가 가진 중요한 정보를 수신한다 하더라도 그 정보의 내용을 정확하게 알지 못하도록 암호화하는 방법을 이용하는 것이 적절하다. 이러한 방법에는 Master key를 이용하여 하나의 키를 이용하여 전체 네트워크의 통신 채널을 보호하고 단일키를 주기적으로 교체하여 부채널 공격을 당하더라도 단일키를 알지 못하면 정보의 내용을 알 수 없게 하는 방법을 사용할 수 있다[94].

제 2 절 USN 보안 기술

USN 네트워크는 수 만대의 컴퓨터가 서로 연결되어있는 기존의 네트워크

와는 달리 위험에 노출된 환경, 동적인 네트워크 토폴로지, 무선 통신의 취약성, 노드 포획의 위험성, 제한된 자원 등으로 인해 보안에 있어서 취약한 면을 가지고 있다. 따라서 USN 환경에서는 기존의 네트워크에서 적용되었던 보안 정책들을 그대로 적용하기에는 어려움이 따른다[74].

본 절에서는 USN의 정보 보호 요구사항을 바탕으로 한 USN 보안 기술에 대해 기술하고자 한다. USN 네트워크에서 사용하는 보안 기술에는 센서 네트워크에서의 키 관리 기술 및 인증 기술을 비롯하여 물리적 공격과 라우팅 공격을 방지하는 기술, DoS 방지 기술, 프라이버시 보호 기술 등이 있다.

1. 키 관리 기술

키 관리 기술은 자원의 제약성 등으로 인해 센서 네트워크의 보안에서 가장 어려운 부분이라고 할 수 있다. 키 관리 프로토콜은 신뢰할 수 있는 어떤 기관이 없는 상태에서 임의로 설치된 센서 노드들 사이에 신뢰 관계를 형성하여 안전한 통신 구조를 구축해야 한다. 또한 이후의 다양한 보안 프로토콜에서 비밀 키 생성해 주기도 한다. 키 분배를 위해서는 각 센서들이 어떤 형태로든 비밀 정보를 가지고 있어야 하며 설치 후에는 이 정보를 이용하여 센서 노드들 간의 상대적인 위치를 파악한 후 키 분배 및 통신을 위한 설정을 하게 된다.

센서 노드의 제한된 자원 능력으로 인해 PKI 등의 기존의 키 관리 기술을 적용하기가 어렵기 때문에 현재 SPINS(Security Protocols for Sensor Networks) 프로토콜을 이용하거나 Key infection, Network-wide shared Key, 베이스 스테이션 노드 pairwise 키(Base station-node pairwise key), 랜덤 키 분배(Random Key distribution), 랜덤 pairwise 키(Random Pairwise key) 등 센서 네트워크에 적합한 키 관리 기술에 대한 연구가 진행되고 있다[71].

키 관리를 위해 보통 다음과 같은 가정을 한다. 이와 같은 가정은 본 보고서의 키 관리 기법에만 국한 된 것은 아니며 보통 많은 암호 프로토콜에서도 사용한다.

o 공격자는 키를 통해 교환되는 모든 메시지를 도청할 수 있다.
o 공격자는 키의 진행을 방해할 수 있다. 특히, 메시지를 변경, 삽입, 차단할 수 있으며, 다른 목적지로 전달 할 수 있다.
o 공격자는 키에 정상적으로 참여할 수 있는 사용자일 수 있으며, 제3자일 수도 있다.
o 오래된 세션 키는 공격자들에게 노출될 수 있다
o 이상적인 암호알고리즘을 사용한다.

2. 경량 암호 및 인증 기술

센서 노드가 센서 네트워크의 보안 기능들을 수행하기 위해서는 암호 알고리즘을 가지고 있어야 한다. 이 때 센서 노드는 메모리, 통신, 연산, 전력 등 전반적으로 매우 제한된 자원을 가지므로 센서 네트워크의 자원 제약성에 적합하도록 가능한 메모리를 적게 사용하고 계산양이 적은 암호화 알고리즘이 적용돼야 한다.

센서 노드에서 가장 중요한 자원은 에너지이므로 최대한 전력 소모를 줄여서 센서 노드의 수명을 늘릴 수 있어야 한다. 전력 소모는 연산량과 통신량에 의해 결정되므로 암호 알고리즘을 선택할 때 우선으로 고려되어야 하는 사항 중의 하나이다. 따라서 대부분의 시간을 Sleep 모드에 머물도록 하고 실행 모드에서도 연산량이나 통신량을 최대한 줄일 수 있는 암호 알고리즘이 필요하다.

예를 들어 AES 대칭 암호 알고리즘을 경량으로 구현할 경우 128비트 암/복호화에 20μW 정도의 전력을 소비하면서 수 msec 이내에 구현이 가능하다. 공개키 암호의 경우에는 RSA는 적용하기 어렵지만 타원곡선 암호 알고리즘(ECC)인 경우 저전력을 사용하도록 만들면 센서 노드에서 사용할 수 도 있다[76].

센서 네트워크 장치의 분실 및 도난, 인증되지 않은 액세스 포인트(AP : Access Point) 등을 방지하기 위해서는 인증이 필요하다. 인증은 네트워크에 무단으로 참여하려는 외부자 공격 방식에 대응하는 가장 기본적인 수단이다.

센서 네트워크는 기존의 네트워크와는 달리 네트워크 연결이 일시적이며 지속적이지 않기 때문에 연결에 대한 불확실성으로 인해 적법하지 않은 노드를 적법한 노드로 인증할 수 있는 경우가 발생한다. 따라서 이를 방지하기 위한 인증 기법의 연구가 필요하다. 센서 네트워크 환경에서 인증을 보장하기 위해서는 노드 간 양방향의 인증, 주기적인 키 변경, 무선 구간 키 교환 기법, 장치에 상관없이 사용할 수 있는 노드의 인증 등의 요구사항을 갖추어야 한다. 또한 암호학적으로 안전한 상호 인증을 수행할 경우 인증과 동시에 링크 계층의 보안을 위한 안전한 키를 생성할 수 있는 기법의 적용이 필요하다[73].

3. 물리적 공격 및 부채널 공격 방지 기술

센서 노드는 일반적으로 자원의 제약성이 높기 때문에 물리적인 공격을 방지하는 기술을 구현하기가 어렵다. 이로 인해 센서 노드는 물리적인 보안 취약성이 있다는 전제하에 보안 기술을 개발하는 경우가 많다. 이에 대해 센서 네트워크에서는 노드의 위변조 및 악의적인 센서 노드에 대한 감지 및 제어, 부채널 공격(SPA, DPA, EM 공격 등)을 탐지 및 방지(Tamper-resistance)하는 기술 개발이 필요하다. 또한 센서 노드 개발 시에 Tamper-resistance 기술을 적용하여, 데이터가 위조된 노드에 대한 사후 탐지 기술이 필요하다.[74] 그리고 부채널 장비를 위한 랜덤 마스킹 기법이나 부채널 공격 기술 감래형 암호 알고리즘과 코딩 기술이 필요하다[75].

4. 라우팅 공격 방지 기술

기존의 라우팅 프로토콜은 DoS 공격 및 패킷 손실, 재응답 공격이 용이하여 사용이 부적합하며, 포획된 노드에 의한 라우팅 프로토콜 tampering을 방지하는 경량 대칭키 암호 사용이나 Disjoint path를 통한 라우팅 공격 탐지 등의 보안 기술이 필요하다. 또한 선택적 전달 공격을 막기 위해서는 다른 라우팅 경로를 식별하기 위한 추가적인 기법이 필요하며, Flooding 공격에는 인증 기법이 효과적이다. 이 밖에도 공용키 암호기법과 전자 서명을 이용하는 기법도

있다[77].

5. DoS(Denial of Service) 공격 방지 기술

서비스 거부 공격(Denial of Service : DoS)은 시스템의 정상적인 동작을 방해하는 공격 수법으로 대량의 데이터 패킷을 통신망으로 보내는 방식을 사용한다. 서비스 거부 공격은 그 종류와 기법이 매우 다양하므로 공격 기법에 따라 대응 기법 역시 종류에 따라 다를 수 있다. 서비스 거부 공격이 발생할 경우 센서 노드들은 다른 노드들과의 통신 시 메시지 전달에 실패가 잦을 수 있다. 이럴 경우 센서 노드는 소비 전력의 낭비를 막기 위하여 잠시 sleep 모드로 들어가거나 메시지 송수신 시도를 줄이는 기법 등으로 대응할 수 있다. 서비스 거부 공격에는 다양한 네트워크 공격(Sybil Attack, SinkHole Attack, Hello Flooding)과 H/W failure, S/W 버그 등의 공격이 발생할 수 있다. 또한 물리 계층에서부터 전송 계층까지 다양한 공격이 발생할 수 있기 때문에 센서 네트워크의 자원의 제약성을 고려한 DoS 공격 방지 기술이 필요하다[76].

6. 프라이버시 보호 기술

신기술의 발달로 인해 개인의 정보 공유가 늘어남에 따라 개인 정보 침해 및 분쟁 사례가 증가하고 있다. 정보를 소유하고 있는 자의 개인정보 침해에 대한 인식 증가와 분쟁으로 인해 공공기관의 위기의식도 고조되었다. 이에 따라 공공기관에 대한 사회적 및 법적 책임과 의무를 요구하는 분위기가 증대되고 대응 전략이 필요하게 되었다. 따라서 개인의 프라이버시 보호를 위해 법과 제도, 정책, PET(Privacy Enhancing Technology) 개발을 통한 기술적인 차원의 대응책이 필요하다[76]. PET 기술은 Security service 특성에 FIPs(Fair Information Practice)를 더한 기술로 프라이버시 보장을 목적으로 하고 있다. 보안 기술을 기반으로 하여 FIPs의 기본 원칙의 요구 조건인 인증, 데이터 무결성, 기밀성, 접근 제어, 부인 봉쇄를 만족시키고자 하고 있다. 보안 기술을 이루는 6개 영역에 걸쳐 세부 PET 기술의 연구가 진행 중이다 [78].

제 4 장 USN 보안 기술 표준화 동향 분석

본 장에서는 USN 보안 기술의 표준화에 대해 분석하였다. 1절에는 USN 보안 기술 표준화의 필요성을 알아보고, 2절에는 USN 보안 기술의 현황을 국외와 국내로 알아보았다.

제 1 절 USN 보안 기술 표준화의 필요성

USN 네트워크는 무선 통신 기술을 이용하며, 다수의 센서 노드들로 구성되어 있는 센서 네트워크와 기존 통신망을 통해 센서 네트워크로 수집된 데이터를 전달하는 IP 코어 망으로 구성된다[36]. 따라서 무선 네트워크에서 발생하는 데이터 도청, 데이터 위변조, 프라이버시 침해 등의 다양한 위협을 그대로 받게 된다. 이러한 위협에 대응하기 위해서는 보다 강한 보안기술이 적용 되어야 한다. 또한 다수의 센서 노드로 구성된 USN 네트워크에서는 기존의 유선 네트워크에서 적용되는 보안 기술을 적용하기 어렵기 때문에 대규모 센서 네트워크에서 그 기능을 발휘할 수 있는 보다 효율적인 키 관리 기술을 비롯하여 인증, 프라이버시 보호 등 USN 보안 기술의 표준화가 필요하다.

제 2 절 USN 보안 기술 현황

1. 국외 USN 보안 기술 표준화 동향

국내의 USN 표준화는 USN 기반 기술을 시범 사업으로 활용하면서 기술과 응용서비스 모델의 표준화를 맞춰가고 있고, 해외의 USN 표준화 방향은 기존의 기술로부터 USN으로의 기술로 접근하고 있다.

국제적인 표준화기구는 ITU-T(International Telecommunication Union

Telecommunication Standardization Sector), ISO/IEC JTC 1/SC 6, IETF, IEEE ZigBee Alliance 등이 있으며 각각의 전문 분야에 대한 표준화를 추진하고 있다.[91] 국제적으로 정보 보호 표준화 기구인 ITU-T의 주도하에 SG 17 (정보보호) 연구과제 6(유비쿼터스 보안)에서는 USN을 위한 보안 프레임워크, USN 미들웨어 보안, USN의 안전한 라우팅의 3가지의 USN 보안 권고안을 개발하고 있다.

USN을 위한 보안 프레임 워크는 한국의 제안에 의해 개발되고 있는 권고안으로 보안 위협과 보안 기능 및 구체적인 보안 기술, 보안 요구 사항을 정의하고 있다. 현재 정의되고 있는 내용은 키 관리 기술, 인증된 브로드캐스트 메시지, 안전한 데이터 수집 및 계산, 데이터 Freshness, USN 미들웨어 보안, IP 코어 망 보안 등이다.

USN 미들웨어 보안과 라우팅은 2008년 9월 S G17 회의에서 한국의 제안에 의해 신규 표준화된 아이템으로 현재 개발 중인 권고안이다.

현재 USN 분야에서 주요 현안 사항중의 하나는 용어 정의로 다양한 그룹에 의해 표준화가 진행되고 있다. 글로벌 표준화 기구 간에 용어 정의를 위한 특별위원회가 구성되어 관련 용어를 정의하고 있으며 현재 개발되고 있는 권고안에도 이러한 용어들을 사용할 예정이다[36].

2. 국내 USN 보안 기술 표준화 동향

USN 보안 기술의 표준화는 아직 시작단계라고 할 수 있다. USN 기술에 사용되는 하드웨어 플랫폼이 다양하기 때문에 그 플랫폼에 따른 요구사항 들도 다양하다. 따라서 USN 기술에 적용할 수 있는 표준들이 아직 충분하지 못한 것이 현실이다. 특히 USN 보안 기술은 다양한 방안들이 제안되어 왔으니 실제로는 초보적인 보안 기술만이 적용되고 있다. 현재 국내에서는 USN이 다양한 기술 결합의 결정체인 만큼, 각각의 기술들이 적용되는 비즈니스 플랫폼에 따라 요구하는 프로토콜에 걸맞게 개별적으로 표준을 갖춰가고 있다[92]. 한국정보통신기술협회는 RFID/USN의 표준화를 위해 USN 표준화 포럼을 설치하고 기술, 응용, 네트워크, 정보보호의 4개 분과로 나누어 표준화를 진행 중이

다.

정보보호 분과는 RFID 보안 W/G, USN 보안 W/G의 2개의 W/G로 구성이 되는데 RFID 보안 W/G는 RFID 태그 등 초경량 환경에 적합한 암호 프리미티브(블록암호, 스트림 암호, 해쉬함수)와 RFID 태그/리더 간 상호인증을 위한 경량화된 인증기술, 그리고 RFID 사용자의 개인정보 및 위치정보 프라이버시 침해방지를 위한 기술을 개발하고 국내 표준 제정 및 국제 표준을 제안하고 있다.

USN 보안 W/G는 USN 환경에서의 라우팅 프로토콜 보호 메커니즘을 개발하고 Ad-hoc 네트워크, USN 등에서의 인증을 위한 기술을 마련하여 국내 표준 제정 및 국제표준을 제안하고 있다[90].

현재 대부분의 USN 보안 권고안이 한국에 의해 추진되고 있고, ETRI가 2009년에 RFID/USN 분야 국제 표준화 의장단에 진출했기 때문에 앞으로 우리 기술의 국제 표준 반영이 적극적으로 이루어질 것으로 예상된다[93]. 따라서 향후 국내 산업체의 다양한 의견 제시와 자발적인 관심이 요구되는 바이다.

제 5 장 u-City와 u-City 시범 서비스

본 장에서는 u-City와 국내외u-City 시범 서비스를 조사하여 분석하였다. 1절에서는 u-City의 개념을 설명하고 2절에서는 국내외 u-City 시범 서비스 조사하여 분석 하였다. 3절에는 분석한 u-City 시범 서비스를 센서의 수와 토폴로지에 따라 통계를 냈으며 4절에서 u-City 서비스의 공격과 보안에 대해서 u-City 보안 고려사항과 u-City 시범 서비스 공격 유형 및 키 관리 기법을 설명한다.

제 1 절 u-City

1. u-City 개요

u-도시법 제2조에 따르면 u-City란 도로, 교량, 학교, 병원 등 도시 기반 시설에 첨단 정보 통신 기술을 융합하여 유비쿼터스 기반 시설을 구축하여 교통, 환경, 복지 등 각종 유비쿼터스 서비스를 언제 어디서나 제공하는 도시를 말한다. 이러한 u-City의 구성요소로는 RFID 등이 부착되어 지능화된 도시 시설의 정보생산, BcN, USN 등 통신 인프라를 타고 생산된 정보가 도시 통합센터로 수집되는 정보 수집, 도시 통합 정보 센터에서 통합 정보를 가공하는 정보 가공, U-교통, U-환경, U-방범, U-행정 등의 U-서비스 제공과 같은 정보 활용이 있다.

u-City는 IT기술이 도시계획, 건설, 관리 및 운영에 도입된 종합플랜트 부문이며 더 나아가서는 도시문화와 디자인, 도시의 문제와 정책, 도시재생, Eco city, 도시성장관리등과 밀접한 관련이 있는 새로운 도시의 패러다임을 의미하기도 한다.

u-City는 u-관광, u-헬스, u-시설물 관리 등의 새로운 산업의 추진으로 인하여 국내 연관 산업을 발전시킬 뿐만 아니라 도시기능, 도시 이미지 및 도시의

위상 향상으로 인하여 지자체 브랜드가치 확보로 인하여 경쟁력 향상의 효과도 가져올 수 있다. 또한 U-도시 관리, u-관광, u-문화, u-환경 등의 서비스가 제공되는 유비쿼터스 도시는 주민들의 삶의 질을 향상시킬 것으로 기대된다[107]. u-City는 첨단 정보통신 인프라와 유비쿼터스 정보 서비스를 도시 공간에 접목시켜 도시 생활의 편의 증대와 체계적인 도시 관리에 의한 안전 보장, 주민들의 복지 향상 등의 도시의 제반 기능을 구축하는 차세대 정보화 도시로서 도시 거주민에게는 쾌적한 도시생활을 제공하고 관리자에게는 도시 운영의 편리성을 제공할 것이다. 따라서 국토의 균형 있는 발전과 도시 거주민의 복지뿐만 아니라 국가의 성장 원동력으로서 기여할 것으로 기대되어진다[108].

(그림 5-1) u-City 개념도[107]

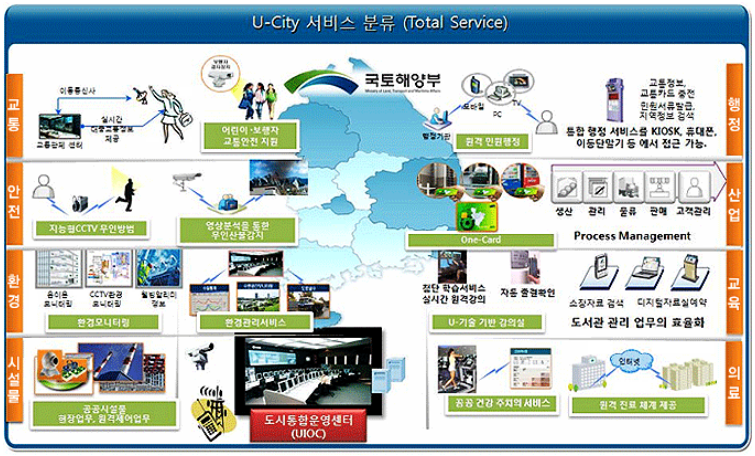
제 2 절 u-City 시범 서비스

1. u-City 시범 서비스 개요

u-City 서비스는 "유비쿼터스 도시의 건설 등에 관한 법률"의 제 2조(2)항에 따르면 유비쿼터스 도시 기반시설 등을 통하여 행정, 교통, 복지, 환경, 방재

등 도시의 주요 기능 별 정보를 수집한 후, 그 정보 또는 이를 서로 연계하여 제공하는 서비스로서 대통령령으로 정하는 서비스를 말한다. 기존의 다양하고 복합적인 도시 문제를 해결할 수 있기 때문에 현대 도시의 문제점으로부터 u-City 서비스를 유도해낼 수 있다.

u-City서비스는 크게 공통기반 서비스와 특화서비스로 구분될 수 있다. 공통기반 서비스는 도시의 기본기능을 수행하기 위해 공통적이고 기본적으로 제공되는 서비스로 u-시설관리, u-방재, u-국방/치안, u-교통, u-행정 등이 해당된다. 특화서비스는 도시 지역의 환경 및 특성에 따른 지역 특화서비스를 말하는데 u-관광, u-항만, u-공항, u-물류/유통 등이 해당된다[109].



(그림 5-2) u-City 분류체계[107]

u-City 서비스는 유비쿼터스 기술을 활용하여 시공간의 제약 없이 제공받을 수 있는 지능화된 정보 또는 콘텐츠의 종합체이다. 개인이나 기업, 정부 등의 도시 활동 주체들은 도시 생활을 영위하기 위해 필요한 문화·관광·스포츠, 물류, 방범·방재, 보건·의료·복지, 시설물관리, 에너지·환경 등에 대한 다양한 u-City 서비스를 받을 수 있다.[110]

이러한 u-City 서비스가 이루어 질 수 있도록 하는 유비쿼터스 도시기술(u-City 기술)은 유비쿼터스 도시 기반 시설을 건설하여 유비쿼터스 도시 서비스를 제공하기 위한 건설・정보통신 융합 기술과 정보통신 기술을 말한다. 이

러한 유비쿼터스 환경에서 u-City 기술은 정보를 인식하고 실행하며 처리하는 일련의 과정에 필요한 센싱(sensing, 정보입력), 네트워킹(정보전달), 프로세싱(processing, 정보처리), 인터페이스(interface, 정보표현), 보안(정보보안)으로 분류된다[120]. 또한 BcN 서비스와 u-City 서비스 제공을 위해 필요한 정보 통신 기술 기반의 설비를 u-City IT 인프라라고 하며, u-City IT 인프라는 기초 인프라, 통신 인프라, 센서망, 정보관리인프라로 구분하여, 그 구성은 아래와 같다[121]. (그림 5-3)는 u-City IT 인프라 개념도를 나타낸 것이다. 기초 인프라로 통신관로/맨홀/공동구와 통신 철탑, 그리고 IT-Pole이 있다. 센서망에는 USN, CCTV, 공통센서접송망이 있고, 통신 인프라는 유무선가입자망, 구내 망이 있다. 하지만 통신 인프라 중 백본망은 도시와 도시를 연결하는 통신망을 말하며, 국가적 관점에서는 중요한 통신 인프라지만 u-City 인프라로는 볼 수 없다. 마지막으로 정보관리 인프라에는 LAN, 서버 등과 같은 하드웨어 플랫폼과 미들웨어, open API와 같은 소프트웨어 플랫폼이 있다.

(그림 5-3) u-City IT 인프라 개념도[121]

[표 5-1]은 u-City 시범 서비스를 구분하여 각각 간단하게 정의를 정리한 것이다.

[표 5-1] u-City 시범 서비스[111]

구 분	서비스 정의
U-홈	주택에 유비쿼터스 기술을 도입하여 집안 기기의 원격 제어, 가스·전기 등의 원격 검침 및 상태모니터링, 생활정보 등을 제공하는 서비스
U-워크, 오피스	다양한 정보통신 기술을 활용해 언제 어디서나 업무를 수행할 수 있는 근로환경을 조성하여 근로자의 편의증진과 업무처리의 효율성을 높이는 서비스
U-교통	도로, 교통, 기반시설, 차량 등 기존 교통 구성요소에 유무선의 통신 구조를 기반으로 유비쿼터스 IT를 접목해 교통인프라의 효율성과 사용자의 안전, 생활 편의성을 증진하는 서비스
U-보건·복지	건강정보를 실시간으로 측정하고 진단 결과에 따른 효율적인 건강관리와 응급 상황 시 개인에 적합한 응급조치 정보를 제공하는 서비스
U-환경	도시의 대기, 수질, 토양 등의 오염 정보를 USN을 이용하여 실시간으로 모니터링 하여 관련 정보를 제공 또는 관리하는 서비스
U-방범·방재	도시의 치안과 방범, 자연재해, 사건·사고 등에 대한 정보를 실시간으로 획득하고 감시, 분석하여 시민 및 관련 치안 기관에게 제공하는 서비스
U-시설관리	도시 지상·지하 시설물을 대상으로 USN을 접목시켜 각 시설물의 이상 여부 및 변화상황을 모니터링 하는 서비스
U-문화·관광	각 지역의 문화와 관광에 관련된 정보를 이용자에게 모바일 단말기 등을 통해 제공하는 서비스
U-물류	RFID등을 활용해 물품 및 이동차량의 이동과정을 실시간으로 모니터링 하여 물류 효율화를 증진시키는 서비스

U-교육	교육환경에 유비쿼터스 기술·서비스를 접목해 교육 콘텐츠를 어디서나 이용할 수 있고, 학사 행정의 편의를 제공하는 서비스
U-비즈니스	상업의 활성화를 위해 지역 상가의 이용정보 및 할인권, 위치안내 등의 정보를 제공하는 서비스를 통한 상품 홍보 및 전자 지불 시스템을 제공하는 서비스
U-행정	공공행정, 민원처리 등의 관련정보를 모바일기기를 통해 제공받아 업무의 효율성과 민원의 만족도를 증대시키는 서비스

2. u-City 시범 서비스 사례

가. 국내 시범 서비스

현재 u-City는 행복도시, 화성, 동탄, 파주 운정 등의 신도시와 서울, 부산 등의 기존도시 20개 이상의 지역에서 벌어지고 있다. 이들 도시 모두 첨단화 뿐만 아니라 각 지역에 특화된 첨단 도시 건설을 목적으로 u-City 시범 서비스가 진행되고 있다.

[표 5-2] u-City가 제공하는 서비스[110]

구 분	제공되는 서비스	사례
U-홈	원격검침, 원격수리, 출입문 자동제어, 홈네트워킹 등	도곡동 '삼성 래미안' u-광주
U-일	재택근무, 원격회의 및 무선 전자상거래 등	원격 영상 협업 서비스 상암 DMC
U교통	교통상황, 교통사고처리, 도로통합관리 및 텔레매틱스 등	u주차관리 서비스

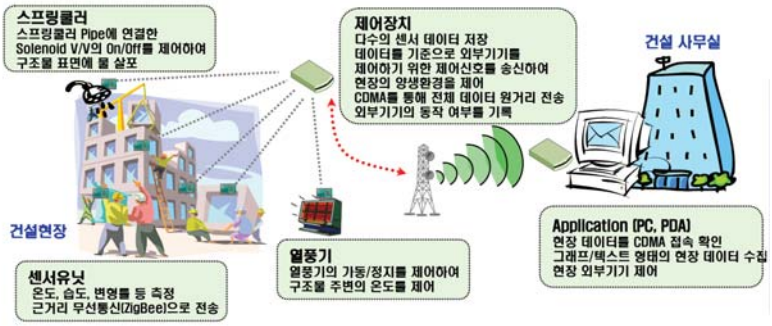
U-건강	헬스 케어, 원격검진, 원격의료/치료 및 응급조치 등	원격진료서비스 USN기반의 혈액 및 항암제 관리 시스템
U-환경	환경관리 및 위생관리 등	파주 운정 '친수 생태도시' IFEZ u-City
U-공공	전자정부, 방범 및 재난관리 등	민원서류 발급 서비스
U-교육	E-Learning, 학교관리 시스템, 등하교 관리시스템 등	연세대, 숙대. 이화여대 등의'u-캠퍼스'

아래는 현재까지 파악된 국내 USN 관련 시범 서비스 중 14개를 상세히 조사하여 이에 대한 정의 및 시범 서비스를 구성하는 방법, 네트워크 토폴로지 등에 대해 정리 하였다. 단, 센서 노드의 이동성이 없는 고정된 환경만을 고려하여 조사 및 정리 한 것이다.

(1) 건설현장의 콘크리트 구조물 양생 이력 관리 시스템

(가) 건설현장의 콘크리트 구조물 양생 이력 관리 시스템 개요

콘크리트 구조물 양생이력 관리 시스템은 현장 구조물에 설치한 USN 센서를 통해 콘크리트 양생 환경을 관리하는 시스템이다. 즉, 건설 현장의 온도, 습도, 변형률 등을 주기적으로 모니터링하고 데이터를 측정하여 수집한다. 이렇게 수집된 데이터는 CDMA 모뎀을 통해서 원거리에 있는 사무실로 전송되고, 사무실에서 현장의 상황을 분석할 수 있으며 스프링클러, 온풍기, 배수기 등을 제어한다. 위의 내용을 (그림 5-4)로 표현하였다.



(그림 5-4) 건설현장의 콘크리트 양생 이력검사를 위한 시스템개념[122]

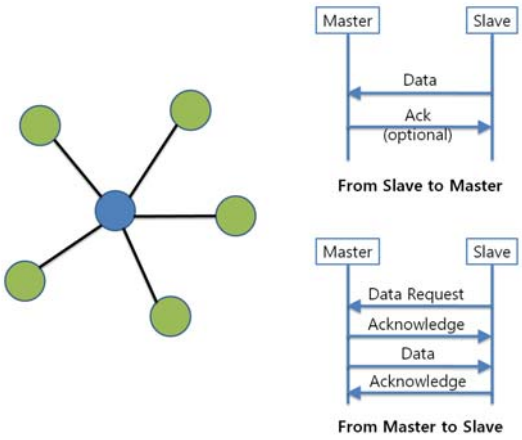
콘크리트 양생 시 온도, 습도, 변형률 정도를 측정한 데이터를 통해 실시간으로 건설 현장 구조물의 양생 환경 파악 및 통제함으로써 최적의 양생조건을 구현한다. 따라서 현장 자동 제어를 통해 구조물의 안전성을 확보하고 최적의 양생환경을 만들며, 장거리에서도 현장의 다양한 환경 변화를 즉각적으로 파악하고 분석하여 현장의 외부기기를 제어하고 모니터링 함으로 최적의 양생환경을 만든다. 그리고 양생 후에도 센서로부터 지속적으로 정보를 측정하여 건물의 노후 상태 등을 모니터링 함으로써 장기적으로 구조물을 안전하게 관리 할 수 있다.

(나) 시범 서비스 구성

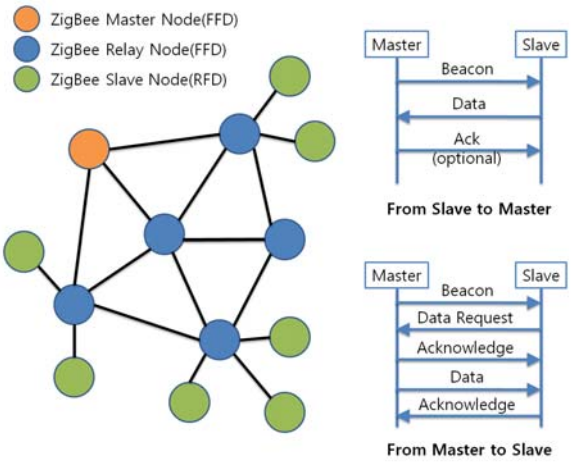
건설 현장의 콘크리트 구조물 양생 이력 관리 시스템은 건설현장의 센서유닛, 제어장치, 외부기기와 사무실의 어플리케이션(PC, PDA)으로 구성되어 있다. 근거리 영역 무선 통신은 ZigBee(RF, Binary-CDMA)방식을 적용하고, 장거리 영역 무선 통신은 CDMA(TDMA, GSM 등) 방식을 적용 한다[122]. (그림 5-5)는 건설 현장에서 실제로 배치된 개발 시스템의 개념도 있다.

(그림 5-5) 개발 시스템 개념도

센서유닛은 콘크리트 양생 할 때 환경정보를 센싱 하여 타설 전에 콘크리트 골격에 설치한다. 그리고 현장 곳곳에 제어장치를 설치하고, 제어장치는 무선으로 센서유닛이 전송하는 데이터를 수신하여 저장한다. 이렇게 저장된 데이터를 분석하여 스프링클러, 열풍기 등의 외부기기를 자동으로 제어한다. 그리고 제어 장치는 수집된 양생이력 데이터를 CDMA 중계기를 통해 사무실의 어플리케이션(Application)으로 전송하여, 사무실에서도 현장의 상황을 원격으로 모니터링 및 제어를 할 수 있다.[124]



(그림 5-6) 스타 네트워크 토폴로지와 데이터 전송 모델l[122]



(그림 5-7) 메시 네트워크 토폴로지와 데이터 전송 모델[122]

건설 현장에 적용 가능한 네트워크 토폴로지는 크게 스타 토폴로지와 메시 토폴로지로 구분할 수 있다. (그림 5-6)과 같이 스타 토폴로지는 마스터 노드가 중심이 되어 주변의 Slave node들과 직접 통신을 하지만 (그림 5-7)과 같이 메시 토폴로지는 Slave node들이 중간에 있는 Relay node를 통해서 마스터 노드와 통신을 한다.

(2) USN 기반의 교량 모니터링 시스템

(가) USN 기반의 교량 모니터링 시스템 개요

USN 기반의 교량 모니터링 시스템은 유비쿼터스 컴퓨팅 개념을 도입하여 실제 교량에 센서노드 등을 설치하고 무선 통신으로 교량의 데이터를 실시간 모니터링 함으로써 교량의 데이터를 수집하는 시스템이다. 이렇게 회득한 정보를 이용하여 교량의 상태를 파악하여 교량 유지보수를 수행한다.

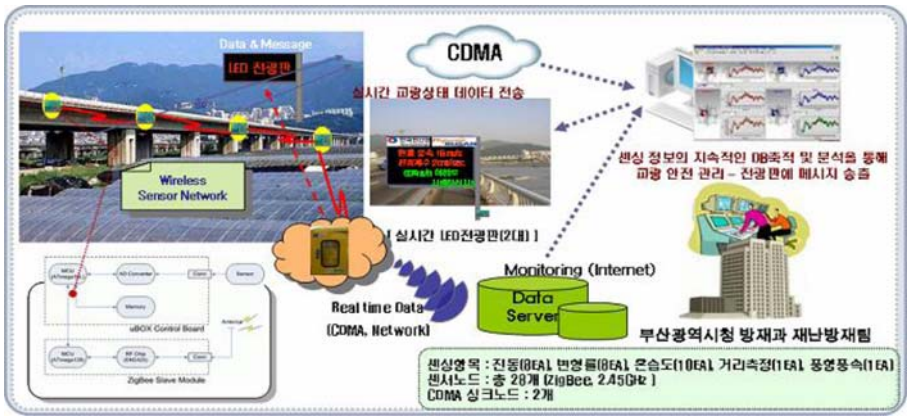
교량 모니터링 시스템의 목적은 교량의 손상을 초기에 파악하여, 교량의 안전성과 이용성을 확보하고, 교량의 유지관리 비용을 최적화한다[123].

교량 모니터링 시스템은 교량에 설치된 센서노드로 데이터를 측정하고 무선

네트워크를 통해 전송한다. 이렇게 확보한 정보를 이용하여 교량 구조를 보안하거나 분석하고, 교량의 수명 측정과 설계 기준에 대한 정보를 얻을 수 있다. 그리고 지속적인 교량의 모니터링을 통하여 교량의 대형 사고를 사전에 예방할 수 있다.

기존의 유선으로 이루어진 교량 관리 시스템과 다르게 USN 기반의 교량 모니터링 시스템은 선이 필요 없는 무선 네트워크를 이용하므로 교량 유지보수 비용을 절감하고 이동성 및 공사기간을 단축 할 수 있으며 센싱 된 데이터를 지속적으로 DB 축적 및 분석을 통행 교량을 안정적으로 관리할 수 있다.

(나) 시범 서비스 구성

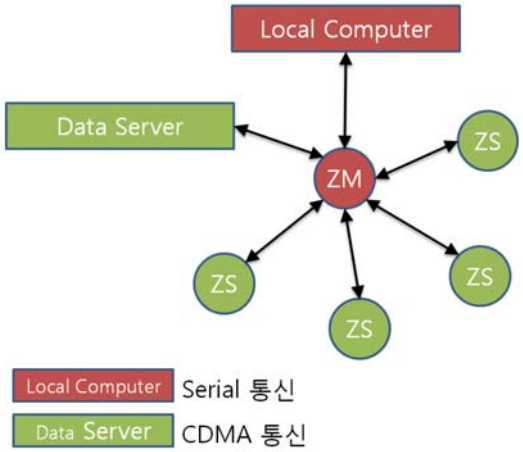


(그림 5-8) USN 기반 교량 모니터링 시스템 개념도 [123]

각각의 센서유닛(Sensor Unit, u-Box)은 각 위치에서 데이터를 측정하여 일정 간격으로 주 제어장치(Main controller, u-Plant)로 전송한다. 주 제어장치는 전송된 데이터를 취합하여 데이터 서버(Data Server)로 전송한다. 데이터 서버와 연결 가능한 S/W Application(PC. PDA 폰)은 데이터 서버에 접속하여 현장의 데이터를 확인하고 데이터를 분석하여 교량의 진행성 거동을 파악한다 [123].

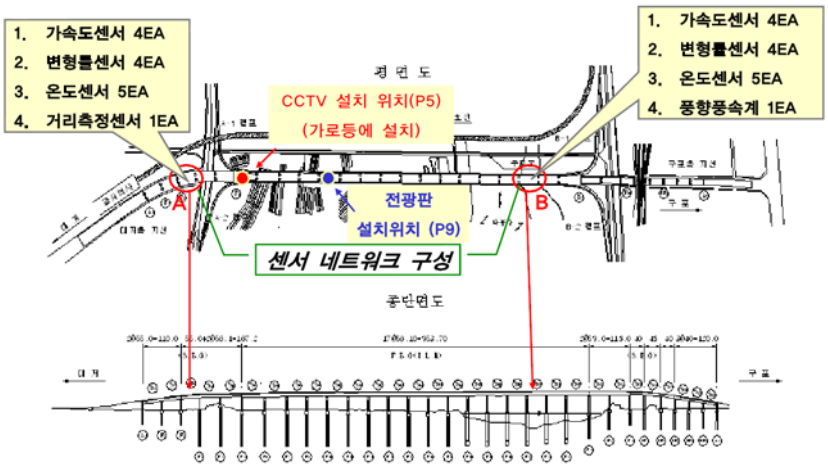
교량모니터링 시스템은 스타 토폴로지의 형태를 가지며, 가속도 센서, 변형

률 센서의 데이터를 60SPS(Samples Per Second)의 속도로 싱크노드로 전송한다. 그리고 최대 50m 이상 통신거리를 유지하며 실시간 데이터의 송수신을 확인한다. 교량 모니터링 시범서비스의 현장 시험에서 데이터 전송 주기는 가속도 센서 60SPS, 변형률 센서 80SPS, 풍향풍속 센서 4SPS, 온도 센서 0.5SPS, 간격측정 센서 1SPS의 간격으로 데이터를 전송하는 것으로 나타났다.



(그림 5-9) 교량모니터링 스타 토폴로지[123]

센서노드(u-Box)는 근거리 무선 네트워크 시스템과 센서와 연결되는 A/D Converter가 연결되어 있는 형태이다. 센서로부터 입력 받은 아날로그 데이터를 A/D Converter를 통해서 싱크노드(u-Plant)에 전송한다. 싱크 노드는 u-Box에서 전송되는 데이터를 집적하고 인지하고 평가하여 제어하는 부분이다. 본 현장시험에 사용한 싱크노드는 다양하게 변화되는 데이터를 저장 및 전송하는 문제점을 극복하기 위해서 H/W에 OS를 탑재한 임베디드 시스템(Embedded System)으로 구현하였다[100]. (그림 5-10)은 현장 시험 모델 중 구포대교의 종평면도를 나타낸 것이다. 이 실험에서 사용된 센서 네트워크를 구성하는 센서는 가속도 센서 4개, 변형률센서 4개, 온도센서 5개, 거리측정센서 1개이다.



(그림 5-10) 현장시험 모델 구포대교 종평면도[100]

부산 구포대교에 설치한 USN 기반의 교량 모니터링 시스템은 구포대교에 온도센서, 변형률 센서, 가속도 센서, 풍향풍속 센서, 거리 측정 센서 등 총 28 Set의 센서 노드를 설치하고 교량의 정보를 실시간으로 모니터링 하게 된다. (그림 5-11)은 좌측의 싱크노드와 우측의 센서노드를 설치한 모습이다.

(그림 5-11) 싱크노드(Sink Node) 센서노드(Sensor Node 우)[126]

(3) 혈액 및 항암제 관리 시스템

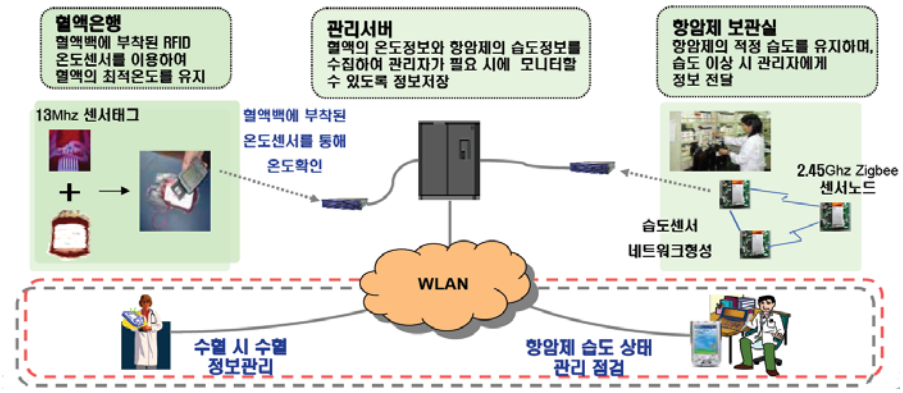
(가) 혈액 및 항암제 관리 시스템 개요

혈액 및 항암제 관리 시스템은 혈액 및 항암제를 효율적이고 안전하게 관리하기 위해 혈액 및 항암제 관리에 USN 기술을 도입한 것이다[124].

이 시스템은 병원의 혈액에 온도센서를 부착하고, 항암제보관실에 습도센서를 설치하여 실시간 모니터링을 통해 온도와 습도를 관리한다.

혈액 관리 및 항암제 관리 시스템은 혈액의 변질 및 오염 가능성을 체크하여 수혈자와 항암제 복용자의 건강을 보호하고, 혈액 및 항암제 보관 과정의 온도와 습도를 체계적으로 관리하여 혈액과 항암제의 검사 신뢰도 및 안정성을 향상시킨다.

또한 혈액 및 항암제 관리 시스템은 잘못된 혈액이 환자에게 공급되거나, 혈액의 온도가 허용된 기준치를 넘어 변질되는 경우와 같은 의료사고를 사전에 방지할 수 있을 뿐만 아니라 혈액과 항암제의 폐기율을 감소시키고 이에 대한 비용을 절감 할 수도 있다.



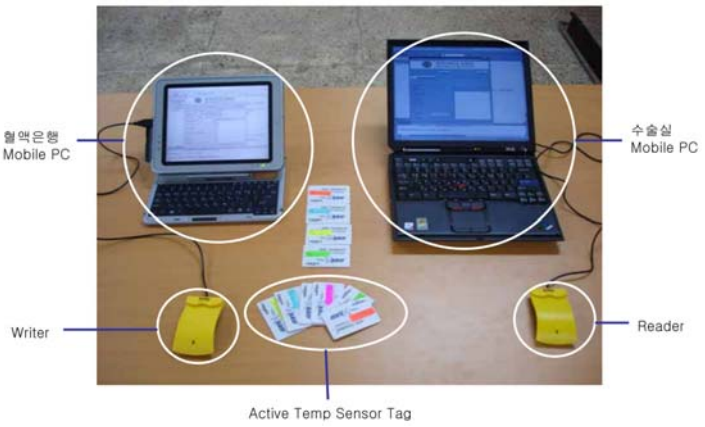
(그림 5-12) 혈액 및 항암제 관리 시스템[128]

(나) 시범 서비스 구성

1) 혈액백 관리

혈액백 보관실과 환자 병동에서 수행하였으며, 적혈구 제제에 적용하여 적정 온도 범위의 이탈 여부를 점검한다.

(그림 5-13)에서 보는 것과 같이 혈액백 온도 센서 현장시험은 혈액은행과 수술실의 Mobile PC 2대와 RFID Interrogator (reader/writer), 온도센서 태그 100개, 혈액냉장고에 설치된 무선 센서 노드10개 등으로 이루어져 있으며, 혈액원과 환자 병동에서 수행되었다.



(그림 5-13) 혈액백 관리 시스템 구성도

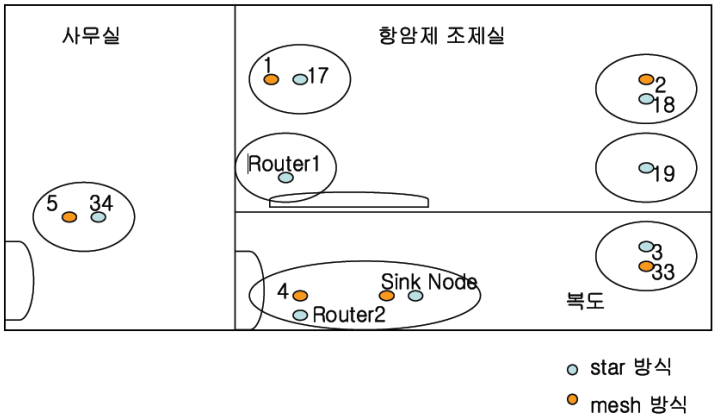
혈액보관 냉장고 온도관리 용 센서 네트워크는 메시 방식을 이루고 있으며 혈액보관 냉장고에 온도 센서 node를 설치하여 혈액보관 냉장고에서 혈액백을 출고하여 온도태그를 부착할 때까지 온도관리의 연속성을 이루었다.

2) 항암제 관리

항암제 습도센서 노드는 항암제 보관실에서 시간대별 센서 노드별 습도 분포를 파악하여 습도를 관리한다. 센서 네트워크의 토폴로지는 라우터를 통해서만 데이터를 싱크 노드(Sink Node)로 보낼 수 있는 스타 네트워크(Star Network) 방식과 라우터 없이 곧바로 데이터를 싱크 노드로 보내는 메시 네트워크(Mesh network) 방식을 혼합하여 시스템을 구성하였다[127]. 항암제 습도 센서 실험은 습도센서 노드 10개와 싱크 노드 2개, Mobile PC 1대 등으로 이루어져 있으며 항암제 조제실에서 시험하였다.

(그림 5-14) 항암제 관리 시스템 구성도[127]

항암제 조제실에 메시 방식과 스타 방식의 습도 센서 노드를 각각 5개씩 설치하고, 각 센서노드들이 전송한 데이터를 싱크 노드를 통해 취합하여 web 서버에 저장한다. PC에서 웹을 통해 그래프 형태로 표현되는 습도변화를 모니터링하고 적정 습도를 벗어났을 경우 담당자에게 핸드폰 문자메시지 및 이메일로 알린다. 다음은 항암제 관리 시스템의 실험 방법 및 실험 절차이다[127]. (항암제시의 제한된 공간에서는 다양한 실험이 불가능하여 넓은 옥외 및 다양한 장소에서 예비 실험을 하였다. 데이터 전송 간격은 5분이다.)



(그림 5-15) 항암제 조제실 센서노드 위치[127]

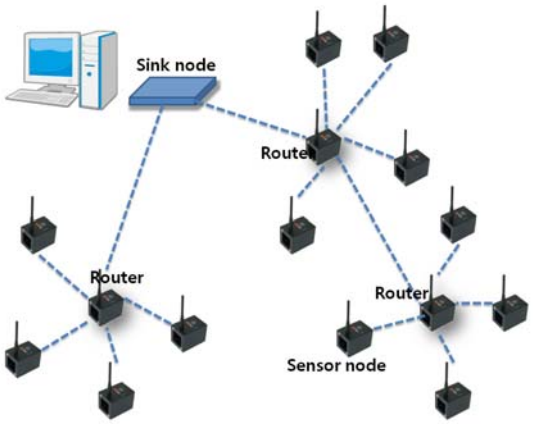
3) 항암제 습도 관리 시스템 구성도

가) 스타 네트워크 방식

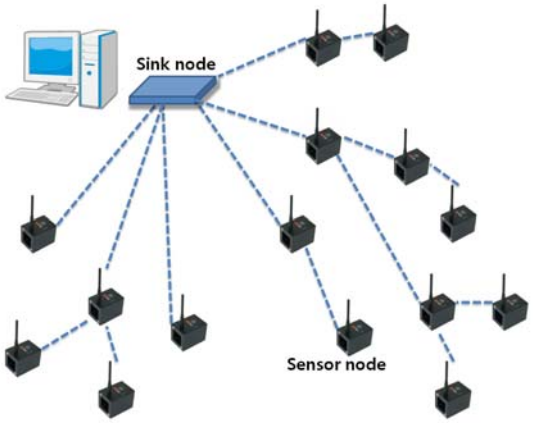
스타 네트워크 방식은 다수의 센서 노드와 라우터, 한 개의 싱크노드와 서버 및 모니터링 시스템 등으로 구성되고, 라우터를 통해서만 싱크노드와 통신을 하며 전력 소모가 적다.

나) 메시 네트워크 방식

메시 네트워크 방식은 다수의 센서 노드와 한 개의 싱크노드, 서버 및 모니터링 시스템 등으로 구성되고, 라우터 없이 곧바로 데이터를 싱크 노드로 보낸다. 이 방식은 멀티 홉 방식으로 중간의 센서 노드가 작동하지 않더라도 다른 센서 노드와 통신하는 유연성을 가진다.



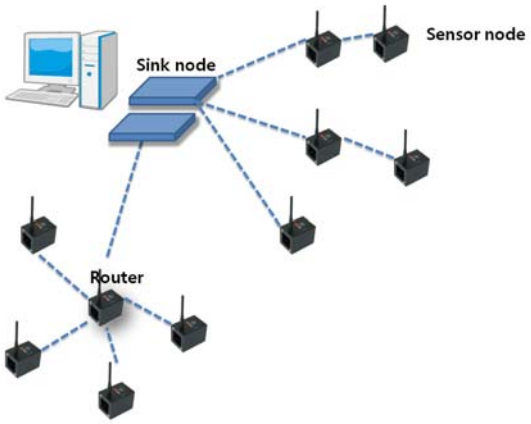
(그림 5-16) 스타 네트워크 방식



(그림 5-17) 메시 네트워크 방식

다) 스타와 메시 네트워크의 혼합 방식

서버에 두 종류의 센서 노드를 연결하였다. 하나는 스타 방식의 네트워크를 구성하였고 다른 하나는 메시 방식의 네트워크를 구성하였다. 즉, 스타 방식과 메시 방식을 혼합하여 연결하였다.



(그림 5-18) 스타와 메시 네트워크 혼합 방식

(4) 홈 네트워크(Home Network)

(가) 홈 네트워크(Home Network) 개요

홈 네트워크란 언제, 어디서, 누구에게나 통신이 가능한 것은 물론 가정 내에 위치한 어떤 기기 간에도 네트워크가 가능하며 사용자가 네트워크를 통해 기기를 제어와 관리가 가능한 통신 서비스 환경을 의미한다. 즉, 가정 내의 정보가전기기들이 모두 네트워크로 연결되어 있고 통신을 통해 공간 제약 없이 가정의 기기들을 제어할 수 있다.

또한 주택이라는 물리적 공간을 전제로 하기 때문에 홈 네트워크는 “주택에 원격제어 기기 등과 같은 정보기기를 설치하고 네트워크로 연결하여 주거성능을 높이는 서비스를 제공하는 설비 및 그 운영체계”로 정의 할 수 있다[129].

홈 네트워크는 개인정보관리, 공공행정, 홈뱅킹, 홈쇼핑 등과 같은 홈 디지털 서비스가 구현된 콘텐츠/솔루션, 위성 혹은 케이블망과 같이 서비스를 전달해주는 방송망, 홈서버, 홈게이트웨이와 같은 홈 네트워크 시스템이 구축되어 있어야 한다.

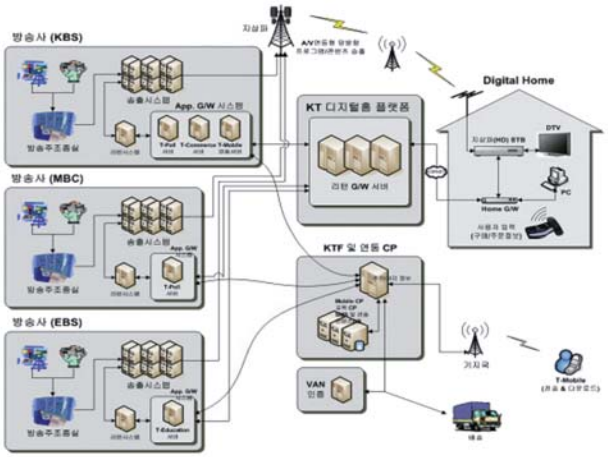
기본적으로 홈 네트워크는 네트워크 인프라를 통해 다양한 데이터를 취합하고 이러한 정보에 사용자가 손쉽게 접근하여 지배할 수 있는 정보통신 환경을

주택과 접목하여 주택이라는 물리적 공간에 구현하고자 하는 데에 그 목적이 있다[129]. 홈 네트워크 기술 및 다양한 이종기기 및 서비스 간 상호 호환성을 검증하고, 기술개발 및 표준화 추진전략을 도축하며 대국민 홍보를 통한 디지털 홈에 대한 인식을 제고한다[130].

(나) 시범 서비스 구성

1) KT 홈 네트워크 서비스

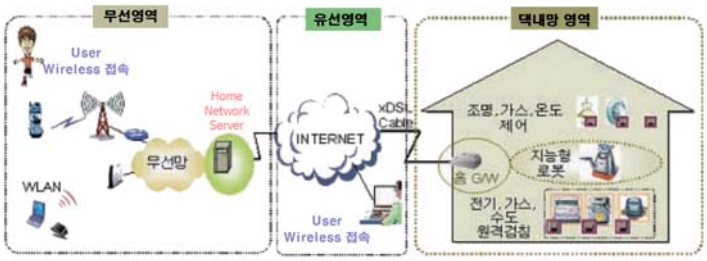
이미 구축된 초고속 인터넷망과 KTF의 무선망의 융합을 통해 유무선 연계하여 단수 제어(Low traffics, High Security)서비스를 제공한다.



(그림 5-19) KT 컨소시엄의 홈 네트워크 시스템 구성도[138]

2) SK 홈 네트워크 서비스

인터넷 망에 물려서 단말기와 통신하고 웹페이지로 서비스를 제공한다. 또한 음성・데이터 통합을 통해 MMoIP 서비스를 제공한다.



(그림 5-20) SK 컨소시엄의 홈 네트워크 시스템 구성도[138]

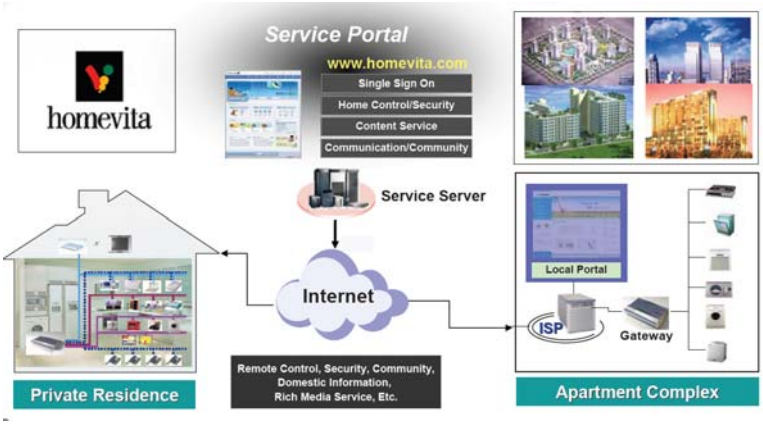
3) 삼성 홈비타(homevita) 서비스

삼성 홈비타는 다양한 콘텐츠 및 비즈니스 프로세스들이 서버에 인터그레이션(Integration)되고 개별 소비자의 취향에 맞게 커스터마이즈(Customized)되어 Home network 망을 통한 다양한 단말기 서비스를 제공한다.

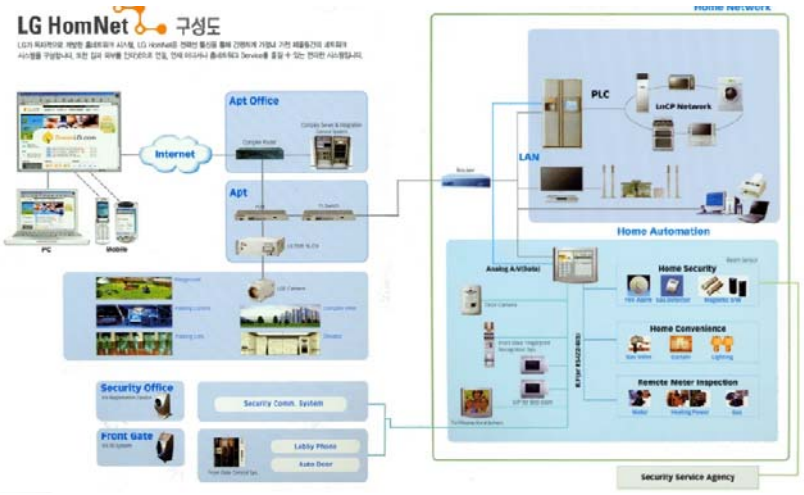
삼성 홈비타는 3대 인프라(IPv6, RFId, BcN)와 홈 네트워크의 연계를 통해 시범서비스를 제공한다. 삼성 홈비타 인프라는 게이트웨이, PAD, Local Portal, Service Portal로 구성되어 있다. 게이트웨이는 홈 패드, 전자레인지, 가스 밸브, 보일러 등 집안의 기기를 관리하고, PAD는 액내/외부 기기 모니터링 및 제어를 위해 게이트웨이와 로컬 서버와 통신한다. Local Port는 게이트웨이와 공동 현관기, 주차 게이트와 같은 외부기기를 관리하고 Service Portal을 통해 상태 감시와 제어 명령을 관리한다. Service Portal은 인터넷 망에 물려있어 단말기와 통신하고 웹 페이지로 서비스를 제공한다.

4) LG 홈넷 솔루션(HomeNet Solution) 서비스

Wall PAD와 게이트웨이 일체형으로 가격이 합리적이고 시공이 간편하다. 그리고 단지 홈페이지 구축을 통한 홈넷 포탈의 맞춤형 정보서비스를 제공하고 댁내 모든 기기의 통합 연동 제어 할 수 있다.



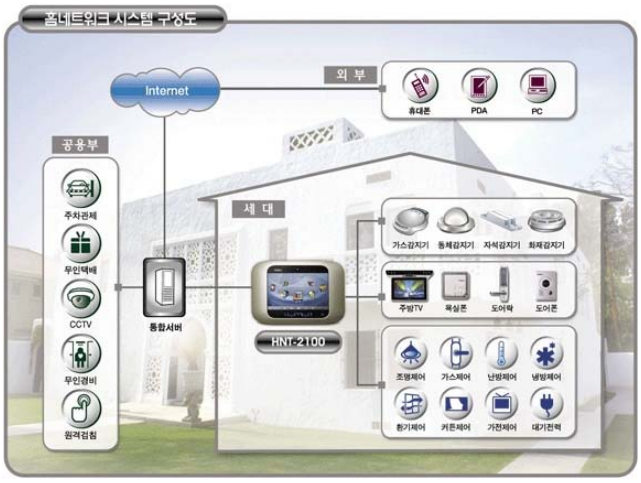
(그림 5-21) 삼성 홈비타(homevita)[152]



(그림 5-22) LG 홈넷(HomeNet) 구성도[153]

5) 현대 홈타운 홈 네트워크

현대 홈타운 홈 네트워크 인프라는 외부 망과 내부 망을 적절히 연계하여 가정 내/외부에서 기기의 제어와 홈 네트워크 서비스를 제공하고 댁내 단자함 중심의 스타 토폴로지로 구성되어 있다. 또한 단자함 내장형 홈게이트웨이가 필요하다.



(그림 5-23) 현대 홈 네트워크 시스템 구성도[154]

(5) 기상/해양 관측 시스템(제주 연해안 정보 수집 시스템)

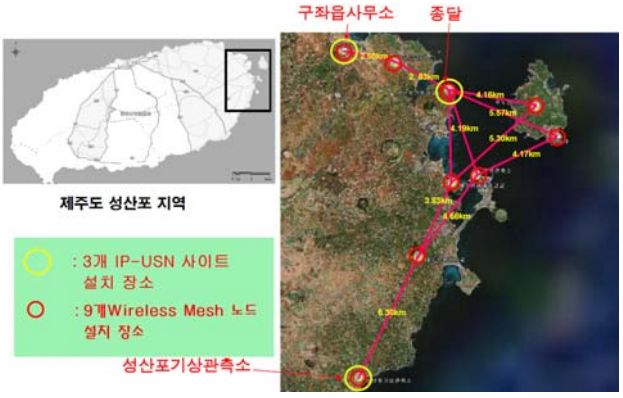
(가) 기상/해양 관측 시스템(제주 연해안 정보 수집 시스템) 개요

USN 기반의 기상/해양 관측 시스템의 시범 서비스인 제주 연해안 정보 수집 시스템은 제주도 연해안에 다양한 USN 기상 센서 및 센서 노드를 설치하고 기온, 기압, 습도, 풍향, 강우량 등 실시간으로 기상정보를 측정하여 용존산소량, 해수온도 등의 데이터를 수집 및 분석하는 기상정보 모니터링이다.

기상/해양 관측 시험망의 첫 번째 목표는 USN 기반의 기상/해양 관측망의 구축과 시험 서비스를 제공하는 것이다[123]. 이를 수행하기 위해서 기상관측 및 해양 관측을 주기적으로 수행하고 있는 공공 기관의 관측 망을 대상으로 USN 기반 기상/해양 관측 시스템을 구축한다. 제주 연해안의 적조 및 기상을 예측하고 어족의 이동경로를 분석하는 활용 등으로 효과적인 수자원 관리 및 기상예측의 정확도를 향상 시킨다. 본 시범 서비스의 두 번째 목표는 USN의 효율적인 서비스 제공과 확산에 중요한 역할을 하는 네트워크 인프라의 시험적 구축이다.

(나) 시범 서비스 구성

AP와 라우터기능을 통신에 하는 메시 노드들끼리 네트워크를 구성하여 망 상황에 맞는 최적 경로를 이용해서 목적지까지 라우팅 된다. (그림 5-28)과 같이 기상/해양 데이터를 측정할 수 있는 USN 장비인 6LoWPAN 노드 사이트를 3개 구축하고, 이들 무선 백본망을 무선 메시 네트워크로 연결하였다. 이 무선 메시 네트워크 무선 백본망에는 IP-CAM을 연동시켜 USN 사이트를 실시간 영상 모니터링 할 수 있도록 했으며, 기존의 기상/해양 관측 장비인 AWS와 조위관측장비도 연동하여하였다[123].



(그림 5-24) USN 기반의 기상/해양 관측 망 무선망 경로[132]

(그림 5-24)는 USN 기상/해양관측 시스템을 설치한 위치와 연결을 보여준다. USN 기상/해양 관측 시스템의 인프라로써 9개 노드를 기반으로 하여 무선 메시 네트워크(Wireless mesh network)로 구축되었으며, 기상/해양 관측 데이터를 성산포기상관측소의 서버까지 수집한다. 즉, 제주지역에 설치된 장소들은 상당히 멀리 떨어져 위치해 있고 메시 네트워크로 연결되었으며 각 장소에서 데이터를 수집하고 메시 네트워크를 통해 정보를 전송 하는 것이다.

(6) USN을 이용한 도시기반시설 관제 시스템

(가) USN을 이용한 도시기반시설 관제 시스템 개요

도시기반시설은 전기, 통신, 도로, 수도, 가스, 지역난방, 송유관 및 지하철 등 지상·지하 시설물과 이에 부속된 관련 시설물을 말한다.

(그림 5-25) 도시 기반 시설 [133]

본 보고서에서는 도시기반시설 관제 시스템 시범 서비스 중 2006년 인천경제자유구역에서 실행된 상·하수도 시설 관제 서비스, 도로시설 기상 관제 서비스, 현장 상황 실시간 관제 및 u-방법 서비스에 대해 분석하였다.

상·하수도 시설 관제 서비스는 하수도관에 유량유속센서를 설치하여 유속 변화 측정을 통해 침입수, 유입수 여부를 파악할 수 있다. 또한 하수도관에 수질 센서를 설치하여 수질 변화 측정을 통해 하수의 오염 정도를 파악 할 수 있고, 상수도관에 압력센서를 설치하여 압력 변화 측정을 통해 누수 여부를 파악할 수 있다.

도로노면 관리 서비스는 도로에 도로노면센서를 설치하여 도로노면의 정보를 수집하고 운전자에게 실시간으로 정보를 제공한다.

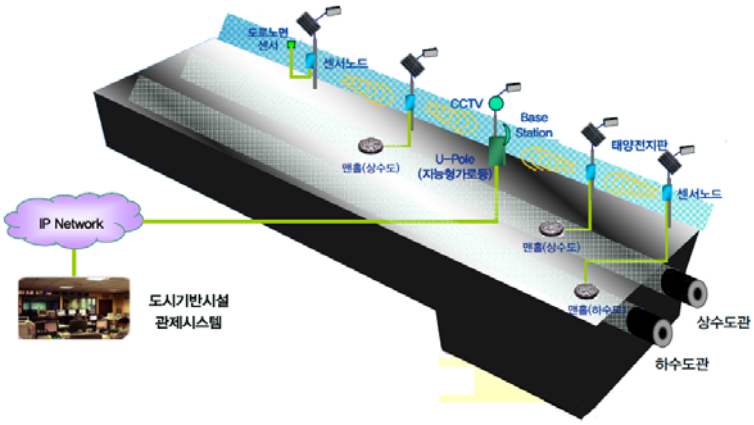
방법 서비스는 지능형 가로등, u-Pole에 설치된 CCTV를 통해 현장 상황을 모니터링하고 통화 장치 및 스피커를 통해 보행자와 영상/음성 통화를 할 수

있다.

도시기반시설은 생활의 편리함을 주지만 관리가 이루어지지 않으면 이용에 불편함을 느끼게 되고 심지어 사고가 생겨 생명이 위험해 질 수 있다. 따라서 USN 기반의 도시기반시설 관제시스템을 구축하고 운영하여 도시기반시설을 실시간 모니터링하고 관리한다. 다시 말하자면 무선 센서 네트워크 기술을 이용하여 비용을 절감하고 추가 확장이 용이하도록 도시기반시설 관제시스템을 구축함으로써 여러 기반시설을 통합 관리 할 수 있고 u-City 건설의 필수 불가결한 도시통합관제센터의 기반을 마련하는 것이다.[123]

(나) 시범 서비스 구성

(그림 5-26)은 도시기반 시설 관제 시스템 개념도이다. 입력, 유량, 수질 센서를 설치하여 상·하수도 시설 관제 서비스를 제공하며 도로노면에 설체된 센서는 도로시설과 기상에 대한 관제 서비스를 제공한다. 데이터 취득을 위해 ZigBee 센서노드를 적용하여 WSN 신뢰성을 검증하고, U-Pole 설치하여 현장 상황을 실시간으로 관제하며 u-방범 서비스를 제공한다. 이러한 도시기반시설 관제시스템 구축 및 운영하기 위해서 도시기반시설 통합관리 방안을 마련했다.



(그림 5-26) 도시기반시설 관제 시스템 개념도[133]

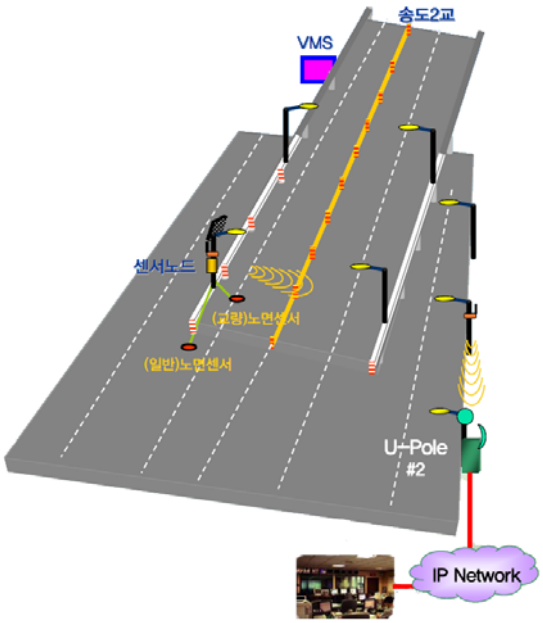
1) 상·하수도 시설 관제 서비스

(그림 5-27)은 상·하수도 시설 관제 서비스를 나타내 것이다. 이 서비스는 압력 센서가 상수도관의 압력을 유량 수질 센서가 하수관의 수위, 유속, 유량, pH 수질 데이터를 검출한다. 검출된 데이터는 가로 주에 설치된 센서노드를 통해서 U-Pole 안의 B/S로 전송되고, 센싱 데이터는 IP 네트워크 장비를 통하여 관제 시스템에 전달 및 저장된다.

(그림 5-27) 상하수도 시설 관제 서비스[133]

2) 도로시설 기상 관제 서비스

(그림 5-28)는 도시시설 기상 관제 서비스를 나타낸 것이다. 이 서비스는 우선 일반도로나 비포장도로에 설치된 도로노면센서가 눈, 비, 결빙 등의 도로 기상 환경 상태 정보를 검출한다. 그리고 검출된 데이터를 가로등 주에 설치된 센서 노드를 통해 U-Pole 안의 B.S로 전송되고 센싱 데이터는 IP 네트워크 장비를 통하여 관제 시스템에 전달 및 저장된다.

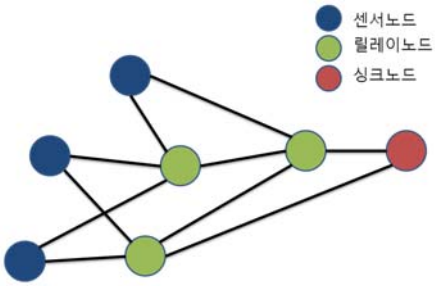


(그림 5-28) 도로시설 기상 관제 서비스[133]

3) 현장 상황 실시간 관제 및 u-방범 서비스

도로변에 설치된 u-Pole이 도로 온습도 및 CCTV 영상 정보를 수집한다. 수집된 정보는 IP 네트워크를 통하여 관제 시스템에 전달하고 관제 시스템은 실시간으로 도로변의 기상 상태와 현장의 영상을 실시간으로 Web에 표출한다.

도시기반시설 관제 시스템에 적용 가능한 ZigBee Network 토폴로지는 크게 스타 토폴로지와 메시 토폴로지가 있다. 스타 토폴로지로 시스템을 구성할 경우 릴레이 노드가 고장 나면 각종 시설의 데이터를 관제센터로 전송하지 못하게 되어 실시간 모니터링이 불가능해지는 문제가 발생한다. 따라서 도시기반시설 관제 시스템은 메시 토폴로지로 구성하였다[123]. 센서의 측정 데이터를 하나의 경로 상에 있는 릴레이 노드들에 의존하여 전송하는 것이 아니라. 여러 경로 상의 릴레이 노드들을 통해 전송함으로써 데이터 전송의 끊임이 없도록 하였다.

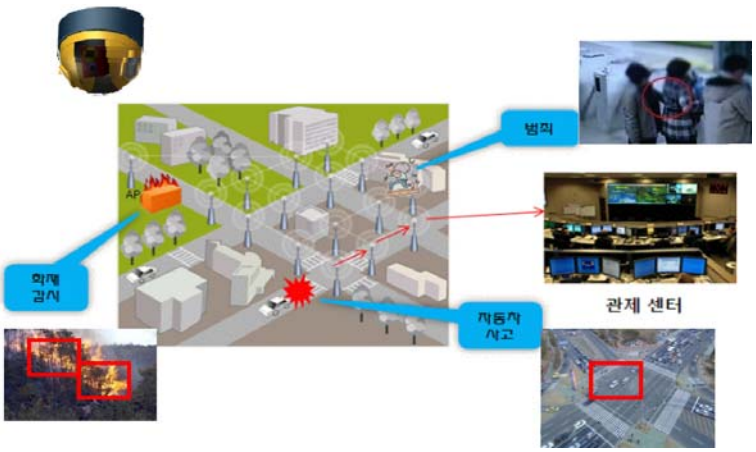


(그림 5-29) 도시기반시설 관제 시스템 메시 토폴로지[123]

(7) 무인 감시 센서 네트워크

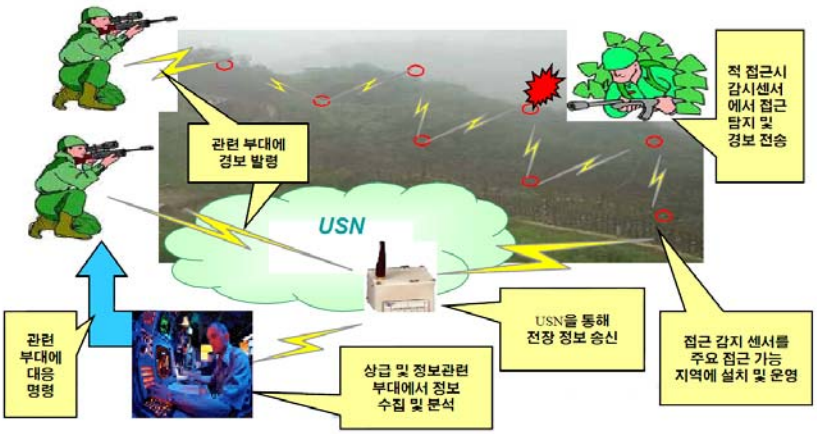
(가) 무인 감시 센서 네트워크 개요

지능형 무인감시 기술은 광범위한 지역에 다중복합 센서 기반의 자율성장 및 사전인지 기능을 가진 지능형 협업 센서 노드들을 설치하고, 무선 메시 망으로 연결하여 사건발생시 센서 노드들이 자율적으로 사건 발생을 인지하고 판단하여 감시요원에게 알려줌으로써 24시간 최소의 감시 인력으로 실시간 감시 및 대응 할 수 있는 시스템의 기술을 말한다[134].



(그림 5-30) 무인감시 시스템 구조

특히, 무인 감시 센서 네트워크 기술을 이용하여 군사 지역을 실시간으로 모니터링하고 감시 및 정찰 할 수 있다. 감시 및 정찰 기능을 수행하는 센서를 휴전선에 설치하여 군의 주·야간 전투력을 향상 시키고 적의 침투를 초기에 발견하여 신속 대응 할 수 있는 시스템을 구축하는 것이다.



(그림 5-31) 휴전선 무인감시[128]

무인 감시 시스템은 첫째, 감시 사각 지역을 최소화 하는 것이다. 반경 50m 감시하는 다중 센서 기반의 지능형 센서 노드가 무선망으로 연결되어 센서 노드 사이의 협업에 의해서 사건을 연속적으로 추적하고 감시한다. 둘째, 지능형 센서 노드가 사건을 자동으로 인지하여 계속 모니터링 하지 않아도 되는 것이다. 그렇기 때문에 최소의 인력만으로 실시간으로 사건의 인지 및 대응이 가능하다. 셋째, 설치가 쉽고 설치 후 빠른 감시 업무가 가능하고(Plug & Play) 설치와 유지보수비가 적게 든다.

지능형 무인 감시 시스템을 이용하여 휴전선 무인 감시 시스템을 구축한다. 따라서 휴전선 무인 감시는 적의 침입을 초기에 발견하고 이를 신속하게 대응할 수 있도록 한다. 이렇게 USN을 이용한 군사 지역 감시 및 관리를 통해 군의 전투력을 향상 시킬 수 있고, 각종 시설물 관리가 용이해진다.

(나) 시범 서비스 구성

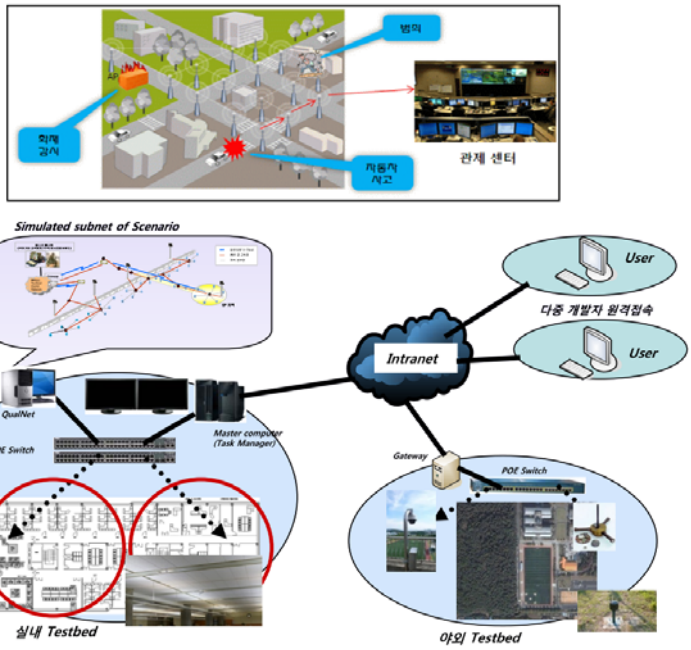
무인 감시 센서 네트워크는 감시 및 정보의 수집·분석하기 위한 센서 노드와 수집·분석된 정보를 관리하고 센서 네트워크를 통해 관제 센서로 전달하는 베이스 스테이션으로 구성된다.

복합하고 다양한 센서 신호를 처리하기 위해서 퓨전 센서 신호처리 알고리즘이 내장되어 수집된 정보의 신뢰성을 향상시켰으며, 저전력 관리를 위하여 최적화된 무선통신 방식을 사용하였다. 또한 무인 감시 서비스의 특성상 보안 프로토콜을 내장하여 정보의 안전성을 높였다. 무인 감시 센서네트워크는 많은 수의 센서 노드로 구성되어 있기 때문에 시스템의 미션을 달성하기 위하여 협력 작업을 하게 된다. 이를 위하여 메시 네트워크 MAC(Media Access Control)프로토콜과 시각동기화를 지원한다[135].

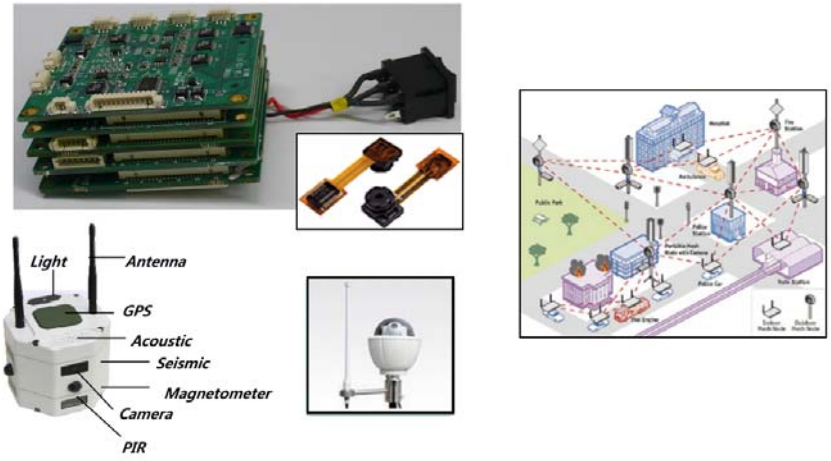
지능형 무인 감시 핵심 기술은 크게 대규모 지능형 협업 무인 감시 시스템 운영 프레임워크, 지능형 협업을 위한 적응적 센서 노드 플랫폼 기술, 다중센서 및 협업을 위한 자율학습 기반 상황인지 기술, 대규모 다중 센서 기반 적응적 융합처리 기술로 나눌 수 있다[134].

(그림 5-32)은 다 계층 센서 네트워크로 구성된 대규모 지능형 협업 무인 감시 시스템 프레임워크 설계를 보여준다. 다 계층 센서네트워크 구성 및 GIS 기반 센서 최적 배치 기술을 개발하였다. 또한 클라우딩 컴퓨터 기반의 테스트베드 기술을 이용하고, 기존 현장 장비와의 Seamless한 연동을 위한 기술 및 표준을 개발하였다[167].

(그림 5-33)는 지능형 협업을 위한 적응적 센서 노드 플랫폼 기술이다. 사건 발생을 감지하는 다중 복합 센서를 가진다. 음향, 진동, 자기장, PIR 영상 등의 이벤트를 감지하는 센서, 온도, 조도, 습도 등의 환경을 감지하는 센서, GPS, 전자 나침반과 같은 기타 센서로 이루어져 있다. 이러한 다수의 센서들로부터 대용량의 센싱 정보를 신뢰적으로 전송하기 위해 메시 네트워크 통신 기술을 적용하였다.



(그림 5-32) 대규모 지능형 협업 무인 감시 시스템 프레임워크[134]



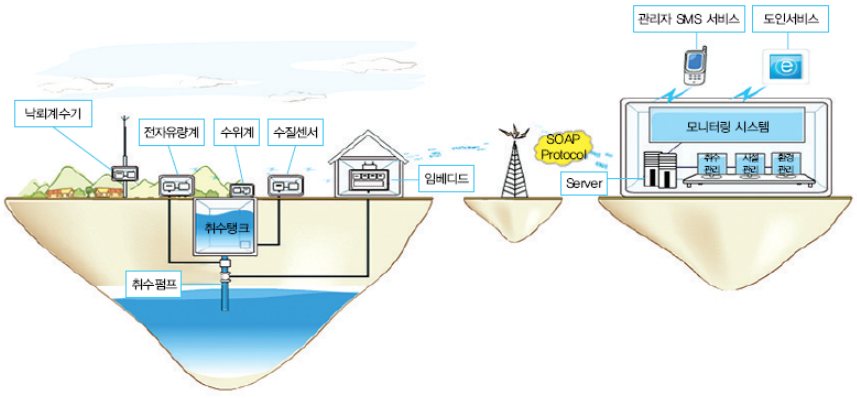
(그림 5-33) 지능형 협업을 위한 적응적 센서 노드 플랫폼 기술[134]

(8) USN 기반 지하수 모니터링 시스템

(가) USN 기반 지하수 모니터링 시스템 개요

제주도는 지리적인 특성상 식수를 지하수에 의존하고 있을 뿐만 아니라 지하수를 활용하는 음료사업을 추진하고 있어 지하수의 오염은 지역생활뿐만 아니라 경제에도 영향을 끼칠 수 있다. 이를 막기 위해 제주도는 USN 기반 지하수 모니터링 시스템 시범사업을 추진하였다[139]. 이 시스템은 USN 기술을 도입하여 지하 상수원의 수질 관리를 위해 암모늄, 용존산소량, 온도 센서 등을 이용하여 실시간으로 하천의 오염 발생 여부와 취수량, 수질, 기상 환경 등의 수자원 관련 정보를 모니터링하고 관제하는 역할을 한다.

USN을 활용하여 제주도의 상수원인 지하수의 수질. 수위, 유량, 낙뢰 정보 모니터링 및 통합 관제 시스템 구축을 통해 취수장 시설물을 효율적으로 관리하고 제주도민들에게 안전한 식수원을 제공한다. 또한 제주도에서 낙뢰가 가장 빈번한 지역을 낙뢰 감시 우선 지역으로 선정하여 취수관정 주변 낙뢰를 예측 경보하여 사전 조치할 수 있는 낙뢰 정보기를 시범 설치함으로써 낙뢰를 감시하고 관련 기기를 보호한다. 시스템의 도입으로 인해 취수장 및 먹는 물의 수질 관리 효율성 증대와 물 공급을 위한 시스템의 기반을 마련함으로써 재난발생 시 관리 경비의 감소가 기대된다.



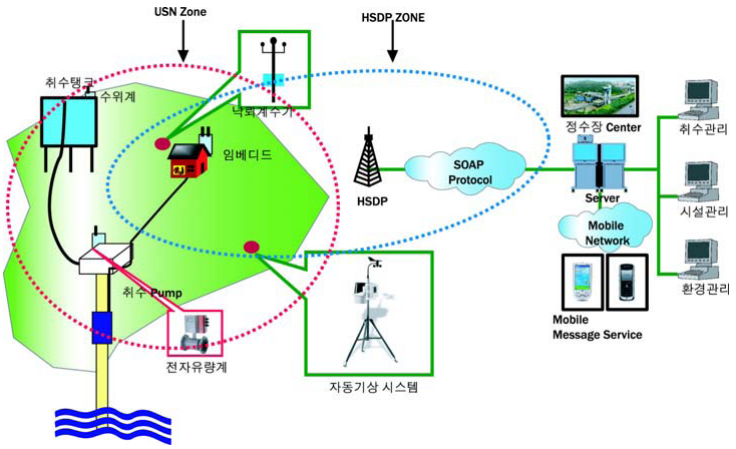
(그림 5-34) 지하수 모니터링 시스템 구성도[11]

(나) 시범 서비스 구성

제주도의 주 취수원인 4개소(광평리, 수망리, 하례리, 성읍리)에 센서 노드를 설치하고 저장 탱크 내 먹는 물의 수온, PH, 전기전도도, 탁도, 잔류염소 등의 수질 정보를 모니터링하고 취수량을 제어할 수 있다 [141].

USN 기반 지하수 모니터링 시스템에 사용되는 센서는 3가지로 유량센서, 수위센서, 수질센서로 구성된다. 유량센서는 취수펌프에 설치가 되어 펌프가 동작하는 동안에 취수되는 물의 양을 단위 시간별로 측정한다. 수위 센서는 취수 탱크 내부에 설치되어 현재 탱크에 저장되어 있는 물의 높이를 측정한다. 수질센서는 취수 탱크에 설치되어 전기전도도, 온도, 잔류염소, pH, 탁도 등의 데이터를 측정하게 된다.

IP-USN은 1개 취수장에 다섯 개의 노드와 하나의 게이트웨이의 세트로 구성이 되어있으며 3개의 센서에서 측정한 데이터를 IP-USN을 통하여 중간 수집 장치에서 수집한 후에 중앙관제센터에 전송하는 구조를 지니고 있다.



(그림 5-35) 지하수 모니터링 시스템 구성도[142]

시스템을 통해 수질 및 수위 정보의 이상 상황이 감지될 경우 현장 관리자에게 전달이 되며 이 데이터를 이용하여 취수장 별 지하수 상태와 각종 통계

정보를 제공받을 수 있다. 또한 취수장 수질정보 및 각종 지하수 관련 통계자료를 인터넷을 통해 확인할 수 있는 서비스도 제공한다.

(그림 5-36) 유량센서[142]

(그림 5-37) 수질, 수위계와 센서 노드[142]

제주도의 주 취수원인 4개소(광평리, 수망리, 하례리, 성읍리)에 센서 노드를 설치하고 저장 탱크 내 먹는 물의 수온, PH, 전기전도도, 탁도, 잔류염소 등의 수질 정보를 모니터링하고 취수량을 제어할 수 있다.

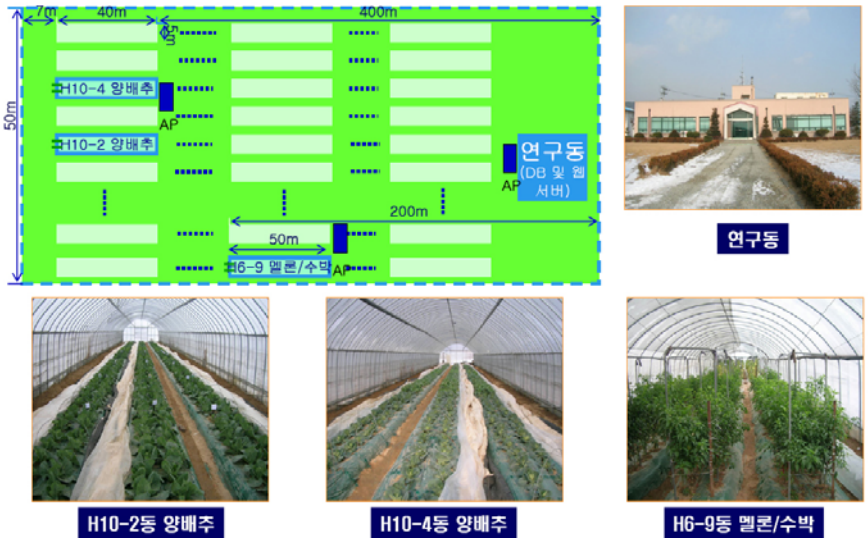
(9) USN 기반의 농산물 재배관리 시스템

(가) USN 기반의 농산물 재배관리 시스템 개요

농업분야에서는 RFID/USN 기술을 농작물 재배환경 모니터링 시스템에 적용함으로서 비즈니스 모델인 u-farm을 도출하고 현장시험을 통하여 이를 검증한 시범 서비스로 u-farm 응용 서비스 모델 발굴을 통해 최적의 농산물 재배환경을 산출할 수 있는 기반을 조성한다[144].

u-farm은 인력과 가축을 이용한 농업에서 농기계를 활용한 생산의 대량화를 구축한 기계화 농업을 거쳐 단일 센서를 활용한 재배 환경을 최적화한 자동화 농업 단계를 넘어선 융합화, 지능화 농업을 목표로 하고 있으며 RFID/USN의 데이터 상호연동을 통한 최적화된 재배환경을 조성하고 농산물 이력 데이터를 제공한다. 또한 상황인식, 유비쿼터스 기술을 이용하여 농산물 품질을 향상시

키고 생산량을 증대시켜 지능화 농업단계구축을 목표로 한다.



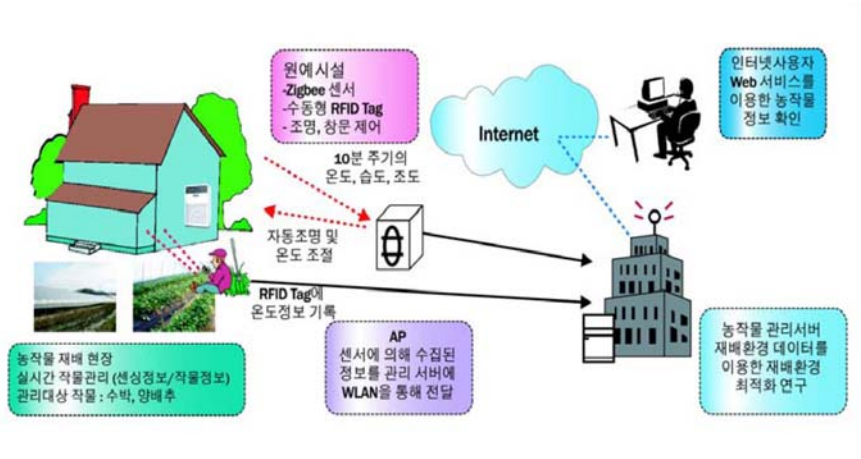
(그림 5-38) 시험장 구성도[144]

재배현장에 센서 네트워크를 구축하여 실시간으로 재배 현장 정보를 수집하고 RFID시스템과 연계하여 체계적으로 농작물 관리를 할 수 있도록 한다. 효율적인 농작물 재배환경 관리를 위해 온도, 습도, 조도 센서를 이용하여 농작물 생장에 필요한 데이터를 수집하고 재배환경을 제어하는 시스템 구축이 주요 목적이다.

(나) 시범 서비스 구성

통합 시스템은 실시간 온도, 습도, 조도 측정을 위한 USN 시스템, 농작물 생장환경 정보 습득을 위한 RFID 시스템, 실시간 최적 생장환경 구현을 위한 환경제어 시스템, 원격지에서 농작물의 환경을 인지할 수 있는 웹서비스 RFID 시스템과 USN 시스템을 연동하는 데이터베이스로 구성되어 있다. 사설원예에 설치한 USN 센서와 RFID를 통해 작물 생장에 필요한 데이터 수집, 현장제어, 현장 온도, 습도 확인 및 분석 가능하다. Ad-hoc 방식의 센서 네트워크를 이

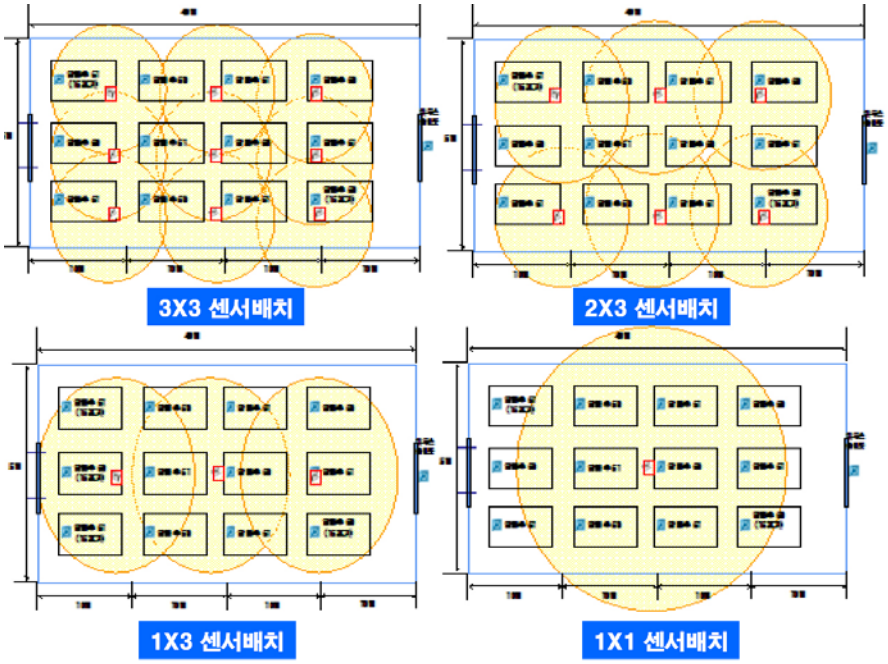
용하여 농작물의 재배와 관련된 온도, 습도, 조도의 데이터를 수집하며 USN에 의해 획득된 생장환경 정보 및 농작물 혹은 비닐하우스 정보를 제공한다. 또한 RFID/USN 통합 응용 서비스는 USN에 의해 수집된 정보와 기존의 농작물 재배에 사용되고 있는 데이터를 비교하여 지역 및 환경 특성에 따라 실제 재배환경의 개선에 이용될 수 있는 정보와 그 특성을 분석한다. 분석된 정보는 웹서비스를 통하여 실시간으로 원격지에서 관련 데이터에 접근할 수 있다. 또한 수집된 정보는 최적의 생장환경 제공을 위하여 생장 환경 조절장치 제어에 데이터로 활용한다[122].



(그림 5-39) 농작물 재배환경 모니터링 시스템 구성도 [122]

생장환경 모니터링을 위해 원예시설에 품종 별로 온도, 습도, 조도 등을 측정할 수 있는 센서 노드를 설치한다. 센서 노드는 5m×40m 크기의 비닐하우스에 (그림 5-41)와 같이 3×3, 2×3, 1×3, 1×1형태 등으로 다양하게 설치가 가능하여 클러스터 단위로 관리가 가능하다. 센서에 의해 센싱 된 정보는 관리 서버와 무선 LAN으로 연결된 베이스 스테이션으로 전달된다. 관리 서버는 수집된 생장 환경 정보를 저장하고 이를 사용자에게 실시간으로 제공한다[122].

(그림 5-40) 현장에 설치된 센서 노드[144]



(그림 5-41) 센서 배치 개념도[144]

(10) U-주차정보 관리 서비스(인프라벨리의 “Upia-Parking")

(가) U-주차정보 관리 서비스 개요

U-주차관리 서비스는 무선네트워크 기술을 활용하여 주차장의 차량 출입관리, 유도정보, 주차가능 위치 정보 등을 이용자에게 제공하는 서비스를 말한다. 주차 정보 관리 서비스는 주차정보를 수집할 수 있는 각종 센서를 통하여 관련 정보를 수집하고 분석/가공하여 주차장의 이용자들에게 제공하고, 주차 이력관리, 주차장 시설물 관리 등의 종합적인 주차정보관리체계를 구축할 수 있다[145].

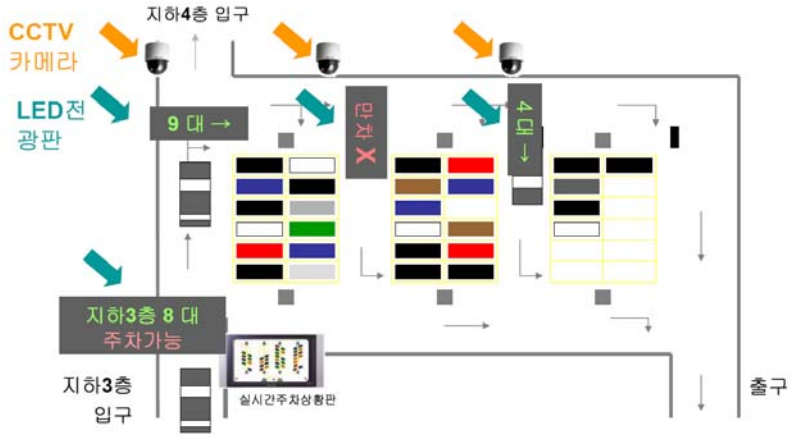
주차 정보 제공 및 유도 서비스는 주차장의 입구와 각 주차 면에 USN 기반의 센서 노드를 설치하고 유/무선 통신을 통하여 서버에서 실시간으로 데이터를 수집하고 전광판, 주차위치 확인기와 같은 제공 장치를 통하여 이용자들에게 주차 정보를 제공하고, 주차위치를 유도하는 서비스를 말한다. 이를 위해 2006년 인프라밸리에서는 주차장 내에서의 모든 상황의 영상인식을 통하여 관리하는 지능형 주차 관제 시스템을 구축하였다. 인프라밸리에서 개발한 "Upia parking"은 차량인식시스템과 주차유도 시스템, 영상보안시스템, 에너지 관리 시스템으로 구성되어 유비쿼터스형 주차관리 기능을 제공한다[146].

USN을 도입한 지능형 주차관제 시스템은 주차장에서 주차공간을 찾기 위한 번거로움과 주차장에서의 장시간 주차대기에 의한 불쾌감, 장시간의 공회전 매연으로 인한 공기오염 등의 문제점을 해결할 수 있을 것으로 기대된다. 또한 불법 주차 및 빈자리 차량을 실시간으로 관리할 수 있어 주차면의 효율적인 관리가 가능하다.

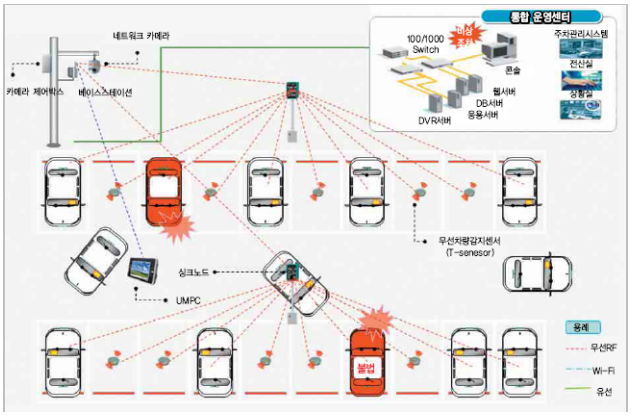
(나) 시범 서비스 구성

지능형 주차 관제 시스템은 주차장에 있는 차량이 인가된 차량일 경우에는 빈자리가 있는 구역을 전광판으로 알려주어 신속한 주차 서비스를 제공한다. 인가되지 않은 차량의 경우에는 차량의 존재 및 위치를 관제 모니터로 전달하

여 운영자가 신속하게 처리할 수 있도록 한다. 시스템에 사용 되는 센서는 배터리 기반으로 동작하며 차량의 존재 유무를 판단하는 복합 센서가 내장되어 현재 주차 면에 차량이 주차하고 있는지 여부를 판단할 수 있다. 주차 노면에 설치한 센서 노드가 감지한 정보는 싱크노드를 거쳐 단일 베이스 스테이션으로 차량의 존재 여부를 전달하게 된다. 또한 베이스 스테이션은 LAN을 통하여 관제 서버에 연결이 되어 주차 면에 차량의 존재 유무에 대한 정보를 해당 지역의 운영자에게 실시간으로 전달한다[135, 146].



(그림 5-42) 주차 유도 서비스 구성도[146]



(그림 5-43) 무인 주차장 서비스 개념도[135]

(11) USN 기반의 식수원 관리 시스템

(가) USN 기반의 식수원 관리 시스템 개요

1991년의 낙동강 오염사례, 1994년의 시화호 오염 사례, 2006년 소양강 상류 인북천 오염으로 인한 국내 주요 수질 오염 사례에 대한 심각성을 인지하고 USN을 이용하여 수질오염을 실시간으로 확인하고 센서노드로부터 얻은 수질 정보를 식수원 관리 기초자료로 활용하고자 하는 목적으로 구축된 시스템이다[123]. USN 서비스의 도입으로 인해 기존의 시스템이 가지고 있던 수질정보에 대한 상황 원인 분석과 현장 수집의 어려움으로 인한 기초 자료 활용의 한계를 극복할 수 있게 되었다. 또한 센서노드를 설치하여 하천의 오염도를 측정하고 재해 당시의 하천의 수질 데이터를 축적함에 따라 수질 정보 분석을 위한 기초 자료 활용 및 수질 관리를 통해 각종 오염원을 실시간으로 관리할 수 있다[11].

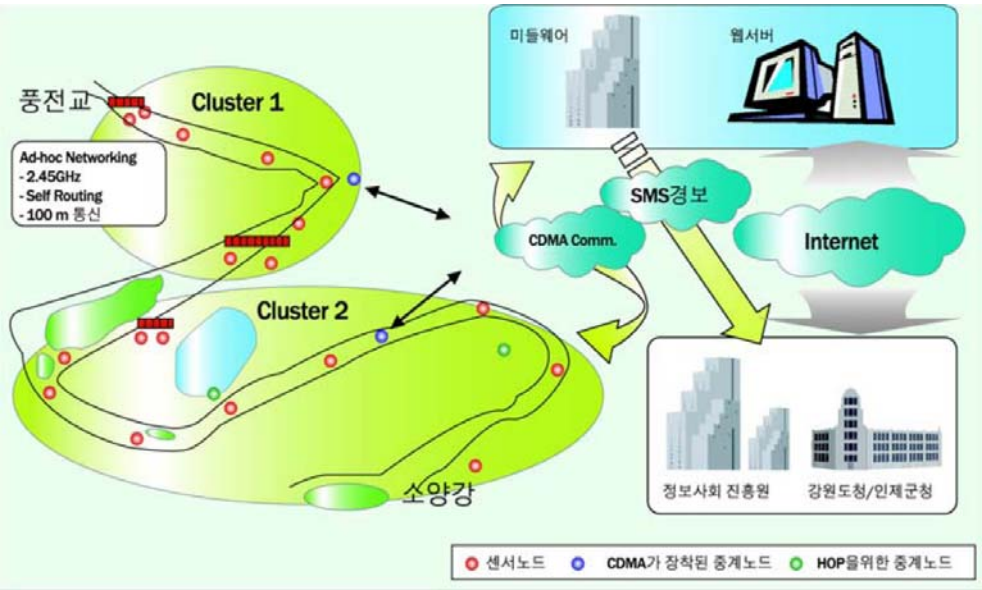
이 밖에도 급격하게 변하는 기상 상태의 변화와 하천 오염의 증대로 인해 발생하는 생태의 변화와 물의 수질 상태의 보장을 위해 하천의 상태에 관한 정보를 지속적으로 얻을 수 있다. USN기반의 식수원 관리 시스템은 소양강에서의 현장 시험을 통하여 수질정보 분석을 위한 기초 자료 수집으로 인하여 앞으로 공장지대 등의 오염지역 관리, 전국적인 오염원에 대하여 과학적이고 체계적인 관리가 가능할 것으로 보인다.

USN기반의 식수원 관리 시스템은 무선 네트워크 기술을 이용하여 실시간으로 소양강 상류(인북천)의 수질 데이터 수집과 분석을 통하여 수질 오염 여부의 식별을 용이하게 하고 관련 업무의 효율성을 증대시키는 수질 모니터링 시스템 구축을 목표로 하였다. 또한 수질에 이상 징후가 발견될 경우 무선 통신과 CDMA통신을 이용하여 원격지의 데이터 서버에 저장이 되고 웹기반의 어플리케이션 소프트웨어를 이용하여 실시간 확인이 가능하다[124].

(나) 시범 서비스 구성

수질 모니터링 시스템은 하천에서 센서를 통해 수집된 pH, DO, 탁도, 온도, 전도도 등의 수질 정보를 싱크노드 역할을 하는 중계노드에 전달하는 ZigBee 방식을 이용한다. 그리고 각 센서 노드들은 30분마다 전송되는 센싱 데이터를 Ad-hoc 네트워크 방식을 이용하여 멀티 홉을 통해 수질 정보를 싱크노드에 전달한다.

중계노드에는 센싱 된 데이터를 싱크노드에서 유선망으로 전달하기 위해 CDMA 기술이 포함된다. 이러한 방식으로 중계노드가 전달받은 수질정보는 유선망을 거쳐 각 서버에 기록이 되며 이들 데이터를 활용하여 각 센서로부터 센싱 된 수질 정보들의 실시간 데이터 분석이 이루어진다. 수집된 정보를 분석할 때 미리 규정해놓은 기준치를 초과하는 상황이 발생 할 경우 경보를 발생하여 관리자에게 통보한다[124].



(그림 5-44) 시스템 구축 개념도[147]

(12) 3대 하천 생태복원 모니터링 시스템

(가) 3대 하천 생태복원 모니터링 시스템 개요

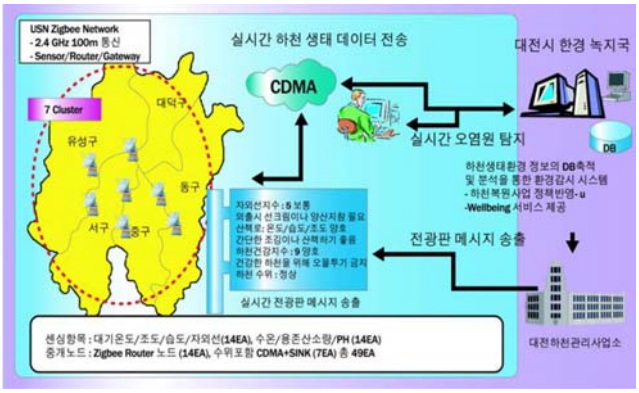
2007년 1월부터 10월까지 약 10개월 동안 대전광역시 첨단산업 진흥재단과 대우정보 컨소시엄의 진행으로 대전 3대 하천의 주요지점(교량 7개)에 USN 기반의 하천 생태감지 센서를 설치하여 하천 생태 사고대응 및 복구 체계 시스템과 환경 모니터링 시스템 및 효율적인 업무 체계를 위한 USN 인프라를 구축하였다[11].

유비쿼터스 기술을 실생활에 적용함과 동시에 대전 3대 하천의 생태복원을 통해 시민들의 삶의 질의 향상을 목표로 한다. 대전 3대 하천의 7개 주요 교량 주변에 USN 센서를 설치해 수소이온농도(pH)·용존산소(DO)·수온 등의 수질정보 뿐만 아니라 수위, 온도, 조도, 습도, 자외선에 대한 정보를 주기적으로 측정하게 된다. 수집된 정보는 마찬가지로 USN 장비를 통해 실시간으로 저장되며 모니터링 된 정보는 전광판을 통해 시민들에게 제공한다. 이를 통해 하천 오염원 탐지 업무를 전산화하여 대전 생태복원 조성사업의 연계를 통한 U-Wellbeing 도시 건설 확대의 효과가 있을 수 있다[148].

(나) 시범 서비스 구성

센서는 탄동천의 내봉교와 장동천 합류지점, 대동천의 제1삼성교, 철갑교, 대전천의 현암교, 천석교, 대전천 하류 1개 지점에 설치된다[140]. 센서들은 중계노드를 통해 ZigBee통신 방식을 이용한다. 설치되는 센서의 종류는 주로 3가지로 수질센서와 조도센서 그리고 대기센서 등이 있다. 이들 센서는 대기온도, 조도, 습도, 자외선, 수온, 용존 산소량, ph, 수위 등의 센싱 항목과 관련된 데이터를 수집한다. 센싱 된 정보는 게이트웨이를 통하여 서버로 전달이 된다. 전달된 정보는 전광판을 이용하여 시민들에게 제공될 수 있도록 가공된다. 예를 들어 환경오염이나 기온의 상승, 자외선 지수 초과 등의 이상 징후가 발견이 되었을 경우에는 CDMA를 통하여 실시간 오염원을 탐지하고 하천 생태

환경 정보의 DB에 축적이 되어 분석을 통하여 결과가 도출된다. 이러한 방법으로 실시간으로 수집되는 하천 생태 정보데이터의 활용으로 대덕대교의 전광판에 U-Wellbeing정보와 관련된 메시지를 송출하고 또한 관리자에게 문자메시지로 전송된다[11].



(그림 5-45) 하천 생태복원 모니터링 시스템 구성도[142]

(13) USN 기반의 문화제 관리 시스템

(가) USN 기반의 문화제 관리 시스템 개요

USN 기술을 도입하여 불국사 및 국보급 문화재 보호에 필요한 정보를 실시간으로 분석함으로써 화재, 부식, 균열 등의 손상 유무를 사전에 파악하고 예방하는 시스템으로 실시간 산불 발생여부 감시 및 문화재 환경 정보를 모니터링 한다. 산불 예방과 문화재 주변 환경 모니터링을 위해 불꽃 감지(산불 모니터링), 온도, 습도 센서를 이용하여 실시간으로 산불의 발생여부를 감시한다. 문화재 관리 시스템 도입으로 수작업 형태의 문화재 관리 업무의 고도화와 사후처리 중심의 복원업무에서 사전 감시로 관리체계를 변경함으로써 관리 인력 및 복원 비용 절감된다[122].

무선 센서 네트워크를 도입하여 불국사 주변에 화재 감지 센서를 설치 및 온도, 습도, 기압, CO센서를 설치하여 화재 요인을 사전 감지한다. 문화재 주

변 환경 훼손을 최소화하면서 실시간으로 문화재의 상태를 모니터링 한다. 또한 대부분의 문화재가 주로 외부 환경에 많이 존재하므로 자연 환경에 대한 영향을 많이 받게 되기 때문에 문화재가 위치하고 있는 주위 자연 환경에 대한 감시와 악의적 의도를 가진 접근자가 문화재 훼손과 약탈 하는 것을 방지하기 위한 감시 및 예방을 목표로 한다.

(나) 시범 서비스 구성

불국사 주변에서 발생 가능한 화재 감시 및 문화재 보존과 보호를 위하여 온도, 습도 센서를 이용하여 데이터를 수집하고 관리한다. 불국사 외부에 설치되는 외부 센서는 화재 및 산불을 예방하기 위한 센서로 불꽃감지센서, PIR센서 등이 있다. 네트워크 형태는 25개의 센서 노드를 각각 12개와 13개로 나누어 두 개의 스트링 네트워크로 구축하고 각각의 센서 노드는 25~30m 간격으로 불국사 경외를 둘러싸는 스트링 토폴로지의 형태로 구축이 된다.

(그림 5-46) 서비스 개념도[149]

불국사 내부의 주요 지역에는 문화재 손상을 방지하기 위한 PIR센서, 온도센서, 습도 센서를 설치하여 데이터를 수집한다. 온도, 습도, 조도, 기압 센서를 가진 2개의 센서 노드는 불국사 경내의 두 지역에 설치되어 환경요소를 측

정하고 측정한 데이터를 베이스 스테이션을 통해 서버로 전송하게 된다.

(그림 5-47) 시스템 구성도[149]

시스템은 (그림 5-47)과 같이 구성되어진다. 센싱 정보는 크게 문화재 손상 요인 분석과 화재 방지를 목적으로 문화재 건물의 온도, 습도, 기압, CO센서와 카메라를 통해 수집된다. 센싱 된 데이터는 CDMA를 이용하여 베이스 스테이션으로 전송되고 이는 다시 통합 서버의 관리 하에 모니터링 시스템의 데이터로 활용될 수 있도록 한다. 이상이 감지될 경우 센서 네트워크와 연동이 되어 있는 카메라를 이용하여 해당지역의 영상 정보를 관할 경찰서나 소방서로 전송한다[124].

불국사 경내 네트워크는 대웅전에 설치되어 있는 베이스 스테이션과 2대의 센서 노드가 트리 라우팅으로 구성된다. 각 센서 노드는 20분 간격으로 센싱된 데이터를 베이스 스테이션으로 전달한다. 이 때 경내 네트워크 구성은 두 가지의 형태로 구성된다. 첫 번째는 베이스 스테이션에서 라우팅 패킷으로 시작되는 Top Down방식이고 두 번째는 센서 노드에서 Search Parent packet을 전송하면서 시작되는 Bottom Up방식이다[123].

외부에 설치되는 네트워크는 12개, 13개로 분리되어 설치된다. 두 개의 네트워크는 서로 다른 채널을 사용하여 데이터 충돌을 방지한다. 스트링 토폴로지 형태로 구성된 두 개의 네트워크가 불국사 경외를 둘러싼 형태로 설치된다.

(14) U-울릉도, 독도 재난・재해 조기예보 시스템

(가) U-울릉도, 독도 재난・재해 조기예보 시스템 개요

U-방재 시스템은 도시의 기반시설, 재해취약시설, 방재시설물 등의 재난 구성요소에 첨단 U-IT 기술을 접목시켜 방재 인프라의 사회적 효율성을 높이고, 안전한 도시 관리를 위해 실시간 재난정보 수집과 분석 예측, 상황판단, 대응조치 등을 자동화하는 미래형 최첨단 방재시스템을 말한다[150]. U-울릉도, 독도 재난·재해 조기 예보 시스템 구축 사업은 2007년 5월부터 11월까지 약 7개월 동안 경상북도와 일진 네트워크 컨소시엄이 주최한 사업으로 울릉도, 독도 지역에 USN 기술을 도입하여 실시간 재난·재해에 대한 정보를 제공하여 거주민과 관광객의 안전을 도모하고, 재난·재해를 조기에 감지하여 향후 복구에 따른 예산 최소화를 위하여 구축되었다. 첨단 IT기술을 기반으로 울릉도 전 지역의 하천 수위 범람 예보 시스템과 독도 접안 시설의 수위, 유속, 온도 감지 센서 구축을 통하여 데이터를 실시간 관리할 수 있는 시스템으로 구성되었으며 해일 등의 기상 이변에 대한 실시간 관측을 통하여 동해안 지역 피해의 최소화 및 안전한 지역 생활을 가능하게 한다.

울릉도 전 지역의 하천 수위 범람 예보 시스템은 울릉도 내 모든 하천에 하천 범람 사전 예보 시스템을 구축하여 해당 부서 간의 정보 공유와 주민들에게 실시간으로 상황을 전달하여 울릉도 내 하천 정보를 분석하여 하천 범람에 대한 조기 예보를 실시한다.

또한 독도 접안 시설에 센서 노드 구축을 통하여 울릉도 및 내륙에 실시간으로 수집된 정보를 전송하여 독도 접안의 허가 여부를 제공하는 등 방문객에게 편의를 제공할 뿐만 아니라 재난 및 재해 현장 정보의 공유가 가능하도록 한다.

(나) 시범 서비스 구성

재난, 재해 감시를 위한 센서 네트워크를 구성하기 위해서는 기상 상태가 좋지 않은 환경에서도 네트워크의 간의 통신 가능성이 보장되어야 하며 실시간으로 통신이 제공되어야 한다. 또한 울릉도 하천과 같이 계곡형 하천에서의 빠른 수위 변화의 관측이 가능해야하고 장시간의 모니터링을 위한 전력 관리가 필요하다. 네트워크의 신뢰성 보장을 위하여 각 센서 노드와 게이트웨이 사이의 모니터링 메시지를 추가하여 네트워크의 연결 유무의 확인이 가능하며 센싱 정보의 미 전달시 게이트웨이를 통한 통신상태의 점검 및 복구가 가능하다.

서버와 네트워크 연결을 위하여 게이트웨이는 주기적으로 CDMA/ADSL망의 연결 상태를 확인하고 연결이 끊어졌을 경우에는 전송된 센싱 정보를 베이스 스테이션의 파일 시스템에 임시 보관이 가능하며 연결이 복구되면 정보가 재전송이 된다.

1) 울릉도 하천 범람 조기 예보 시스템

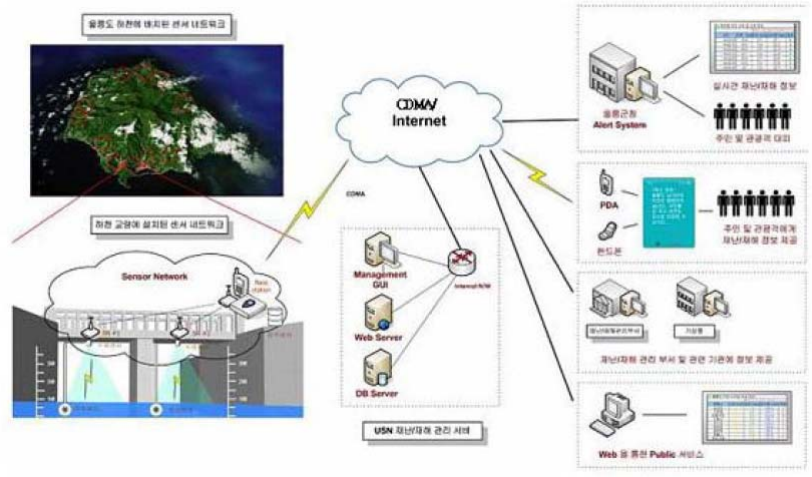
유량, 유속, 수위센서를 사용하여 일정한 단위 시간마다 데이터를 수집하고 이를 분석하여 일정치 이상의 값이 감지될 경우가 발생할 때 수집한 데이터를 게이트웨이를 통하여 관제서버로 전달한다. 센서 노드는 실시간 정보 수집과 분석의 효율성을 위하여 전원 제어 시스템을 내장하고 있으며 다수의 센서 노드 운영과 네트워크 효율성 증대를 위해 트리 형태의 토폴로지로 구성이 된다 [135].

2) 독도 접안 지원 서비스

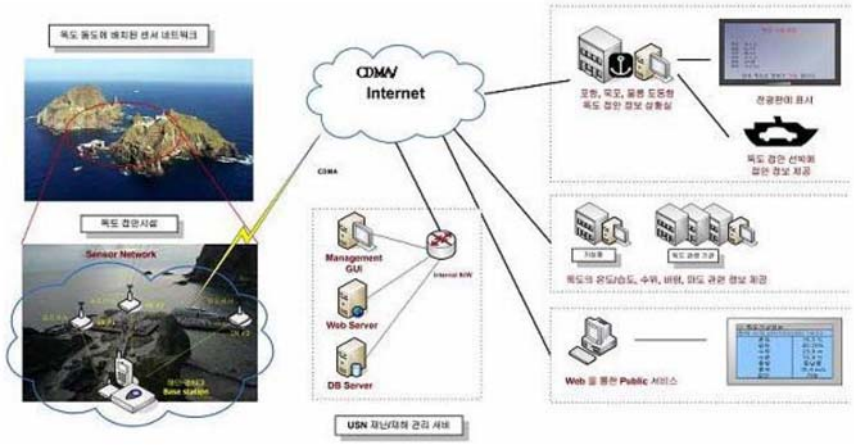
독도 접안 시설에 센서노드 구축을 통해 울릉도 및 내륙에 실시간으로 수집된 정보를 전송하여 관광객에게 하전에 독도 접안 가능성에 대한 정보를 제공, 방문객에게는 편의를 제공하여 재난·재해 현장 및 유관기관, 국민들은 재

난 정보 공유가 가능해진다.

접안 지역용 센서 노드는 독도에 배가 접안하는 시기에는 수위 및 파도 관련 센서의 측정 횟수 빈도수를 늘려 측정을 자주 하도록 하고 평소에는 그보다 측정 주기를 길게 두어 측정하도록 한다.



(그림 5-48) 울릉도 하천 범람 조기예보 시스템 구성도[142]



(그림 5-49) 독도 접안시설 지원 시스템 구성도[142]

나. 국외 시범 서비스

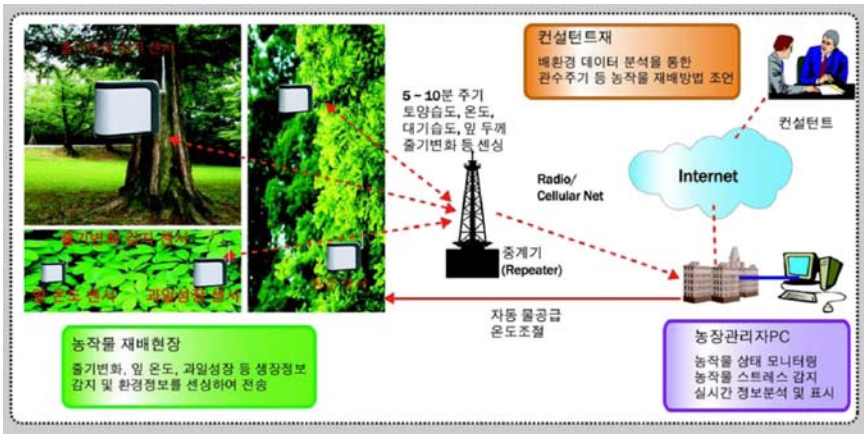
국외의 u-City 시범 서비스의 경우에는 각 도시의 특성과 장점을 부각시켜 도시의 경쟁력을 높일 수 있는 방향으로 서비스가 진행되고 있다. 또한 해외의 경우에는 국내 사례와는 달리 개인 서비스 분야에서의 서비스보다는 공공이나 기업체의 물류/유통 분야에서 서비스가 진행되고 있다[112].

[표 5-17] 국외 u-City 사례[[157]

구 분	해외 USN 구축 사례
국방 외교 침입	○ 군사용 지형 탐사 : 이스라엘 공군이 팔레스타인 교전지역의 지형 탐사용으로 무인 무선데이터 전송 비행물체 개발 ○ 금속탐지 : Magnetometer 센서 및 임펄스 레이더 센서 이용 ○ Military Surveillance : 미국 해군함선에 RSC(보안과 감독을 위한 분산형 센서)를 통해 무선 센싱 네트워크 사용 o 스웨덴 WSAN for intrusion monitoring : 침입 모니터링으로 SaaB system과 스웨덴 연구기관(SICS)가 개발, WSN 네트워크는 센서가 leaf node로 연결되어진 백본으로 구성[117]
유통 물류	○ 청과류에 대한 유통 환경 센싱 : 일본에서 딸기 유통과정에서의 온도 변화를 센싱하기 위해 포장박스 내에 초소형 액티브 센서 설치 ○ 신선 생선 유통 : 일본 총무설 실증 실험의 일환으로 2004년 실행
도로 교통	○ 미국 교통국의 ITS : 전보된 통신 기술을 사용하여 운송 안전과 이동성을 개선 ○ IrisNet의 The Seeing Internet : 주정차 된 자동차의 이상 상태를 사진을 찍어 사용자의 PDA에 전송하여 물리적인 피해 보상
의료 보건	○ e-Nightingale Project : 일본의 병원 간호사들이 입을 수 있는 u-센서를 이용하여 실제 의료 환경에서 도처에 산재된 지식을 프로세싱 ○ 하버드 대학의 Vital Sign Sensor : 환자의 몸에 착용하여 심장 박

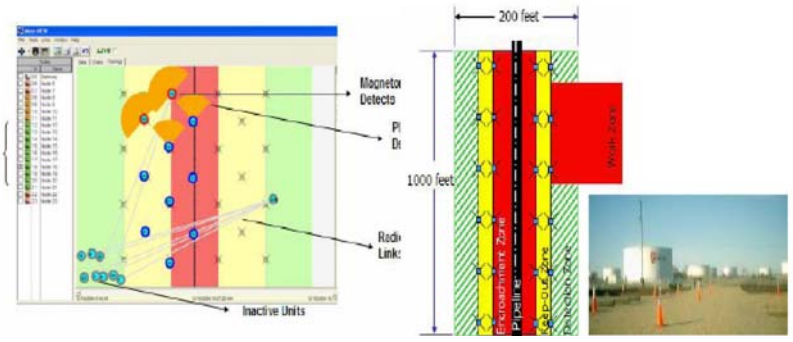
	동수 또는 산소포화 심전도 등을 체크하여 이상 시 보건소나 의사에게 위험 신호 발신 ○ 의약품에 장착된 액티브 태그를 활용한 병원 의료사고 개선 : 일본 병원 내에 사용되는 약품에 액티브 태그를 설치, 약품의 과오용으로 인한 의료사고 방지
환경 보전	○ NASA의 남극지역 원격 탐사 및 데이터 수집 시스템 : 남극의 원격지역 운석탐사 프로젝트로 노출된 기반암과 모래인 물질 반응이 일어나는 곳에서 온도 변화 측정 ○ CENS의 NIMS : 불특정한 지역에서 예측할 수 없는 시간 변수적인 자연환경의 센싱 o 이스라엘 무선 식물 모니터링 : 식물 생장 모니터링을 통해 생성량을 자동으로 측정하여 관수 주기, 관수량 등의 재배법 개선에 활용 (그림 5-50)[117]
산업 건설	○ 일본의 건물 위험 모니터링 : 지진으로 인한 진동, 충격 및 화재에 인한 온도 상승 등을 감지하여 건물에서 일어날 수 있는 위험물 조기 발견 및 최적 조치 ○ JENNIC의 가스 감지 시스템 : 산업현장에서의 심각한 재해를 가져올 수 있는 가스 사고에 대해 센서 노드를 통한 신속한 대응 ○ JENNIC의 Commercial Building Automation : Intelligent 빌딩 곳곳에 설치된 센서 노드들은 실시간으로 연기, 화재 발생위치, 환풍, 조도, 온도 등을 센싱하여 보다 쾌적하고 안전하게 빌딩을 유지 ○ 일리노이 대학의 스마트 벽돌 : 벽돌 안에 들어가는 칩을 이용해 기울기, 진동, 습도 등의 정보 제공 ○ Intel의 진동 모니터링 : 무선 센서 네트워크를 이용, 반도체 제작 장비의 상태 감시 ○ Savi Technology의 CubeInfo : 콘크리트 벽돌에 태그를 부착해 벽돌의 품질 검사를 원활히 수행할 수 있도록 시스템 구축 o 미국 Geo-Fencing Service : Geo-Fencing은 공간경제 트리거로 일정 지역 이탈 방지 및 출입을 감지하는 역할을 수행함, 미국에서 지하 가스 파이프라인 파손으로 인한 대형 사고를 막기 위한 Crossbow

	사의 솔루션으로 BP사의 gas pipelins에 구 출(그림 5-51)[117] o 스위스 The SensorScope Project : 스위스 로잔 연방 공과 대학에서 long-running 시스템을 통해, 실제 배치의 제약을 이해하기 위한 프로젝트로 빌딩자동화 어플리케이션의 상업화 및 WAN의 개념을 제공, EPFL 캠퍼스 건물 내에 빛, 온도, 음향 등의 다양한 센서가 장착된 motefm 설치하였으며, 센서보드의 혼합으로 노드를 구성[117]



(그림 5-50) 무선 농작물 모니터링 시스템 구성도

<출처 : 파이토크사 홈페이지>



(그림 5-51) Geo-Fencing 서비스의 구동예제

<출처 : Wiless Sensor Network, (주)유비알에프, 2007>

다음 [표 5-18]은 그 밖의 국외 u-City 특징 및 현황을 나타낸 것이다.

[표 5-18] 국외 u-City 특징 및 현황[151]

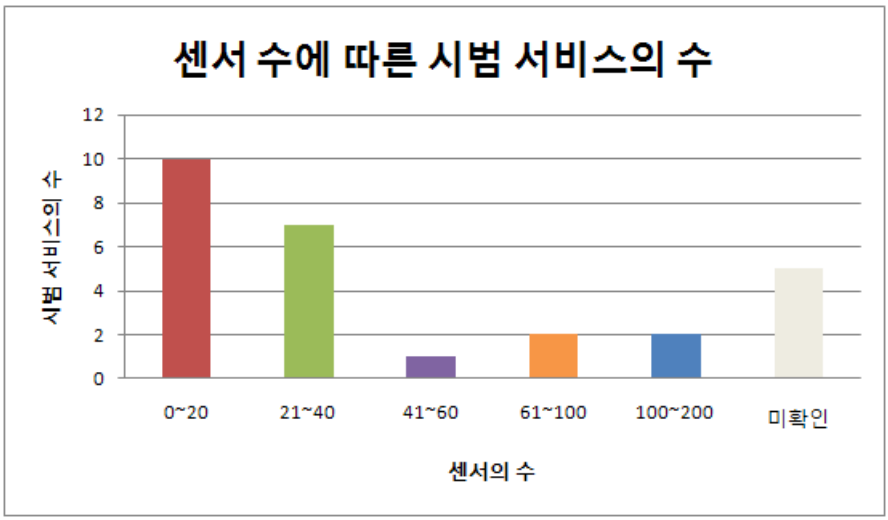
u-City	사 업 대 상	특 징
홍콩 Cyber City	금융, 무역, 광고, 통신	멀티미디어 관련 기업과 전문 인재 및 설비를 집중 유치, 세계적인 통신 기반 시설과 멀티미디어, 하이테크 기반으로 이루어진 기관들의 집합체
핀란드 헬싱키	초고속 통신망, 지리정보, 웹진 서비스 포털 서비스	민관이 개발주체 및 관련 연구기관으로써 학교도 사업에 참여
덴마크 u-City	3D 위치기반 모바일 통신, 지리정보 서비스, 교육솔루션 서비스	Living Lab이라는 연구실 개념화를 통해 일반인들이 원하는 주거환경을 수용하고 도시방향을 제시
독일 퀠른 Media Park	병원, 미디어파크, KOMED, House, Cinedom, 뮤지타워	50% 이상의 건물이 공모에 의해 건설 ,유선통신망 위주의 구축
싱가포르	의학, 문학, 미디어 허브	아시아 최고의 물류와 금융 인프라, 다국적 기업의 아·태평양 지부가 대부분 위치
말레이시아	초고속 통신망, 인적자원 투입관리	학생들의 벤처 기업 창업을 위한 사이버 인큐베이터 건설, Project Monitoring System 운영
일본 오카야마	초고속 정보통신망, 네트워크 운용 관리	네트워크 기반 확충으로 지역통합 및 발전 추진, 고속도로망과 물류 인프라의 완비
중국 종관춘	전자상가, 과학촌, 정보산업단지	국가차원의 중관춘 클러스터 시작, 산, 학, 관의 협력에 의한 첨단산업 개발이나 벤처 육성
UAE 두바이	포털 서비스, 부동산, 창업, IT 서비스	도시계획 하에 기능별 인프라 구축 도시, 미디어산업 도시, Knowledge Village 개발

제 3 절 u-City 시범 서비스 크기 및 센서의 수 통계

1. u-City 센서의 수에 따른 시범 서비스의 수

각 u-City 시범 시버스에서 사용되는 센서의 개수에 따라 국내 u-City 시범 서비스의 수를 알아보았다. 국내 19 사이트, 국외 8사이트를 대상으로 사용되는 센서의 수가 비교적 정확한 u-City 시범 서비스 총 27개를 대상으로 하였다.

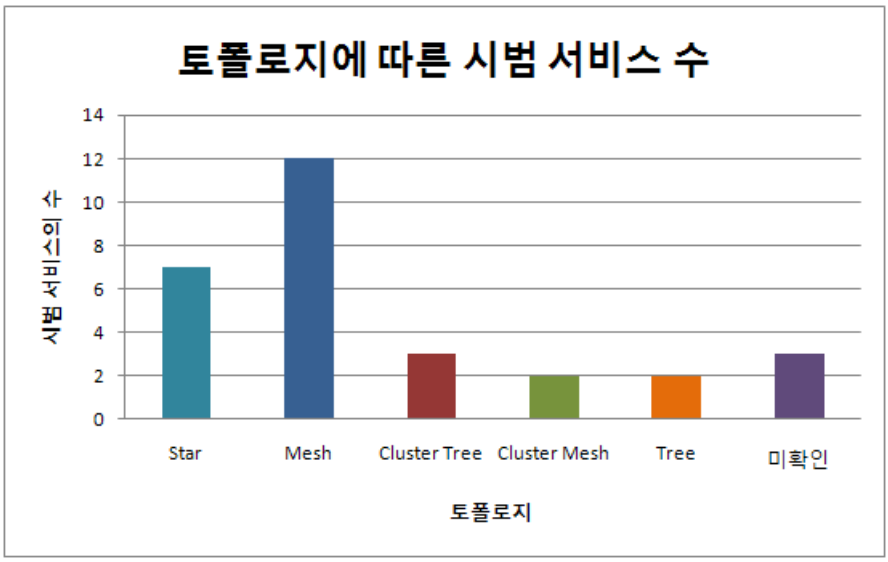
통계 결과 대부분 100개 이하의 센서로 서비스가 이루어지고 있으며, 센서의 수가 21개에서 40개 사이의 시범 서비스가 가장 많았다. 시범 서비스 중 4개(홈 네트워크, 무인 감시 시스템, u-주차장, u-울릉도독도 재난 재해 조기 예보 시스템)는 서비스가 이루어지는 장소의 크기가 유동적이기 때문에 정확한 센서의 수를 파악할 수 없었다.



(그림 5-50) 센서 수에 따른 시범 서비스의 수

2. 토폴로지에 따른 시범 서비스의 수

(그림 5-51)은 u-City 시범서비스에서 사용되는 토폴로지에 따라서 서비스를 분류한 것이다. u-City 시범 서비스의 토폴로지로 메시 토폴로지가 가장 많이 사용되며, 건설현장 관리 시스템과 혈액 및 항암제 관리 시스템은 스타 토폴로지와 메시 토폴로지 모두 사용된다.



(그림 5-51) 토폴로지에 따른 시범 서비스의 수

3. 시범 서비스의 토폴로지와 센서의 수

[표 5-19]는 네트워크 토폴로지에 따른 시범 서비스의 수와 각 시범 서비스마다 사용되는 센서의 수를 나타낸 것이다. 대부분의 서비스가 메시 토폴로지의 형태로 구성이 되었으며 건설 현장 관리 시스템처럼 한 서비스 안에 2가지의 토폴로지가 같이 사용된 경우도 있다. 서비스 구성 지역이 좁은 경우에는 비교적 센서 개수를 분명하게 가늠할 수 있으나 서비스의 지역이 불분명한 곳은 정확한 센서의 수를 알 수 없었다.

[표 5-19] 토폴로지에 따른 시범 서비스의 수와 사용되는 센서의 수

토폴로지	개수	u-City 시범 서비스	사용된 센서 수
스타	7	건설현장 관리 시스템(배터리사용)	40
		교량모니터링	28
		스키장 사각지대 안전 관리 시스템	21
		홈 네트워크	n/a
		혈액 및 항암제 관리 시스템	20
		Lagrge-scale Campus of EPFL	97
		Plaine Morte	13
메시	12	건설현장 관리 시스템(각각의 센서노드에 전원공급)	40
		기상/해양 관측 시범망 구축 및 시범 서비스	13
		도시기반시설 모니터링 시스템	23
		무인감시센서네트워크	n/a
		터널 관리 서비스	46
		U-캠퍼스	n/a
		혈액 및 항암제 관리 시스템	20
		Morges	6
		Gé né p	16
		Grand St. Bernard	17
		Wannegrat	20
		Outdoor testbed Campus of EPFL	10
클러스터 트리	3	지하수 모니터링 시스템	12
		농산물재배관리시스템	27
		U-주차관리서비스	n/a
클러스터 메시	2	USN 기반의 식수원 관리 시스템	17
		하천 생태복원 모니터링 시스템 구성도	105
트리	2	USN 기반의 문화재관리 시스템	27
		U-울릉도, 독도 재난, 재해, 조기예보시스템	n/a
	3	초등학교	149
		상수도관 망 관리	22
		미국 캘리포니아 Golden Gate Bridge 구조물 상태 모니터링	200
합	29		

제 4 절 u-City 서비스 공격 및 보안

1. u-City 보안 고려 사항

u-City는 국가 균형 발전을 위한 신도시 개발 모델로써 기존의 복잡하고 다양한 도시 문제를 해결하기 위해 u-City 서비스를 도입하였다. 이러한 u-City 서비스가 제대로 제공되기 위해서는 편리함만을 강조하는 것이 아니라 u-City 환경에서의 보안 취약점들까지 고려하는 것이 중요하다. 일반적으로 u-City는 기존의 도시운영에 비해 정보 시스템에 대한 의존도가 높기 때문에 도시 설계 시 정보 보호 부분에 대한 선행적인 이해가 필요하다.[155]

u-City 서비스 환경에서의 보안 취약점은 다음과 같다[156].

- o 불법 도청의 위험 : 인가되지 않은 노드를 이용하여 개인 정보를 침해할 수 있고 자신이 필요한 정보를 가져갈 수 있음.
- o 통신 간 트래픽 분석 : 센싱 되는 데이터의 트래픽 분석으로 센서 노드의 위치를 추적 가능.
- o 악의적인 의도의 스푸핑 공격 : 노드들에게 거짓된 정보를 전달 가능.
- o 서비스 거부 공격 : 악의적인 목적을 가진 노드가 특정 노드에게 데이터가 집중되도록 함으로써 노드가 정상적으로 동작 방해.

2. u-City 시범 서비스 공격 유형 및 키 관리 기법

u-City 센서 네트워크에서 예상 가능한 공격 유형에서 물리 계층에는 부채널 공격, 도·감청, Rogue node, Rogue Sensor, 신호방행 공격, 배터리 소진 공격이 있고, 논리 계층에는 도·감청, IP 스푸핑, DoS, 바이러스, 트로이 목마, 웜, 악성코드, 라우팅 공격이 있으며, 컨텍스트 계층에는 메시지 위·변조 공격 등이 있다[125].

본 보고서에서 조사한 u-City 시범 서비스 중에서 홈 네트워크를 제외한 대

부분의 시범 서비스들은 서비스 제공 방법 및 활용에만 중점을 두었기에 보안 사항을 고려하지 않았다. 그래서 본 보고서에서는 각 시범 서비스에서 발생 가능한 공격 유형을 파악하여 사용 가능한 키 관리 기법을 정리하였다.

[표 5-20]는 u-City 시범 서비스에 대하여 일어날 수 있는 공격 유형을 정리하고 시범 서비스의 보안 여부를 파악 하여 보안을 위한 키 관리 기법을 정리한 것이다. 본 보고서에서 조사한 시범 서비스 결과 홈 네트워크를 제외한 다른 시범 서비스에서 보안에 관련된 내용을 확인 할 수 없었다.

[표 5-20] 시범 서비스의 공격 유형 및 보안

u-City 시범 서비스	공격 유형	보안 적용 여부	사용 가능한 키 관리 기법
건설 현장 관리 시스템	센서 파손・유실・도난, 부채널 공격	n/a	Pairwise 키, 랜덤 Pairwise 키, q-합성수, SPINS, LEAP
교량모니터링	Rogue Node, 데이터 위・변조, 불법접근, 해킹, DoS, 라우팅 공격	n/a	Master 키, SPINS, Pairwise 키, 랜덤 Pairwise 키
홈 네트워크	해킹, 악성코드, 웜, 바이러스, DoS, 도・감청	○	Master 키, Pairwise 키, 랜덤 Pairwise 키, q-합성수, multi-path, SPINS
혈액 및 항암제 관리 시스템	데이터 위・변조, 불법접근, 해킹, DoS, Privacy	n/a	Master 키, Pairwise 키, 랜덤 Pairwise 키, q-합성수, multi-path, SPINS
USN 기반의 기상/해양 관측 시범망 구축 및 시범 서비스	부 채널 공격, 도・감청,	n/a	q-합성수, 랜덤 Pairwise 키, LEAP, multi-path

도시기반시설 모니터링 시스템	도청, DoS, 데이터 위・변조, Bogus 센서, 부채널 공격	n/a	q-합성수, 랜덤 Pairwise 키, LEAP, multi-path
무인 감시 센서 네트워크	도청, DoS, 데이터 위・변조, Bogus 센서, 부채널 공격	n/a	q-합성수, 랜덤 Pairwise 키, LEAP, multi-path
지하수 모니터링 시스템	데이터 위・변조	n/a	그룹 키, Pairwise 키, 랜덤 Pairwise 키, multi-path
농산물 재배 관리시스템	노드 탈취, 데이터 위・변조	n/a	그룹 키, Pairwise 키, 랜덤 Pairwise 키, multi-path
U-주자관리서비스	도청, 데이터 위・변조, 센서 탈취	n/a	그룹 키, Pairwise 키, 랜덤 Pairwise 키, multi-path
USN 기반의 식수원 관리 시스템	도청, 데이터 위・변조	n/a	그룹 키, q-합성수, 랜덤 Pairwise키, LEAP, multi-path
하천 생태복원 모니터링 시스템 구성도	도청, 데이터 위・변조	n/a	그룹 키, q-합성수, 랜덤 Pairwise키, LEAP, multi-path
USN 기반의 문화재관리 시스템	부 채널 공격, 데이터 위・변조	n/a	multi-path, Pairwise 키, 랜덤 Pairwise 키
U-울릉도, 독도 재난, 재해, 조기예보시스템	데이터 위・변조, 서비스 거부 공격, 라우팅 공격	n/a	multi-path, Pairwise 키, 랜덤 Pairwise 키

제 6 장 네트워크 형태별 키 관리 모델

본 장에서는 위에서 조사, 분석한 내용들을 바탕으로 USN 환경에서 키 관리 기술 적용 모델을 도출하였다. 1절에는 센서 네트워크 키 관리를 위한 보안 요구사항 및 키 관리 기법을 살펴보고, 기존에 있는 키 관리 기법 분류의 문제점을 지적하였다. 이러한 기존의 문제점을 극복하기 위해 센서 노드의 키 개수에 따른 네트워크 형태별 키 관리 모델을 도출하였다. 2절에는 새로 도출한 네트워크 형태별 공격 유형 및 키 관리 모델을 예시와 함께 자세히 설명한다. 분류는 실내와 실외, 대규모 네트워크와 소규모 네트워크, 센서 네트워크의 토폴로지를 기준으로 총 6가지 상황을 분류하였다. 이렇게 분류하여 각 케이스마다 USN 환경에 가장 적합한 키 관리 기법을 도출하였다.

제 1 절 개요

1. 센서 네트워크 키 관리를 위한 보안 요구사항 및 키 관리 기법

가. 센서 네트워크 키 관리 보안 요구 사항

센서 네트워크를 위한 키 관리를 위해서는 다음과 같은 사항을 고려해야 한다. 우선 센서 노드들이 랜덤하게 배치되기 때문에 네트워크 토폴로지 정보를 사전에 획득하기 어려우며, 센서 노드는 제한된 자원을 가지고 있기 때문에 경량화된 암호 알고리즘이 필요하다. 또한 센서 노드의 잘못된 동작과 에너지 소모 등으로 인해 센서 노드의 추가적 설치가 필요한 경우가 발생할 수 있기 때문에 키의 추가 및 제거가 용이해야 한다. 그리고 센서 네트워크가 실외에 설치될 경우 물리적 공격으로 인한 노트 탈취의 문제를 고려해야 하며 마지막으로 확장성도 함께 고려해야 한다.

센서 네트워크는 다양한 분야에 적용될 수 있기 때문에 기본적으로 알려진

다양한 공격 방법에 내성을 가져야 한다. 특히 공격자가 키 생성 및 분배 과정에서의 트래픽 분석을 통해 키의 생성 정보 및 네트워크 환경 정보를 쉽게 획득할 수 있기 때문에 중요한 메시지는 암호화를 통해 전달되어야 한다. 또한 물리적인 공격을 통해 탈취한 노드로부터 노드에 저장된 키의 정보, 네트워크 토폴로지, 베이스 스테이션의 위치 등과 같은 중요 정보를 획득할 수 있다. 따라서 센서 노드가 탈취되더라도 그 영향을 최소화하며 노드의 배치 이후에는 칩 디버깅을 통한 정보 획득이 불가능해야 한다[159].

나. 공격 유형과 키 관리 기법

[표 6-1]은 공격 유형과 그에 대응할 수 있는 키 관리 기법을 나타낸 표이다. 도청은 센서 노드 간 통신을 모니터링 함으로써 정보를 획득하는 공격이므로 데이터를 암호화해서 주고받음으로써 방어할 수 있다. 데이터 위변조 또한 특정 노드로부터 변조된 메시지를 받지 않도록 상호 노드 간 암호화 키를 설정하여 메시지를 인증하는 방법을 이용하여 방어할 수 있다. 따라서 각 노드마다 다른 키를 설립하는 Pairwise키나 Random Pairwise 키 기법 등을 이용 한다. Radom Pairwise 키는 Pairwise의 비효율적인 메모리 문제를 해결하면서 노드 캡쳐에 대한 저항성을 가지는 키 관리 기법으로 확장성이 있기 때문에 대규모의 네트워크에서도 사용할 수 있다. 서비스 거부 공격이나 라우팅 공격 등은 정상적인 노드로부터 전파 방해, 선택적 전달 등의 공격을 통해 다른 노드들에게 비정상적인 정보를 전달하는 방식이다. 이 경우 공격자가 아닌 정상적인 노드만이 네트워크에 참여하는 방식을 사용한다. 또한 물리적인 공격으로 인해 노드가 탈취되었을 경우 이를 대체할 노드 추가가 용이한 확장성이 있는 키 관리 방법을 선택할 수 있다. 라우팅 공격의 경우에는 키 관리 기법 이외에도 LEAP를 사용하면 HELLO flood 공격과 Wormhole 공격을 제외한 대부분의 외부 공격에 내성을 가지고 있기 때문에 공격을 막을 수 있다[159].

마스터 키 관리 기법은 마스터 키를 이용해 Pairwise키를 생성하고 사용한 마스터 키를 주기적으로 교체하는 방법을 이용하여 공격을 막을 수 있다. 하

지만 마스터 키 관리 기법은 공격자가 마스터 키를 교체하기 전에 노드를 탈취할 수 있으며, 이 경우에는 공격자가 센서 네트워크에 사용되는 모든 Pairwise 키를 알 수 있기 때문에 노드 탈취에 약하다는 단점이 있다.

[표 6-1] 공격 유형과 키 관리 기법 특징

키의 사전 분배	공격	특징
마스터 키		o 센서 네트워크를 구성하고 있는 모든 센서 노드가 단일키를 사용 o 단일키 노출 시 전체 센서 노드의 키가 노출이 되므로 소규모 네트워크에 적합함
Pairwise 키	도청 데이터위변조	o 모든 센서 노드와 키를 설립하는 방식 o 한 노드가 노출이 되어도 전체 네트워크에 미치는 영향이 적음 o 센서 노드의 제한된 자원으로 인해 소규모 네트워크에 적합
q-합성수 랜덤 키	데이터위변조 DoS 공격 라우팅 공격	o 한 노드가 공격자에게 노출이 되어도 센서 네트워크 내의 다른 통신 내용이 공격자에게 노출되는 것을 보안 o 공격자는 두 노드 사이에 사용된 q개의 공통 키들을 모두 알고 있어야만 도청이 가능함 o 두 노드 사이의 키를 인접한 다른 노드가 가질 수 있음.
Multi-path 키	도청 물리적 공격	o 기본적인 세션 키 설정 후 독립적인 경로를 통해 새로운 세션 키를 생성 o 키가 노출되어도 전체 네트워크에 미치는 영향이 적음 o 중간 노드의 신뢰가 있어야 함.

랜덤 Pairwise 키	데이터위변조 DoS 공격 라우팅 공격	o 불필요한 메모리 사용문제를 해결하면서 키의 저항성을 가짐 o 메모리의 효율적인 사용으로 인해 확장성을 가지면서 큰 규모의 네트워크 지원이 가능하다. o 베이스 스테이션이 없이도 손상된 노드를 감지하여 취소할 수 있음 o 노드 캡쳐 및 물리적 공격으로 인한 노드의 탈퇴 등에 빠른 회복력을 가짐

2. 기존 키 관리 기법 분류

가. 침해 유형에 따른 분류

USN 네트워크에서 보안 위협을 해결하기 위해 제시되는 보안 요구사항에 따라 키 관리 기법을 분류 하였다. 보안 요구 사항에 맞는 보안 위협에 대해서 대응이 가능하지만 지속적으로 추가되는 요구 사항에 대한 분석과 키 관리 기법의 적용 여부에 대한 명확한 분석이 필요하다.

[표 6-2] 침해 유형에 따른 분류

침해 유형	공격 종류	키 관리 기법
기밀성	도청, 노드 탈취 스누핑, 트래픽 분석	Multi-path, Pairwise, SPINS
익명성	도청, 데이터 위변조	Multi-path, Pairwise
무결성	데이터 위변조	Pairwise 키
인증성	노드 탈취, 라우팅 공격	Multi-path, Pairwise, SPINS

나. 수동/능동적 공격에 따른 분류

노드 사이의 키를 도청하거나 노드 간 전송되는 데이터의 특성을 파악하기만 하는 수준의 수동적인 공격과 시스템의 취약점을 적극적으로 이용하여 데이터의 정보를 변조하고 위장하여 공격의 목적을 달성하려는 시도의 능동적 공격으로 공격 유형을 분류할 수 있다. 수동적 공격의 관리가 능동적 관리보다 용이하며 공격이 변할 때마다 키 관리 형태가 계속 변한다는 특징이 있다.

[표 6-3] 수동/능동적 공격에 따른 분류

공격분류	공격 종류	키 관리 기법
수동적 공격	도청, 스누핑, 트래픽 분석	q-합성수, Pairwise키, Multi-path
능동적 공격	노드 캡쳐, DoS, 라우팅 공격 데이터 위변조, 부채널 공격 서비스 거부	Multi-path, Random Pairwise 키, SPINS

다. 외부자/내부자 공격에 따른 분류

Chris Karlof가 제시한 2가지 공격 모델 중의 하나로 외부자/내부자 공격으로 공격 유형을 분류하였다. 공격 초기에 외부자 공격만 있다고 가정할 경우 외부자 공격을 차단하는 방식을 이용하면 내부자 공격의 피해를 최소화 할 수 있다. 하지만 네트워크 내에서 내부자 공격 자체에 대한 탐지와 공격자 분석이 어려울 수 있다.

[표 6-4] 외부자/내부자 공격에 따른 분류

공격분류	공격종류	키 관리 기법
외부자 공격	도청, 데이터위변조	q-합성수, Multi-path, Pairwise
내부자 공격	노드캡쳐, 라우팅 공격	Multi-path, Random Pairwise

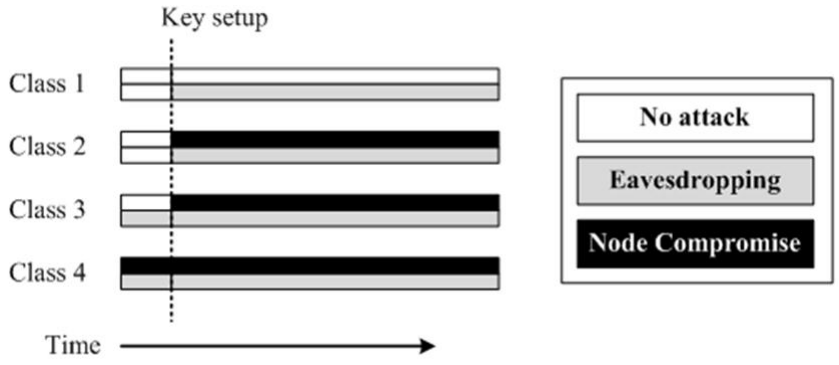
3. 기존 키 관리 기법 분류의 문제점

USN 환경에서 위협적인 공격들을 방어하기 위해 다양한 키 관리 기법들을 적용한다. 이러한 키 관리 기법을 보다 쉽고 편리하게 적용하기 위해서 이미 다양한 방법으로 공격 유형을 분류하였다. 우선 USN 네트워크에서 보안 위협을 해결하기 위해 제시되는 보안 요구 사항에 따라 키 관리 기법을 분류할 수 있다. 즉 기밀성, 익명성, 무결성, 인증성과 같이 침해 유형에 따라 분류하는 것이다. 또한 정보를 도청하거나 데이터 파악 수준의 수동적인 공격과 시스템의 취약점을 적극 이용하는 능동적 공격으로 분류하는 방법이 있고, Chris Karlof가 제시한 공격모델 중의 하나로 외부자/내부자 공격으로 공격 유형을 분류하는 방법이 있다.

USN 환경에서는 위와 같이 기존의 공격유형을 분류한 방법을 적용하여 키 관리를 하기에 문제점이 존재한다. USN 네트워크에서 임의의 공격자가 공격을 할 경우 다양한 공격 유형 중에서 특정한 경우에만 위반되는 것이 아니기 때문에 공격자가 한 가지 공격을 한 경우라도 여러 기준이 동시에 위반될 확률이 높다. 예를 들어 침해 유형으로 나뉜 USN 환경이 있다고 가정하자. 이때 공격자가 기밀성을 위협하기 위해 노드 탈취 공격을 시도할 경우 이 공격으로 인해 기밀성만 위협받는 것이 아니라 익명성, 인증성도 동시에 위협을 받게 된다. 수동/능동적 공격에 따른 분류에서도 처음에는 수동적 공격을 시도하다가 능동적 공격으로 바뀔 수 있고, 외부자/내부자 공격에서도 외부자

공격을 시도하다가 내부자 공격으로 공격 형태가 바뀔 수 있다. 따라서 위와 같이 한 가지 기준으로만 분류하여 공격 유형에 따른 키 관리 기법을 적용하기에 효율적이지 않다.

또한 International Telecommunication Union(ITU)의 Temporary Document(TD)에서 제시한 키 관리 클래스 분류 역시 USN 환경에서 공격 유형별 키 관리 기법을 적용하기에 부적절하다고 판단된다. 여기에서 제시한 방법은 키 셋업의 전과 후에 공격하는 방법을 클래스별로 1~4까지 분류하였다. 다시 말하자면 공격자가 키 셋업 이전에 공격하는 것과 키 셋업 이후에 공격하는 것으로 분류되고, 그리고 각각의 경우에 어떤 공격을 하는지에 대해 클래스 별로 구분한 것이다.



(그림 6-1) 키 관리 클래스

o Class 1 : 공격자가 Key setup 이후에 도청 공격함
o Class 2 : 공격자가 Key setup 이후에 도청하거나 Node Compromise에 대해 노드 capture와 reprogram함
o Class 3 : 공격자가 Key setup 전, 노드 배치 될 때 도청 공격함.
o Class 4 : 공격자가 Key setup 전, 노드 배치 될 때 도청과 Node Compromise 함. 가장 높은 레벨의 강력한 공격임.

하지만 USN 환경을 구축하기 위해 네트워크 구조를 만들 때 어느 클래스

에 해당하는 구조인지 미리 알 수 없다. 따라서 이러한 방법으로 키 관리 기법을 적용하기에 효율적이지 않다.

또한 기존의 분류법에 따라 USN 환경에서 키를 관리 한다면 어떤 유형의 공격을 받을 것인지 미리 알 수 없기 때문에 다양한 방법으로 방어를 하게 된다. 따라서 저 비용으로 막을 수 있는 공격도 많은 비용이 소모되는 키 관리로 방어하게 되는 비효율적인 상황이 발생 할 수 있다. 그러므로 USN의 환경과 센서 노드의 제약 사항 등을 고려하여 USN에서의 공격을 키 관리기법을 사용하여 효율적으로 방어 할 수 있는 분류 기법이 필요하다.

4. 센서 노드의 키 개수에 따른 네트워크 형태별 키 관리 이유

본 보고서에서는 센서 네트워크의 규모와 센서 네트워크가 배치되는 장소 및 센서 노드가 가지는 키의 개수를 고려하여 네트워크의 형태를 분류하고, 각 조건에서 발생할 수 있는 공격 유형을 정의한 후에 공격에 대응할 수 있는 키 관리 기법을 제시하고자 한다.

USN 환경은 다양한 서비스를 포함하고 있으므로 이동통신과 같이 특정한 하나의 네트워크 구조를 가지고 있지 않으며 서비스에 따라 다양한 형태의 네트워크 구조를 가질 수 있다. 따라서 IEEE 802.15.4에서 지원하는 USN 환경에서 사용되는 대표적인 네트워크 토폴로지인 스타 토폴로지, 메시 토폴로지, 클러스터 토폴로지로 구분 하고, 센서 네트워크의 규모와 설치되는 장소를 고려한다. 이에 따라 다양한 케이스가 발생하며 해당 케이스마다 공격 유형을 더 세분화 하여 공격을 방어하기 위해 가장 효율적인 키 관리 기법으로 분류 하였다.

기존에 사용하였던 수동적, 능동적 공격에 따른 분류 방법, 보안 요구사항을 침해하는 공격 유형 분류 방법, 내부자, 외부자 공격에 따른 분류 방법을 사용할 경우 복합적인 문제로 인해 공격 유형을 임의의 한 가지 분류 방법으로 구분 짓기에 어렵다는 문제점이 있다. 이러한 문제를 해결하기 위해 센서 네트워크를 크기와 장소 및 센서 노드가 가지는 키의 개수를 고려하여 네트워크 토폴로지 형태로 분류할 경우 각 케이스마다 공격의 효과가 더 잘 나타나고

발생 빈도수가 많은 공격 유형들을 추출할 수 있기 때문에 센서 네트워크의 보안 능력이 더 향상 된다.

또한 센서 네트워크는 공격 위협을 조기에 찾아내고 방지할 수 있는 보안 관리와 서비스 거부 공격에 충분히 감내할 수 있는 구조가 필수적이며, 이러한 보안 개념이 설계 시점부터 반영되어야 한다. 따라서 네트워크 형태 별로 공격 유형을 분류하게 되면 구축하고자 하는 네트워크가 어떤 공격에 취약한지 알 수 있고 적절한 보안 방법을 적용할 수 있기 때문에 키 관리 기법을 적용할 경우에도 센서 노드의 자원을 효율적으로 사용할 수 있다.

제 2 절 네트워크 형태별 공격 유형 및 키 관리 모델 도출

다양한 센서 네트워크의 많은 특성으로 인해 키 분배 기법 모델을 도출해야 한다. 그렇지 않으면 보안 성능이 낮아지게 된다. 이에 본 보고서에서는 아래와 같이 센서 네트워크 규모와 설치 장소, 센서 노드가 가지는 키의 개수, 그리고 네트워크 토폴로지(Network Topology) 형태를 기반으로 하여, USN 환경에서 공격에 대한 방어를 위해 적합한 키 관리 기법을 적용 할 수 있도록 새로운 분류 기준을 제시한다. [표 6-5]는 위의 사항을 보기 쉽게 간략히 정리한 것이다.

기본적으로 모든 케이스에서 도청, 데이터 위변조, 서비스 거부, 라우팅 공격, 물리적 공격이 발생 할 수 있다. 하지만 센서 네트워크의 규모와 설치 장소, 네트워크 특성 및 구조 형태, 센서 노드가 가지는 키의 개수 등의 특성을 고려하여 보다 더 공격당하기 쉬운 공격 유형을 정리하고 그에 따른 보안 요구 사항을 적용한 적합한 키 관리 기법을 도출하였다.

공격에 대해서 센서 노드에게 인위적으로 물리적 공격을 가하지 않는다고 가정하면 실내보다는 실외에서 물리적 공격이 발생할 확률이 높다. 왜냐하면 자연 재해와 같은 홍수, 번개, 지진 등으로 인해 센서 노드에게 물리적 공격이 가해질 확률이 높기 때문이다.

1. 분류 기준에 따른 공격 및 키 관리

가. 실내외 실외

우선 크게 센서 네트워크가 설치되는 장소로 실내와 실외를 구분한다.

실내 응용 서비스는 USN 센서 노드의 설치 위치가 특정 건물 내부에 설치되며 센서 네트워크의 구축 및 관리가 용이하고 센싱 및 제어 등에 있어 신뢰성을 확보할 수 있다. 대표적인 예로는 스마트 빌딩 서비스, 공공안전 서비스, 창고관리 서비스 등이 있다.

실내는 크기가 제한적인 장소이므로 센서 네트워크의 크기 및 토폴로지를 정의하지 않는다. 또한 실내는 건물 안이므로 건물 안에서 자체 방법 시스템이 작동 하는 것을 고려 할 때 노드 캡쳐(node compromise) 공격이 발생하기 어렵다고 할 수 있다. 그러므로 노드 캡쳐 공격을 당할 확률이 낮기에 노드 캡쳐 공격이 발생하지 않는다고 가정한다. 따라서 이러한 케이스처럼 제한된 크기와 네트워크 토폴로지와 상관없이 가장 효율적인 Pairwise 키 기법을 사용하여 공격에 방어 할 수 있다.

실외의 경우에는 센서 네트워크 내의 센서 노드가 가지는 키의 개수에 따라 소규모 네트워크와 대규모 네트워크로 구분한다. 실외 응용 서비스는 USN 센서 노드의 설치 위치가 건물 외부에 위치하며, 해양 목장 서비스, 가로등 관리 서비스, 상하수도 관리, 대기/악취 환경 모니터링 서비스에 이용할 수 있다. 이 서비스는 센서 네트워크 구축 및 관리에 있어서 외부 환경 요인에 따라 제약이 있으며 센싱 및 제어 등에 있어서 신뢰성을 확보가 어려울 경우가 있다.

나. 소규모와 대규모

본 보고서에서 소규모와 대규모 네트워크의 기준은 Blom의 Polynomial 기법을 바탕으로 한다. 기존 Polynomial 기반은 두 노드간의 직접적 키 셋업을 제공하나, λ 개까지의 안전만을 보장하기 때문에 그 이상의 노드가 캡쳐 될

경우에는 전체 시스템이 무너질 가능성이 있다. 따라서 본 보고서에서 제안한 사전 키 분배 프레임워크의 기본 요소로써 Polynomial 기법을 사용한다. 이것에 대한 자세한 것은 다음 장에서 설명한다.

여기서 센서 네트워크에서 한 센서 노드가 저장 할 수 있는 키의 수를 m이라고 하고, 계수(coefficient)의 비트 사이즈는 세션 키의 실제 사이즈라고 한다. 따라서 만약 센서 노드가 하나의 키만 공유한다면 Polynomial은 m-1 degree를 가질 수 있다. 상이한 센서 네트워크에서 센서 노드의 특성에 따라 센서 노드가 여러 키 값을 가질 수 있다. 그러나 본 보고서의 프레임워크에서 우리는 센서 노드가 최소 m개 키를 가질 수 있다고 가정한다. 만약 모든 센서 노드 내의 Polynomial의 차수가 t라면 $N_t \times (t+1) >= m$이 된다. 만약 N_t가 1보다 크면, t는 m보다 훨씬 작게 된다. 따라서 이 기법은 t값만큼 안전하다고 할 수 있다.

위의 내용에 의해 소규모 네트워크는 센서 네트워크 내에 존재하는 센서 노드의 수가 각 센서 노드가 보유할 수 있는 키의 개수인 m보다 작은 것이라고 정의한다. 이 상황에서, 전체 센서 네트워크가 하나의 그룹이 되고, 하나의 Polynomial instance가 각 노드에 Polynomial 부분정보를 부여하기 위해 존재한다. Polynomial의 차수는 m-1로 맞춰지게 된다. 센서 네트워크에 존재하는 노드의 숫자가 m 보다 작기 때문에, 노드가 캡쳐 되어도 Polynomial은 밝혀지지 않는다. 또한 모든 노드가 Polynomial instance에서 받은 Polynomial 부분정보를 갖게 되기 때문에, 어떤 노드쌍이라도 세션 키를 설정할 수 있다.

따라서 이러한 소규모 네트워크에서 토폴로지를 구분하는 것은 무의미하다고 볼 수 있으며, 이러한 소규모 네트워크에 가장 적합한 마스터 키를 이용하여 USN 공격을 방어 하도록 한다. 하지만 소규모라고 해서 하나의 마스터 키만 가지고 센서 네트워크를 보호하기에 무리가 있다. 그러므로 마스터 키를 주기적으로 교체하여 노드 캡쳐 공격에 대비해야 한다.

센서 네트워크가 보유하는 키의 개수보다 더 많은 센서 노드를 가지고 있는 대규모 네트워크에서는 센서 네트워크 토폴로지로 구분하여 적합한 키 관리 기법을 도출한다. 대규모 네트워크에서 많이 사용 하게 될 키 관리기법은 Random-pairwise key, q-Composite, Multi-path, Group key, LEAP이다. 이러

한 키 관리 기법에 사용될 키도 모두 Polynomial의 degree에 의해 바뀌게 된다.

다. 네트워크 형태

현재 센서 네트워크의 통신 계층 중에서 물리계층(PHP)과 매체접근제어계층(MAC)은 IEEE 802.15.1(블루투스), IEEE 802.15.4, IEEE 802.15.3a(초광대역통신(UWB, Ultra Wide Band)), 첩 신호 확산 스펙트럼(CSS, Chirp Spread Spectrum)등에 대한 표준화가 진행되어 있으나 기술의 발전에 따라 새로운 표준이 지속적으로 요구될 것이다. (IEEE 802.15.3, 3a, 3b 등은 고전송률 개인영역 무선통신(High Rate WPAN)관련규격) 센서 네트워크 계층에 대한 표준화는 IEEE 802.15.4 기반의 ZigBee 프로토콜 스택, 6LoWPAN(저전력 소모 개인영역 무선통신, IP over LoWPAN)등이 대표적이지만 유수의 기관들에서 아직도 많은 연구가 진행되고 있다. 본 보고서에서는IEEE 802.15.4에서 지원되는 네트워크 토폴로지(스타 토폴로지, 메시 토폴로지, 클러스터 트리 토폴로지, 클러스터 메시 토폴로지) 위주로 설명한다[73].

USN 환경에서 사용되는 대표적인 네트워크 토폴로지(IEEE 802.15.4에서 지원하는 네트워크 토폴로지 형태)는 다음과 같은 4가지로 스타 토폴로지, 메시 토폴로지, 클러스터 트리 토폴로지, 클러스터 메시 토폴로지가 있다. 이러한 토폴로지를 이용하여 총 4가지 케이스의 센서 네트워크를 형성하여 해당 케이스에 따라 적합한 키 관리 기법을 도출한다.

첫 번째는 교량모니터링과 같이 스타 토폴로지를 사용하는 케이스이고, 두 번째는 도시 기반 시설 모니터링 시스템이나 터널 관리 시스템과 같이 메시 토포롤지를 사용하는 케이스이다. 세 번째는 지하수 모니터링 시스템과 농산물 재배관리 등의 클러스터 트리 토폴로지를 사용하는 케이스이며 마지막 네 번째는 식수원 관리 시스템과 하천 생태복원 모니터링 시스템과 같은 클러스터 메시 구조를 사용하는 케이스로 구분한다.

스타 토폴로지를 사용하는 경우 Polynomial 기법을 사용한다. 센서 네트워크 내의 각 노드는 그룹을 형성한다. 즉, n 센서 노드가 센서 네트워크에 존재

한다면 n 그룹을 가지는 것이다. 이때 Polynomial의 degree는 0이며, Polynomial은 반드시 상수를 포함한다. 따라서 각 그룹마다 다른 Polynomial이 주어지므로 스타 토폴로지내의 각 노드는 다른 키가 주어지는 것이다.

메시 토폴로지를 사용하는 경우 스타 토폴로지에 비해 여러 개의 라우팅 경로가 존재하므로 일부 노드에 문제가 생기거나 필요에 의해 경로를 바꿀 수 있는 멀티 홉 통신이 가능하므로 Multi-path 기법을 사용한다. 그리고 여러 경로를 위해 키링(key ring)으로부터 임의의 키를 받아서 노드들 사이에 임의의 pairwise key를 설정 할 수 있는 Random pairwise key 기법을 사용한다. 만약 더 강력한 보안을 원할 경우 Random Pairwise key 기법보다 더 강한 q-합성수 기법을 사용 할 수 있다.

클러스터 트리의 케이스에서는 스타 토폴로지의 단점을 개선하여 구성과 관리가 비교적 간단하면서도 넓은 범위를 지원 할 수 있지만, 각 노드 사이에 하나의 경로만 존재하게 된다. 또한 경로상의 노드 중 특히 코디네이터들 중 하나에 문제가 생기면 네트워크가 분할될 수 있다. 따라서 이러한 경로에 대한 키로 가장 안전한 기법이 q-Composite 기법이다. 노드가 키링(key ring)으로부터 랜덤하게 받아온 키들 중 q 개가 일치해야만 노드 사이의 경로가 생기므로 가장 적합한 기법이라고 할 수 있다. 그리고 클러스터의 보안을 더 강력하게 하기 위해 그룹 키 관리 기법을 사용한다. 그룹 키 기법은 그룹 키가 노출되면 해당 클러스터 전체가 위험하므로 클러스터 내에서 가장 신뢰할 수 있는 베이스 스테이션을 두어 클러스터 내의 노드를 관리하고 주기적으로 그룹 키의 변경이 요구된다.

마지막으로 클러스터 메시를 사용하는 케이스는 Random Pairwise key와 LEAP, Multi-path를 사용하도록 한다. 클러스터 메시의 경우 메시 토폴로지와 유사하며, 클러스터 트리 토폴로지의 단점을 개선할 수 있지만 상대적으로 네트워킹은 복잡해진다. 따라서 여러 경로를 위해 Random Pairwise key 기법을 사용한다. 특히 클러스터 구조를 가지고 있으므로, 개인키, pairwise 키, 그룹 키, 클러스터 키를 이용하여 여러 가지 전송 현태를 지원하는 LEAP 기법을 사용한다. LEAP는 한 노드가 공격을 당해도 그 노드에 인접한 다른 노드에게 피해를 최소한으로 해 주는 기법이다. 또한 여러 경로를 가지고 있으므로 데

이터를 여러 경로를 통해 송수신할 수 있는 Multi-path 기법을 사용할 수 있다.

센서 네트워크에 사용되는 각 토폴로지에 대해서 간략히 설명하면, 노드와 PAN coordinator 사이에 연결로 구성된 스타 토폴로지, coordinator까지 전달되기 위해서 다른 노드를 경유하는 트리토폴로지, 마스터 coordinator 없이 각 노드가 라우팅 하는 메시 토폴로지에 결합된 센서 노드로부터의 데이터를 목적지까지 전달하는 등의 구조를 가진다[98].

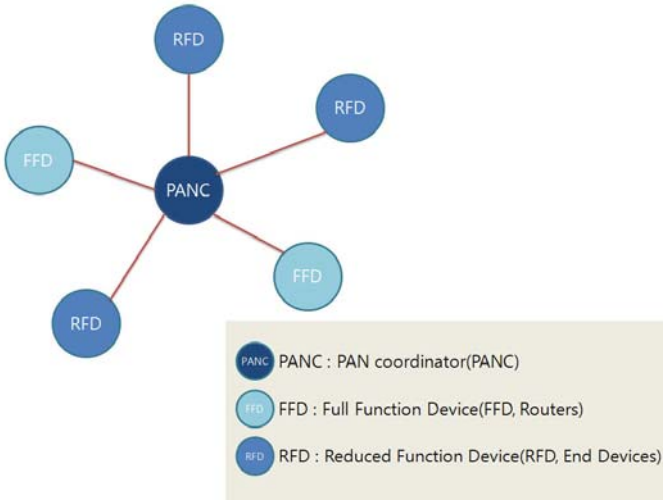
- o FFD(Full Function Device) : 큰 메모리, 큰 컴퓨팅 파워, 큰 배터리 또는 일반 전원을 갖으며, 모든 기능을 가지는 노드로 PAN Coordinator, Coordinator, 종단장치(End System)등 모든 기능을 가진다.
- o RFD(Reduced Function Device) : 작은 배터리, 작은 메모리, 제한된 컴퓨팅 파워를 갖으며 일부 기능만을 갖는 종단장치(End System)로만 동작할 수 있다.
- o PAN Coordinator : 개인영역통신망(PAN, Personal Area Network)을 구성하는데 필요한 대표 노드로 네트워크 전체를 구성하고 관리하는 역할을 하는 FFD이다. 일반적으로 배터리가 아닌 일반 전원을 공급받는다.
- o Coordinator(Cluster Head) : 작은 네트워크가 많이 모인 큰 네트워크에서 작은 네트워크를 구성하는 대표 노드로 종단장치(End System)의 정보를 받아 PAN Coordinator에게 데이터를 중계하는 역학을 한다. 배터리로 동작하는 FFD이다.

다음은 각 토폴로지에 대한 간략한 설명이다[78].

(1) 스타 토폴로지

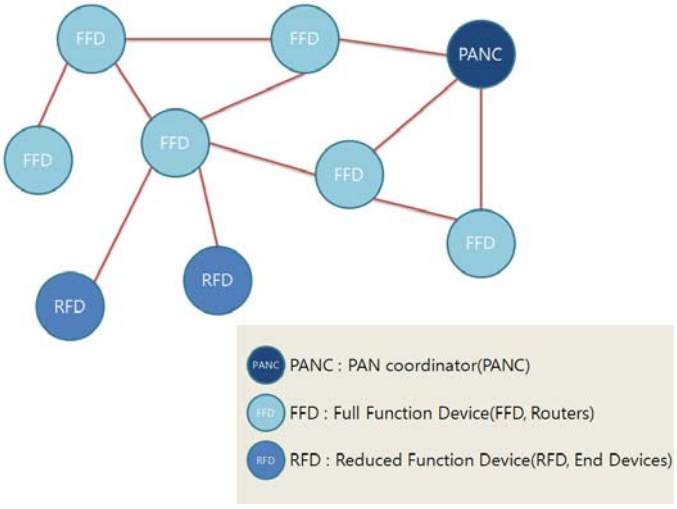
스타 토폴로지는 모든 센서 노드들이 중앙의 개인영역통신 중개기(PANC, PAN Coordinator)와 한 노드마다 통신을 하는 구조이다. 네트워크를 구성하고 센서 노드들의 관리나 라우팅이 간단하고 중앙의 PANC 노드를 중심으로

한 번의 통신 거리 내에 모든 노드들이 위치해있다. 그래서 PANC에 문제가 발생하면 모든 통신과 노드들이 위험해지며, PANC의 소모 전력이 높다.



(그림 6-2) 스타 토폴로지

(2) 메시 토폴로지

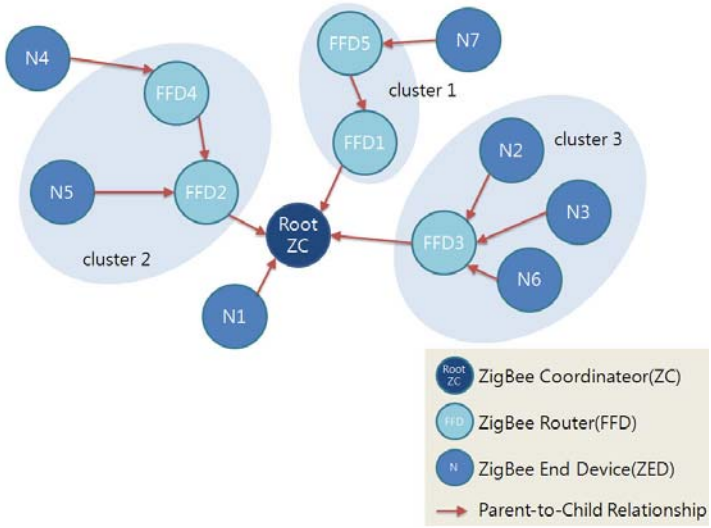


(그림 6-3) 메시 토폴로지

메시 토폴로지는 여러 개의 라우팅 경로가 존재하므로 일부 노드에 문제가 발생하여도 전체 네트워크 구조에 영향을 끼치지 않고 조건과 필요에 의해서 송수신 경로를 변경 할 수 있다. 또한 멀티 홉(Multi Hop) 통신이 가능하므로 스타 토폴로지를 사용할 수 있는 영역보다 더 넓은 지역에 적용할 수 있어서 많은 시범 서비스에 사용된다.

그러나 PANC(PAN Coordinator)와 FFD(Full Function Device)로 표시된 노드들은 다른 노드들의 데이터를 전달해 항상 동작하므로 전원 소모가 많고, 그렇기 때문에 배터리로 구동되는 경우에 네트워크의 수명도 줄어들게 된다.

(3) 클러스터 트리 토폴로지



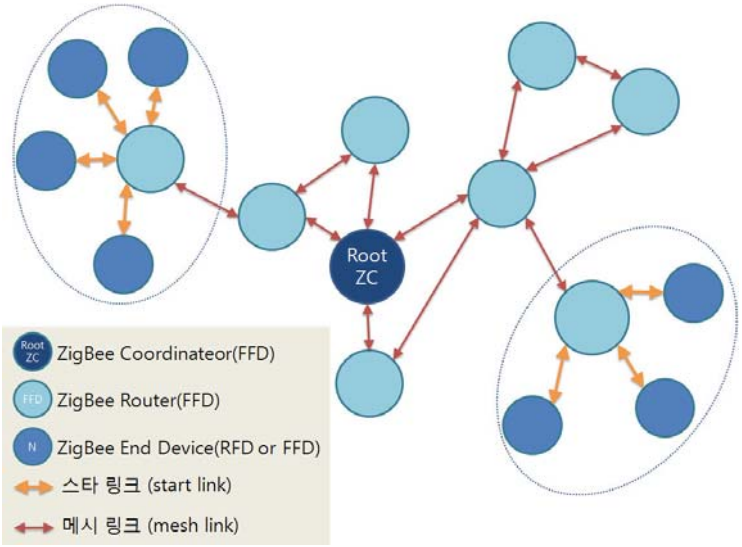
(그림 6-4) 클러스터 트리 토폴로지

클러스터 트리 토폴로지는 좁은 범위에서만 망을 구성하는 스타 토폴로지의 단점을 개선한 것으로 각각의 클러스터가 하나의 중심 노드를 중심으로 스타 구조를 취하면서 각 중심 노드끼리 트리 구조를 형성하는 구조이다. 이 구조에서 중심 노드 역할을 하는 노드를 클러스터 헤드(Cluster head)라고 부르기도 한다. 구성과 관리가 비교적 간편한 구조이므로 넓은 범위를 지원 할 수

있지만, 각 노드 사이에 하나의 경로만 존재하므로 경로상의 노드 중, 특히 코디네이터들 중 하나에 문제가 생기면 네트워크가 분할되는 단점이 있다. 그리고 코디네이터들은 라우팅을 위해 계속 동자가해야 하므로 소모 전력이 많고, 배터리를 사용할 경우 네트워크의 수명도 짧아진다. 이러한 클러스터 트리 토폴로지에서 사용되는 키 관리 기법에는 신뢰 가능한 베이스 스테이션을 통하여 이웃 센서 노드와 키를 교환하는 키 관리 방법을 사용할 수 있다.

(4) 클러스터 메시 토폴로지

클러스터 메시 토폴로지는 센서 노드들 사이에 하나의 경로만 존재하여 클러스터 헤드에 이상이 생기면 네트워크가 분할되는 단점을 개선한 구조로 기본적인 장단점은 클러스터 트리 토폴로지와 유사하다.



(그림 6-5) 클러스터 메시 토폴로지

다음 [표 6-5]는 위의 기준을 중심으로 총 6가지 케이스를 보여주고 있다. 각 케이스마다 위험이 큰 공격과 적합한 키 관리 기법, 그리고 그에 따른 보안 요구 사항과 예시를 간략히 정리하였다. 특히 Polynomial 기법은 모든 키 관리 기법을 아우르며 degree에 따라 Pairwise key 기법이나 Random Pairwise key 기법 등 다른 기법으로 사용하게 된다.

[표 6-5] 네트워크 형태별 키 관리 기법과 공격 및 요구사항

장소	크기	토폴로지	키 관리	공격	요구사항	시범서비스
실내	·	·	마스터 키	· 도청 · 데이터위변조	· 데이터암호화 · 데이터인증	· 홈 네트워크 · 빌딩 모니터링
실외	소규모	스타 메시	Blom's method Polynomial	· 데이터위변조 · 서비스거부 · 물리적 공격	· 데이터인증 · 노드상호인증 · 물리적 통제	· 터널 모니터링 · 도로관리 모니터링
	대규모	스타	Pairwise	· 데이터위변조 · 물리적 공격	· 데이터인증 · 물리적 통제	· 교량 모니터링
		메시	Polynomial Random	· 서비스거부 · 라우팅공격 · 물리적 공격	· 데이터암화 · 노드상호인증 · 노드포획에 대한 탄력성 · 물리적 통제	· 기상/해양 관측모니터링 · 도시기반시설 모니터링
		클러스터 트리	Polynomial Random-pairwise q-합성수 LEAP	· 데이터위변조 · 서비스거부 · 물리적 공격	· 데이터인증 · 노드상호인증 · 물리적 통제	· 지하수 모니터링 · 농산물 재배관리 시스템 · 주차관리 시스템
		클러스터 메시	Polynomial Random key q-합성수 LEAP	· 서비스거부 · 라우팅공격 · 물리적 공격	· 데이터암화 · 노드상호인증 · 노드포획에 대한 탄력성 · 물리적 통제	· 식수원 관리 시스템 · 하천 생태복원 모니터링 시스템

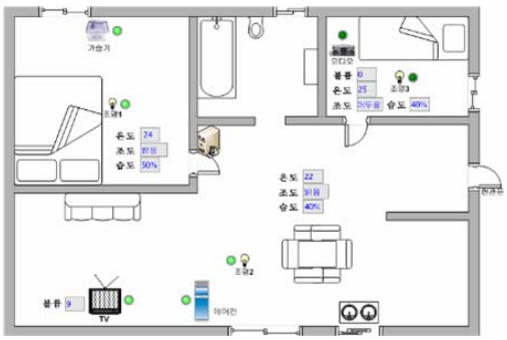
2. 해당 케이스에 따른 공격 유형 및 키 관리 기법

가. case 1 : 실내

(1) 환경

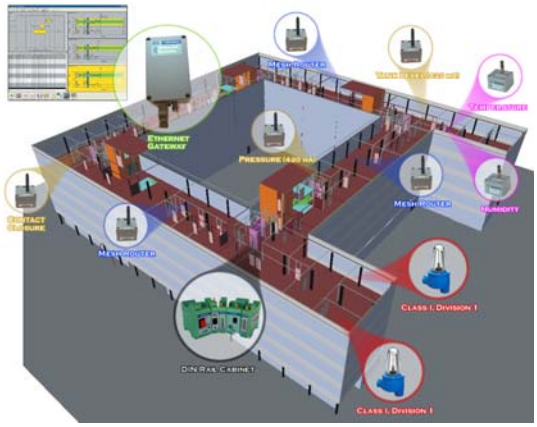
이 케이스는 USN 센서 네트워크를 설치 할 때 건물 안쪽인 실내에 설치하는 것이다. 실내는 이미 한정된 공간이고, 건물 자체의 방법 시스템에 의해서 센서 네트워크의 규모나 네트워크 토폴로지를 정하지 않고 자유롭게 사용하도록 한다. 따라서 센서 네트워크에 참여하는 노드의 수나 센서 노드가 보유하고 있는 키의 수가 일정하지 않고, 스타 토폴로지, 메시 토폴로지, 클러스터 트리 토폴로지, 클러스터 메시 토폴로지의 선택에 대한 제한이 없다고 할 수 있다.

이러한 케이스로는 홈 네트워크 또는 건물 모니터링 시스템 등이 대표적이다. (그림 6-6)은 홈 네트워크를 보여준다.

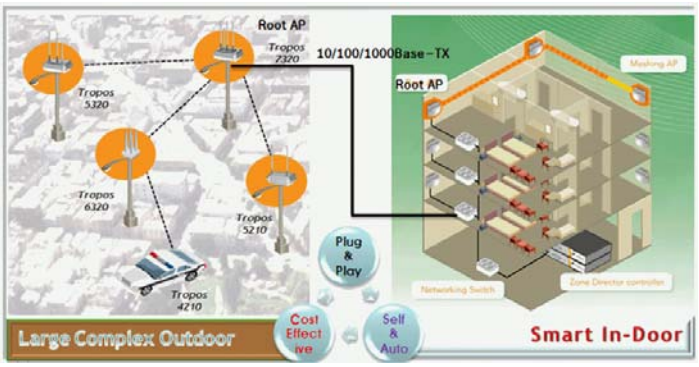


(그림 6-6) 홈 네트워크 [96]

아래 (그림 6-8)과 (그림 6-9)는 건물 내 설치된 메시 네트워크 구조와 건물 모니터링 시스템을 보여준다. 이처럼 건물 내의 벽과 천장 혹은 기둥 등에 센서 노드를 설치하여 서비스를 제공한다.



(그림 6-8) 건물 내 설치된 메시 네트워크 구조 [102]



(그림 6-9) 건물 모니터링[103]

(2) 공격 유형 및 요구사항

실내에 설치된 센서 네트워크는 실내라는 제한된 공간으로 인해서 통신 범위가 제한되어 있고 건물 내의 자체 방법 시스템 등을 통해서 노드 관리가 이루어지므로 이러한 환경에서 node compromise(capturing) 공격이 없다고 가정하는 것이다.

일반적으로 센서 노드들이 무선으로 데이터를 송수신 하므로 데이터에 대한 기밀성이 제공되지 않으면 도청을 당하기 쉽다. 도청을 방지 하기위해서 데이터를 암호화 하여 암호화된 데이터를 송·수신해야 하며, 데이터 전송 경로에

대한 암호화도 제공되어야 한다.

도청뿐만 아니라 데이터에 무결성이 제공되지 않으면 전송되는 데이터가 위조되거나 변조되어 전송 될 수 있으므로 송·수신 하는 데이터가 정당한 정보인지 확인하기 위한 인증도 필요하다.

(3) 키 관리 기법

위와 같이 노드 캡쳐로 인해 도청이나 데이터 위변조 공격을 당했을 때 마스터 키를 이용하여 센서 네트워크에 참여하고 있는 정상적인 센서 노드들의 모든 키를 빠르게 바꿔줘야 한다. 단일키를 사용하는 마스터 키 기법을 사용하기 위해서는 키 서버(key server)의 강력한 보안이 이루어 줘야 하며, 보안을 위해 주기적으로 키를 변경하여 센서 노드들에게 배포해야 한다. 이렇게 함으로써 키가 유출되었을 때에 유출된 키를 사용 할 수 없는 키로 만듦으로서 센서 네트워크의 보안성을 높일 수 있다.

다음은 실내에서 각 토폴로지마다 이러한 마스터 키 기법을 이용하여 키를 분배하는 방법이다.

- o 스타 토폴로지 : 중앙의 강력한 보안을 유지하는 PAN Coordinator(PAN coordinator : 개인영역통신 중재기) 센서 노드에서 다른 노드들에게 키를 배분하도록 한다.
- o 메시 토폴로지 : PAN Coordinator와 FFD(Full Function Device) 노드들을 통해 다른 노드들에게 마스터 키를 안전하고 정확하게 전달하도록 한다.
- o 클러스터 트리 토폴로지 : Root ZC(ZigBee Coordinator)로부터 각 클러스터 헤드(Cluster Head)에게 마스터 키를 전달하며, 클러스터 헤드는 자신이 속한 클러스터의 노드들에게 키를 전달한다.
- o 클러스터 메시 토폴로지 : 메시 링크에서는 메시 토폴로지와 같이, 스타 링크에서는 스타 토폴로지와 같이 키를 전달한다. 즉, ZigBee 코디네이터(FFD)에서 ZigBee Router(FFD)에게 키를 전달하고 클러스터를 이루고 있

는 클러스터의 FFD는 자신이 클러스터 내의 다른 노드들에게 키를 전달하는 것이다.

나. case 2 : 실외 - 소규모 네트워크

(1) 환경

이 케이스는 실외에서 소규모 네트워크로 설치된 것이다. 센서 네트워크 내에 참여하는 노드의 수가 각 센서 노드가 보유하는 키의 개수보다 적은 소규모 네트워크에서는 클러스터 토폴로지를 제외한 스타 토폴로지와 메시 토폴로지를 사용한다.

이러한 케이스로 터널 관리 시스템, 지능형 도로 관리시스템(Smart way System) 등과 같은 것이 있다. 아래 (그림 6-10)는 터널관리 시스템을 나타낸 것이다.

(그림 6-10) 터널관리 서비스 [101]

(2) 공격 유형 및 요구사항

소규모 네트워크임에도 불구하고 실외에 설치된 환경이므로 외부로부터 물리적 공격을 받기 싶다. 도로 모니터링과 같은 경우 교통사로와 같이 인위적으로 센서 노드가 망가지거나, 천둥 혹은 번개, 홍수와 같이 자연적으로 센서 노드가 파괴되는 경우가 있다. 그리고 공격자에 의해 노드가 탈취되어 노드 내부의 정보가 유출되는 경우도 발생한다. 이러한 물리적 공격에 대해서 물리적인 통제가 요구된다.

특히 노드 캡쳐 공격으로 인하여 데이터가 위조 혹은 변조되어 시스템에 위·변조된 정보가 전달 될 수 있으며, 심지어 정상적인 서비스를 받지 못하도록 방해하는 서비스거부 공격을 당할 수 있다. 따라서 데이터가 정상적인 데이터임을 데이터 인증을 통해 확인 하고, 노드 사이의 상호 인증을 통해 공격 노드가 주는 잘못된 정보를 막도록 해야 한다.

(3) 키 관리 기법

위와 같은 케이스에서는 Blom's method와 Polynomial 기법을 사용한다. Polynomial 기법은 각 노드들이 적은 정보만 저장함에도 불구하고 각 노드 사이에 필요한 세션 키를 계산 할 수 있다. 특히 공격자에 의해 노드 캡쳐를 당해도 저항력이 높고, 노드의 차수(degree)가 t인 Polynomial을 사용할 때, t개 이상의 노드가 캡쳐 당하지 않으면 키들의 안전성이 보장되므로 소규모 네트워크의 안전성을 증가시킨다. Blom's method 역시 Polynomial과 비슷하며 단지 키를 생성하고 분배하는데 행렬을 사용한다는 차이점만 있다.

다. case 3 : 실외 - 대규모 네트워크 - 스타 토폴로지

(1) 환경

이 케이스는 실외에 설치된 대규모 네트워크 중에서 스타 토폴로지를 사용

하는 것이다. 대규모 네트워크는 센서 네트워크 내의 센서 노드가 각 센서 노드가 보유하고 있는 키의 개수보다 많은 경우이며, 대규모 네트워크를 실외에 스타 토폴로지로 설치한다.

이러한 예로 교량 모니터링, 건설현장모니터링(배터리사용), Lagrge-scale Campus of EPFL, Planie Morte 등이 있다. (그림 6-11)은 부산의 구포대교를 모니터링 하는 사진이다.

(그림 6-11) 부산 구포대교 교량 모니터링

(2) 공격 유형 및 요구사항

실외에 설치된 센서 네트워크에서는 사람에 의해 인위적이든 자연 재해에 의해 자연적이든 센서 노드가 물리적 공격에 노출되기 쉽다. 이러한 물리적 공격은 물리적 통제를 통해 센서 노드를 보호 한다.

스타 토폴로지는 중앙의 센서 노드(PANC)를 통해 모든 센서 노드들이 직접 연결되어 있다. 이때 중앙의 센서 노드가 공격을 당하면 모든 센서 노드들 역시 쉽게 공격을 당하게 된다. 따라서 중앙의 센서 노드가 캡쳐 당하여 위조 또는 변조된 데이터를 다른 센서 노드에게 전송하면 센서 네트워크는 모든 공격에 노출되게 된다. 그러므로 이러한 공격에 대비하여 데이터인증이 필요하

고, 인증된 데이터만 중앙의 센서 노드로부터 송수신 하도록 해야 한다.

(3) 키 관리 기법

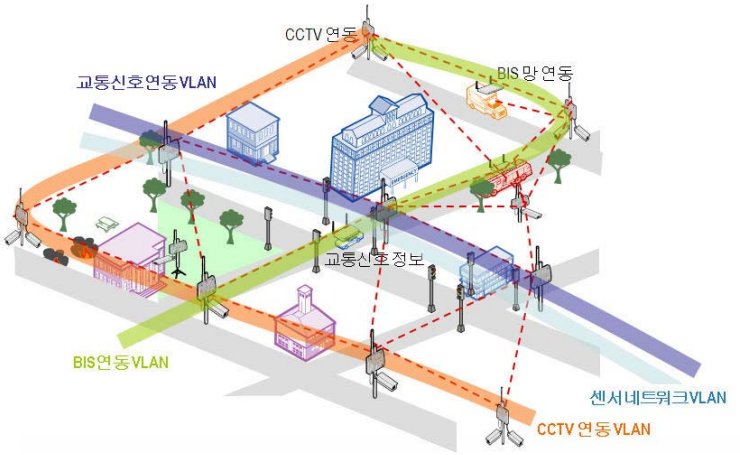
위와 같은 케이스에서 데이터 위변조 공격에 대응하기 위한 키 관리 기법으로 Pairwise key 기법을 사용한다. 중앙의 센서 노드와 통신하는 모든 센서 노드 사이에 다른 세션 키를 사용하기 때문에 모든 키들이 동시에 유출되지 않는 한 위의 공격을 충분히 방어 할 수 있다. 따라서 Pairwise key 관리 기법을 이용하여 센서 노드간의 데이터를 송수신 하는 경로에 대한 보안을 강화하면 실외의 대규모 스타 토폴로지에서 발생하는 데이터 위변조 공격을 막을 수 있다.

다. case 4 : 실외 - 대규모 네트워크 - 메시 토폴로지

(1) 환경

이 케이스는 실외에 대규모 네트워크를 메시 토폴로지로 설치한 것이다. 메시 토폴로지는 멀티 홉을 지원하므로 센서 노드의 장애 발생 시 우회할 수 있는 방법을 제공하여 신뢰성이 우수하다. 이렇기 때문에 실외 환경에 최적화된 토폴로지로 대학교나 대규모 공장 등 무선 서비스를 제공하는 모든 시장에서 가장 많이 사용되고 있다. 즉, USN에서 사용되는 메시 토폴로지는 한 링크 실패가 발생하더라도 다른 링크를 통해 데이터를 전송 한다 해도 문제가 없어야 한다.

이러한 예로는 기상해양 관측 모니터링, 도시기반시설 모니터링 등이 대표적이다. (그림 6-12)는 실외에서 대규모 네트워크 메시 토폴로지를 사용한 u-City를 보여준다. 도심에 설치된 메시 토폴로지를 통해 교통관제, CCTV 망 등을 한 번에 수용한다.



(그림 6-12) 실외 대규모 메시 토폴로지의 예 u-City [104]

(2) 공격 유형 및 요구사항

USN 서비스를 제공하기 위해서는 노드의 정보를 안전하게 유지하고 다른 노드로 전달하는 것이 중요하다. 실외의 센서 네트워크는 실외라는 환경적 특성으로 인해 노드의 손실, 탈취 등의 물리적 공격이 발생하기 쉽다. 이러한 공격을 막기 위해서는 인증 받지 못한 정보기기의 사용을 제한하거나 불법 접근을 차단하는 물리적 보안대책을 강구하고, 데이터 보호를 위한 법제도와 인증체계를 마련이 필요하다.

물리적 공격 이외에도 메시 토폴로지에서는 서비스 거부 공격과 라우팅 공격 등이 발생 한다. 서비스 거부 공격을 방어하기 위해서 송수신되는 데이터를 암호화하고, 센서 노드들의 상호 인증하는 것이 필요하다.

또한 메시 토폴로지의 경우 토폴로지의 특성상 멀티 홉을 지원함으로 다중 라우팅 경로를 가지게 된다. 이러한 네트워크에서 메시지가 정상적인 경로를 통해 싱크 노드로 전달되는 과정을 방해하는 라우팅 공격이 발생하게 된다. 따라서 라우팅 공격에 대응하기 위해서 통신하는 노드 사이의 상호 인증이 필요함은 물론이고, 통신이 이루어지는 통신 채널뿐만 아니라 라우팅 정보도 제한된 자원을 고려한 경량 암호화 방법이 이루어 져야 한다. 그리고 한 노드가 캡쳐 당해도 빠르게 다른 경로를 통해 전보를 전달 할 수 있는 노드 포획에

대한 탄력성이 요구된다.

(3) 키 관리 기법

실외 대규모 네트워크의 메시 토폴로지 환경에서는 Random 키 기법과 Multi-path 기법을 사용하도록 한다.

- o Random-pair wise 키 : Random pairwise key를 통해 노드와 노드 사이에 각각 다른 키를 가진 링크가 생성되도록 해야 한다. 또한 공격자가 정보 송수신의 경로 바꾸거나, 다양한 경로를 통해 노드가 서비스를 제대로 받지 못하도록 할 때 Random Pairwise 기법으로 노드 사이의 경로에 대해 키를 재분배하거나 Multi-path 기법을 통해 정산적인 서비스가 이루어지도록 한다.
- o Multi-path : 노드 캡쳐 공격을 당한 노드에게 정보가 유입되지 못하도록 해야 하고, 캡쳐 된 노드를 피해 정보가 송수신 되어져야 한다. 따라서 이러한 경우에 Multi-path 기법을 사용한다.

다. case 5 : 실외 - 대규모 네트워크 - 클러스터 트리 토폴로지

(1) 환경

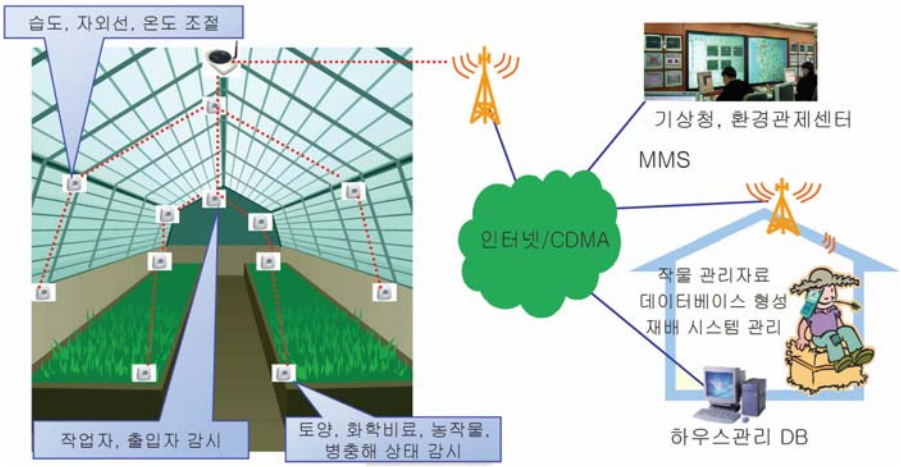
이 케이스는 실외의 대규모 네트워크를 클러스터 트리 토폴로지로 설계한 것이다. 클러스터 트리 토폴로지는 네트워크 관리가 용이하고 추가적인 가지를 가질 수 있어 확장성이 우수하다는 특징을 가지고 있기 때문에 대규모의 네트워크에 적합한 구조이다. 또한 통신 속도가 연결되는 노드 수로 나눈 만큼 감소될 수 있다는 특징이 있다. 따라서 데이터의 전송률이 높지 않은 환경에 사용이 가능하다.

이 구조는 데이터를 지역적으로 모아서 처리하는 분산 처리 환경에 적합하며, 센서 노드의 실시간 정보 수집, 분석의 효율성을 위하여 다수의 센서 노드

운영을 위한 네트워크 효율성 증대를 위해 트리 방식의 토폴로지를 사용하는 경우도 있다. 하지만 계층 구조이기 때문에 상위 노드가 고장이 나면 하위 노드들의 네트워크가 마비되거나 더 크게는 네트워크가 단절 된다는 단점이 있다.

이러한 케이스로는 산업용 공장 모니터링(그림 6-13), 지하수 모니터링, 농산물 재배관리 시스템(그림 6-14) 등이 대표적이다.

(그림 6-13) 산업용 공장의 모니터링 [106]



(그림 6-14) 농산물 재배 관리 시스템 [169]

(2) 공격 유형 및 요구사항

클러스터 트리 토폴로지를 사용할 경우에 발생할 수 있는 공격에는 물리적 공격과 데이터 위변조 공격, 서비스 거부 공격이 있다.

특히 물리적 공격의 경우 넓은 지역에 센서 노드가 분산되어 있고 실외라는 환경적 특성 때문에, 자연 재해 혹은 인위적인 공격으로 센서 노드가 물리적인 손상을 입게 되는 것이다. 또 다른 물리적 공격으로는 부채널 공격이 있을 수 있다. 부채널 공격은 또 다른 형태의 물리적 공격으로 노드가 동작하고 있을 때 사용하는 소비 전력 혹은 방사되는 전자파 정보를 이용하여 노드가 가지고 있는 중요한 정보를 알아내는 공격이다. 부채널 정보는 공격자에게 좋은 정보가 될 수 있고 부채널 정보를 분석하는 것은 전체 암호 시스템의 약점을 찾아 공격하는 현실적인 공격법이 될 수 있기 때문에 암호 시스템을 견고하게 하는 것이 필요하다.

그리고 클러스터 트리 토폴로지에는 데이터 위변조 공격이 있다. 트리의 클러스터 헤드(Cluster head)를 맡고 있는 노드가 캡쳐 될 경우, 캡쳐 된 클러스터 헤드를 통해 위조 또는 변조 된 정보가 클러스터 내부의 노드들에게 잘못 된 정보가 전송된다. 이런 식으로 데이터 위변조 공격이 이루지면 데이터 정보 전달에 있어 정확성을 왜곡시키게 된다. 따라서 데이터를 암호화 하여 정확한 데이터만 송수신 될 수 있도록 하는 것이 필요하다.

물리적 공격과 데이터 위변조 공격뿐만 아니라 서비스 거부 공격이 있다. 이는 위의 데이터 위변조 공격과 비슷하며 - 클러스터 헤드가 캡쳐 되는 경우 - 데이터의 암호화뿐만 아니라 메시지와 노드 사이의 인증 등을 통하여 정상적인 정보를 송수신해야 하고, 정상적인 노드만이 통신을 하는 것을 허용해야 한다. 또한 지속적인 서비스 거부 공격으로 인하여 센서 노드의 에너지가 소모되어 급격하게 성능이 저하되는 것을 방지하는 것도 요구된다.

(3) 키 관리 기법

이 케이스에서는 q-합성수 기법과 LEAP를 이용한다.

o q-합성수 : 물리적 공격의 센서 노드의 손상이나 탈취는 실질적인 물리적인 통제가 필요하다. 부채널 공격의 경우에는 부채널 정보를 막기 위해서는 자료나 키가 사용될 때마다 다른 값을 갖도록 한다. 이를 위해 q-합성수 기법을 이용한다. 그리고 클러스터 트리 토폴로지의 특성상 각 센서 노드 사이에 하나의 경로만 존재하므로 q개의 공통키로 센서 노드 사이의 링크를 더욱 강력하게 보호하여 데이터 위변조나 서비스 거부 공격을 방어한다.
o LEAP : LEAP는 4개의 키, 개인키, Pairwise 키, 그룹 키, 클러스터 키를 사용하여 서비스 거부 공격을 당하더라도 이웃 노드가 당하는 피해를 최소한 할 수 있다. 그리고 대칭키를 이용하여 초경량 메시지를 암·복호화하며, 노드 사이에 MAC 확인을 통해 인증을 한 후에 수신한 메시지를 포워딩하거나 프로세싱 함으로써 서비스 거부 공격과 같은 공격을 막아 에너지 소비를 줄일 수 있다.

다. case 6 : 실외 - 대규모 네트워크 - 클러스터 메시 토폴로지

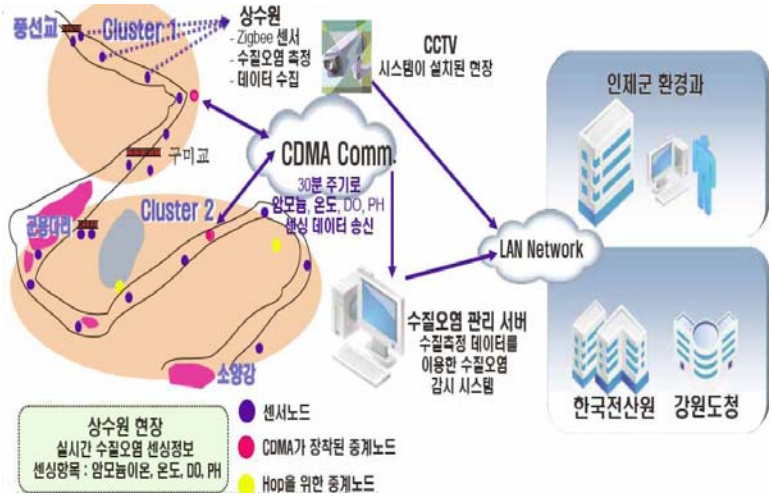
(1) 환경

이 케이스는 실외에서 대규모 센서 네트워크를 설계 할 때 클러스터 메시 토폴로지로 설계한 것이다. 클러스터 메시 토폴로지는 센서 네트워크 확장성이 용이하고, 센서 노드들이 클러스터를 이루기 있기에 네트워크 관리가 편리하다. 또한 메시 토폴로지와 비슷하면서도 메시 토폴로지의 단점을 극복하여 많은 센서 노드들의 사용이 가능하도록 하였다.

이러한 케이스로 식수원 관리를 위한 수질 모니터링 시스템(그림 6-15), 하천 생태복원 시스템, 수질 관리 등이 대표적이다.

(2) 공격 유형 및 요구사항

클러스터 메시 토폴로지는 메시 네트워크의 특성을 가지고 있으므로 메시 토폴로지와 마찬가지로 서비스거부 공격과 라우팅 공격에 쉽게 당할 수 있다.



(그림 6-15) 수질관리 모니터링 [124]

메시 토폴로지의 요구조건과 마찬가지로 서비스 거부 공격은 데이터를 암호화 하여 노드 상호 인증을 통한 신뢰된 노드끼리 혹은 클러스터끼리 통신을 하도록 해야 한다.

클러스터 메시 토폴로지 역시 다중 라우팅 경로를 가지게 된다. 따라서 정보가 정상적인 경로를 통해 싱크 노드로 전달되는 과정을 방해하는 라우팅 공격이 발생한다. 그러므로 라우팅 공격에 대응하기 위해서 통신이 이루어지는 노드 사이의 상호 인증이 필요하며, 일어한 통신 채널뿐만 아니라 라우팅 정보도 제한된 자원을 고려한 경량 암호화 방법이 이루어 져야 한다. 또한 일부 센서 노드가 공격을 당해서 정상적인 기능이 어려워도 전체 네트워크에 미치는 영향이 적어야 한다. 특히 클러스터 구조이므로 클러스터 헤드의 노드 에너지를 적게 사용 할 있도록 하여 클러스터 헤드에게 전파나 트래픽이 집중

되는 것을 방지한다.

이 케이스 역시 실외에 설치되어 있어서 전파 방해 등과 같은 인위적인 공격뿐만 아니라 천둥, 번개, 홍수 같은 자연적 공격도 받을 수 있다. 이러한 물리적 공격에 대응하기 위해서 센서 노드를 보호 할 수 있는 물리적인 통제와 감시 제어가 필요하다.

(3) 키 관리 기법

위와 같은 요구사항을 반영하여 실외의 대규모 센서 네트워크 클러스터 메시 토폴로지에서 공격을 대응하는 키 관리 기법으로 LEAP, Random key, multi-path 방법을 이용한다.

- o Random key : 이 케이스는 메시 토폴로지와 유사하며, 클러스터 트리 토폴로지의 단점을 개선한 것이다. 하지만 상대적으로 네트워킹이 복잡해졌다. 따라서 메모리의 용량과 네트워킹 등을 고려하여 Random key 기법을 사용한다.
- o q-합성수 : 메시 토폴로지에서는 많이 분산되어 있는 센서 노드들의 더욱 강한 보안을 위해 Random Pairwise 키 기법보다 더 강한 키 기법으로 q-합성수를 사용 할 수도 있다.
- o LEAP : LEAP는 4개의 키, 개인키, Pairwise 키, 그룹 키, 클러스터 키를 사용하여 서비스 거부 공격을 당하더라도 이웃 노드가 당하는 피해를 최소한 할 수 있다. 그리고 대칭키를 이용하여 초경량 메시지를 암·복호화하며, 노드 사이에 MAC 확인을 통해 인증을 한 후에 수신한 메시지를 포워딩하거나 프로세싱 함으로써 서비스 거부 공격과 같은 공격을 막아 에너지 소비를 줄일 수 있다.
- o Multi-path : 서비스 거부 공격이나 라우팅 공격을 당해서 노드가 올바른 서비스를 받을 수 없을 때에는 메시 토폴로지의 장점인 멀티 홉을 이용하여 다른 경로를 통해 정보를 안전하게 전달 해 주는 Multi-path 기법을 사용한다.

제 3 절 통합 키 사전 분배 프레임워크와 응용

앞에서 살펴본바와 같이 센서 네트워크는 다양한 형태를 가지고 있고, 이들 형태를 고려하지 않는 키 관리 기법은 그 성능을 최대한으로 발휘하기 힘들다. 이에 따라 6장 2절에서 분류한 바와 같이 각 네트워크 형태에 따라 서로 다른 기법을 사용해야 함을 보였다. 하지만 센서 네트워크의 종류별로 서로 다른 키 사전 분배 기법을 사용하는 것은 센서 네트워크 개발자 입장에서 매우 비효율적인 상황이 된다. 따라서 제 3 절에서는 제 2 절에서 도출된 모델의 다양한 키 관리 기법을 하나의 통합 프레임워크에서 구현할 수 있도록 '통합 키 사전 분배 프레임워크'를 제시한다. 센서 네트워크의 형태에 따른 적절한 키 관리 기법은 이 프레임워크의 여러 가지 파라미터를 조절함으로써 구현 가능하게 한다.

1. 통합 키 사전 분배 프레임워크(Unified Key Pre-Distribution Framework)

본 보고서에서 제시하는 통합 프레임워크는 앞에서 설명한 다양한 키 사전 분배 기법 중 하나를 선택하고 이를 확장시켜 정의한다. 따라서 이 통합 프레임워크에 적합한 키 분배 기법을 선택하기 위해서 앞에서 설명한 키 관리 기법들의 장점과 단점을 분석하였다. 랜덤 키 분배 기법은 랜덤한 키 분배 때문에 인접한 두 노드간의 직접적인 통신이 불가능하게 되는 경우도 발생된다. 이에 반해 Polynomial 기반의 분배 기법은 임의의 두 노드 간에 직접적인 키 설정이 가능하다. 다만 λ-secure 하기 때문에 캡쳐에 대해서 λ 개 노드까지는 안전을 보장하지만 λ개 이상의 노드가 캡쳐 되는 경우에는 전체 시스템이 무너질 수도 있다는 단점을 가진다. 하지만 인접한 두 노드 사이에 항상 세션 키를 설정하는 것이 중요하기 때문에 통합 프레임워크의 기본적 키 사전 분배 기법으로 Polynomial 기법을 사용한다.

통합 키 사전 분배 프레임워크는 [표 6-6]에 상세히 설명되어 있다.

[표 6-6] 통합 키 사전 분배 프레임워크

i. 각 센서 노드는 키 서버와 노드 사이에 안전한 통신을 위해 키 서버와 각 센서 노드 간에 Pairwise 키 형성한다.
ii. 시스템의 다양한 기준에 따라 센서 노드를 복수개의 그룹으로 나눈다. 나누는 적합한 기준으로 장소와 토폴로지 등을 예로 들 수 있다.
iii. 키 서버는 Polynomial의 집합을 유지한다. 각 Polynomial은 Polynomial의 계수에 대한 지수(coefficient-exponent) 쌍의 집합으로 나타낼 수 있다. 차수(degree)에 따라서 다양한 Polynomial이 형성될 수 있다.
iv. 키 서버는 각 그룹에게 Polynomial을 할당한다.
v. 각 센서 노드는 하나의 그룹에 속하고, 속해 있는 그룹의 Polynomial로부터 Polynomial Share를 받는다. 또한 센서 노드가 속한 그룹의 주변 그룹에 할당된 Polynomial Share도 할당 받는다. 각 센서 노드가 보유해야 하는 Polynomial Share의 최소수를 N_i라고 한다. 어떤 노드는 노드의 활용 가능한 메모리 크기가 클 경우, N_i 개 이상의 Polynomial share를 가질 수도 있다.
vi. 센서 노드는 최소 1개 이상의 이항 Polynomial (Bivariate polynomial)을 공유하는 다른 노드와 공통 세션 키를 생성한다. 세션 키의 확립은 한 Polynomial Share만을 이용하지 않고, 공유하는 공통 Polynomial 모두를 기반으로 한다. 즉, 각각의 공통 Polynomial로 세션 키를 생성하고, 이 키들에 서로 XOR 연산을 적용하여 하나의 키를 만들어 낸다. 이와 같이 복수개의 Polynomial을 바탕으로 하나의 세션 키를 생성하는 방법을 “강화된 직접 키 확립 옵션”이라고 부른다.
vii. 공통된 Polynomial Share가 존재하지 않는 경우에는 일반적인 path key 확립 기법을 사용 할 수 있다.

단계 vi에서 XOR 연산 대신에 다양한 hash 함수를 사용할 수 있는데, 연산 시간 측면에서 XOR를 사용하는 것이 효율적이다. 한 가지 주의할 점은 이 통합 프레임워크에서의 그룹의 수는 실제로 시스템 안의 Polynomial의 수가 된다는 점이다. [표 6-7]은 뒤에서 설명할 때 사용할 파라미터를 요약하고 있다.

[표 6-7] 파라미터(Parameter)

파라미터(Parameter)	의미
N_i	센서 노드가 가져야 하는 전체 키 공유의 최소값
N_g	시스템 내 그룹의 수
m	센서 노드가 저장 할 수 있는 키 개수의 최소값
P	Key Pool의 크기
t	Polynomial의 차수(degree)

m은 센서 노드가 저장 할 수 있는 키 값들의 개수이다. 하지만 Polynomial 기법의 경우 하나의 Polynomial에 대해 (t+1) 개의 계수 (Coefficient)를 저장해야 한다. 여기에서 계수의 크기 (bit size)는 사용할 세션 키의 크기와 동일하기 때문에 m은 하나의 센서 노드가 저장할 수 있는 전체 계수의 개수라고도 할 수 있다. 예를 들면 센서 노드가 하나의 Polynomial만을 사용한다면, 이 Polynomial은 m-1 차수 (degree)를 가져야 하고, m 개의 계수가 센서 노드에 저장된다. 만약 센서 노드가 2개의 Polynomial을 저장하게 된다면, 각각의 Polynomial은 m/2-1의 차수 (degree)를 가지게 된다. 서로 다른 형태의 센서 네트워크에서, 센서 노드의 수용 능력에 따라 센서 노드들은 다른 키 값의 수를 유지할 수 있다.

하지만 여기서 제안하는 공통 프레임워크에서는 각 노드가 적어도 키 값 m을 유지할 수 있다는 것을 가정한다. 이것은 만약 센서 노드의 모든 Polynomial 몫의 차수(degree)가 t 라고 하면 $N_i \times (t+1) \geq m$이 되어야 함을 의미한다. 일반적으로 모든 센서 노드가 같은 m 값을 가지게 되면, N_i가 1보

다 클 경우 차수 t는 m 보다 작아지게 된다. 그런데 이러한 통합 프레임워크의 Polynomial 기법은 t-secure가 되는데, 차수가 m 보다 작기 때문에 그냥 하나의 Polynomial만을 사용하는 경우에 얻을 수 있는 m-secure 보다 더 안정성이 떨어지게 된다는 문제점이 있다(t < m이기 때문에). 하나의 Polynomial을 사용하지 않고, 여러 개의 Polynomial을 사용하게 되면, 센서 노드의 저장 공간이 m으로 제한되어 있기 때문에 각 Polynomial의 차수가 작아지게 된다는 것이다. 따라서 이 통합 프레임워크의 안정성을 유지하기 위해서는 해당 Polynomial을 공유하는 센서 노드의 수를 t보다 작게 유지하는 것이 필수적이다. 이 경우 완전한 보안을 이룰 수 있다.

이와 더불어 앞에 설명한 프레임워크는 원래의 Polynomial 기법인 RS(Random Subset) 기법이 가지고 있지 않은 특성을 보여준다. 첫 번째로, 두 개의 노드가 하나 이상의 공유 Polynomial shares를 가지고 있을 수도 있기 때문에 이 하나의 링크를 캡쳐하기 위해 더 많은 노드 캡쳐가 요구된다. 따라서 강화된 직접 키 확립 옵션은 보안 성능을 증가 시킬 수 있다. 두 번째로, 이 프레임워크가 고성능의 노드는 더 많이 Polynomial shares를 유지할 수 있도록 허용하였기 때문에 고성능 노드는 높은 연결 확률과 높은 보안을 가질 수 있다. 따라서 고성능 노드 간에 세션 키를 설정하는 경우 더 많은 공통 Polynomial을 사용할 수 있게 되어 더 강화된 보안을 이룰 수 있게 된다.

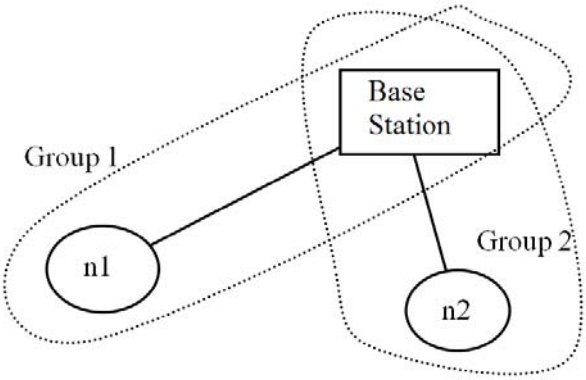
2. 케이스에 따른 통합 키 사전 분배 프레임워크 적용 방법

가. 스타 토폴로지에서의 적용 방법

통합된 키 분배 프레임워크는 다양한 케이스에서 적용이 가능하다. 첫 번째 케이스는 스타 토폴로지로만 구성된 것이다. 이 타입의 센서 네트워크에서는 각 센서 노드가 오직 베이스 스테이션과만 통신한다. 그래서 키 서버가 센서 노드 사이에 Pairwise key를 부여하지 않아도 된다. 이 경우, 각 센서 노드와 베이스 스테이션 사이의 통신에서만 이용되는 각 센서의 고유한 키는 완벽한 안정성을 보장 할 수 있다. 이러한 통합 프레임워크 상에서, 다음과 같이 센서

네트워크를 구성함으로써 목적을 이룰 수 있다.

센서 네트워크안의 각 노드는 각각의 그룹을 형성한다. 따라서 센서 네트워크에 n개의 센서 노드가 존재하면, n개의 그룹을 가지게 된다. 또한 이 케이스의 Polynomial은 차수(degree)가 0을 가진다(이 경우 Polynomial은 상수가 된다). 그리고 각 그룹마다 다른 Polynomial이 주어지므로, 스타 토폴로지 내의 각 노드는 다른 상수 키 값을 가지게 된다. 따라서 통합 프레임워크는 완벽한 보안성을 갖게 된다. (그림 6-16)는 이러한 예시를 나타낸다.



(그림 6-16) 스타 토폴로지 그룹화 예시

나. 소규모 센서 네트워크에의 적용 방법

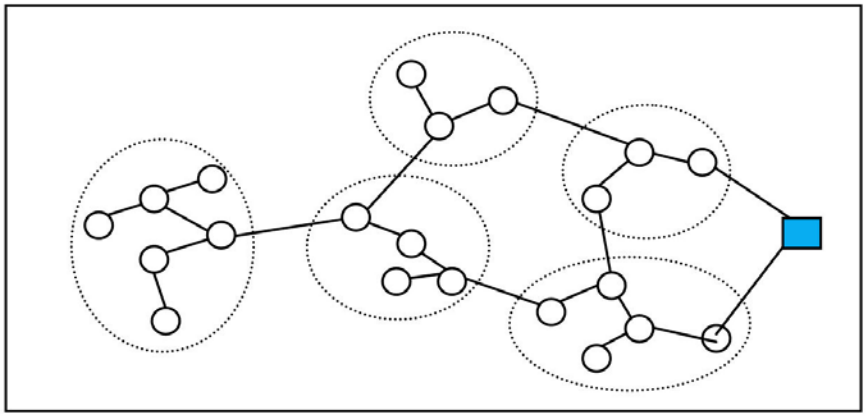
두 번째 케이스는 소규모 네트워크이다. 본 보고서에서 소규모 네트워크의 정의는 센서 네트워크에 참여하고 있는 노드들의 수가 각 센서 노드가 보유할 수 있는 키 값인 m보다 작은 경우이다. 즉, 한 센서 노드가 보유 할 수 있는 키 값 m이 센서 네트워크 내의 노드들의 수보다 크다는 것이다. 이 상황에서 전체 센서 네트워크가 하나의 그룹이 되고, 하나의 Polynomial로 부터 각 노드의 Polynomial share를 생성한다. Polynomial의 차수(degree)는 m-1로 설정된다. 센서 네트워크 내에 존재하는 노드의 수가 m보다 작기 때문에, 노드 캡쳐 (node compromises)가 되더라도 Polynomial은 노출되지 않는다. 또한, 모든 노드가 동일한 Polynomial로부터 Polynomial shares를 갖게 되기 때문에,

어떤 노드 쌍이라도 그들의 통신을 위한 세션 키를 설정 할 수 있다.

다. 클러스터 토폴로지에서의 적용 방법

센서 네트워크 토폴로지들은 일반적으로 4개의 그룹으로 분류 된다 : 클러스터 트리, 클러스터 메시, 평범한 메시(여기서 평범한 메시란 스타토폴로지와 메시 토폴로지를 말한다). (그림 6-17)은 클러스터가 있는 토폴로지의 예이며 클러스터는 대규모 네트워크에서만 사용 하도록 한다. 스타 토폴로지는 평범한 케이스이므로 본 장 3절 2에서 설명했다.

토폴로지 정보를 활용함에 있어서, 가장 중요한 문제는 각 클러스터의 크기이다. 각 클러스터를 통합 프레임워크의 한 그룹으로 생각한다면, 그 클러스터의 센서 노드의 수가 그 그룹에 할당된 Polynomial의 차수보다 작은 경우 완전한 보안을 이룰 수 있게 된다. 만약 각 클러스터 내의 노드의 수가 메모리 크기 (m)보다 작으면, 이 통합 프레임워크에 의해 캡쳐 공격으로부터 완벽한 보호를 받는 것이 가능하게 된다. 하지만 이러한 클러스터 크기나 클러스터들 간의 연결 정보 등이 센서 네트워크가 배치되기 전에 미리 제공될 수 있는 지에 대한 문제점이 있다.



(그림 6-17) 클러스터 토폴로지의 예

그러므로 우리는 클러스터 케이스를 두 가지로 구분한다. 첫 번째는 클러스터링 정보가 이미 주어진 케이스이고, 두 번째는 센서 노드가 배치된 후에 클러스터가 형성되는 케이스이다. 두 번째 경우에는 주어진 토폴로지에 관한 정보가 없는 것과 마찬가지 이다. 이것은 클러스터를 가진 토폴로지가 통합 프레임워크에서 키 분배 기법을 설정하는 방법에 대한 어떤 단서도 제공하지 않는다는 것이다. 따라서 보안성을 증가하기 위해 강화된 직접 키 설립 옵션을 사용하도록 한다.

클러스터링 정보가 미리 주어지는 경우에는 위치 정보가 주어지는 경우와는 다르다. 따라서 이 통합 프레임워크를 적용하기 위해서는 다른 방식이 필요하다. 이 통합 프레임워크에서 사용할 그룹은 각각의 클러스터가 하나의 그룹이 된다. 그리고 각 그룹에 하나의 Polynomial이 할당된다. 이 때 클러스터 안의 노드의 수가 메모리 크기보다 클 때 보호가 완벽하지 않다는 문제점이 있다. 그러나 일반적 클러스터 안의 노드의 수가 작기 때문에 우리는 보안이 무너지지 않는다고 가정한다. 클러스터의 노드 수가 할당된 Polynomial의 차수보다 큰 경우에 보안이 깨지는 경우가 발상한다. 이에 관해 본 보고서의 제 7 장에서 시뮬레이션을 통해 그 정도를 파악한다.

또 다른 문제는 토폴로지 기반 클러스터 내에서 다른 클러스터들 내의 노드와 통신할 필요가 있다는 것이다. 하지만 단지 클러스터 소속 정보만으로는 어느 클러스터의 노드가 어느 다른 클러스터의 노드와 통신이 필요한지를 알 수가 없다. 그래서 본 보고서에서는 사전에 제공되는 클러스터링 정보에 각 클러스터의 이웃 클러스터 정보도 포함한다고 가정한다. 이를 바탕으로 각 센서 노드는 자신의 클러스터와 이웃 클러스터의 Polynomial을 모두 보유하도록 한다. 하지만 노드의 메모리 크기가 m으로 제한되어 있기 때문에 하나의 센서 노드가 여러 개의 Polynomial의 가지는 경우 각 Polynomial의 차수가 작아지게 된다. 즉 이웃 클러스터의 수가 가장 큰 클러스터의 이웃 클러스터의 수를 k라고 하자. 이 경우 이 클러스터에 속하는 노드는 k+1 개의 Polynomial을 가지며, Polynomial의 차수(degree)는 $t = \left\lfloor \frac{m}{k+1} \right\rfloor$ 이 될 것이다. 각 노드들이 가지는 Polynomial의 차수는 동일하게 유지해야 하기 때문에, 각 노드는

항상 k+1개의 Polynomial을 가지도록 한다. 그렇지 않으면 인접 클러스터의 수가 작은 클러스터 내의 노드의 메모리는 더 이상 Polynomial 공유를 유지하지 않고 낭비하게 된다. 이것은 내부 클러스터 통신의 보안을 약화시킨다. 이러한 상황을 방지하기 위해 k+1이 되는 Polynomial의 수를 생성하여 클러스터에 추가적인 Polynomial을 할당한다. 이렇게 되면 클러스터 내부의 통신은 k+1개의 공통 Polynomial을 이용하기 때문에 m-secure를 달성할 수 있다.

두 이웃 클러스터에 속한 노드가 통신을 하게 되는 경우, 위에서 설명한 Polynomial 배분 방식에 의해 최소 2개 이상의 공통 Polynomial이 존재하게 된다. 따라서 클러스터 A와 B가 서로 이웃하게 되면, 클러스터 A의 노드는 클러스터 A와 B에 할당된 Polynomial을 가지고 있고, 클러스터 B의 노드도 마찬가지로 클러스터 A와 B에 할당된 Polynomial을 가지고 있게 된다. 이에 더하여 각 클러스터가 서로 이웃한 다른 공통 클러스터가 있는 경우 공통 Polynomial의 수는 더 증가하게 되어, 보안이 더 향상되게 된다. 예를 들면, 클러스터 A와 B가 서로 이웃한데, 이 두 클러스터가 모두 클러스터 C와 이웃하는 경우, 클러스터 A의 노드는 클러스터 A, B, C에 할당된 Polynomial을 가지고 있고, 클러스터 B의 노드도 클러스터 A, B, C에 할당된 Polynomial을 가지고 있게 된다. 클러스터가 보통 이웃들을 더 많이 가지면, 보통 Polynomial 공유가 증가한다.

3. 강화된 직접 키 확립 옵션 활용 및 센서 노드와 위치 정보 활용과 시간에 따른 교체

가. 강화된 직접 키 확립 옵션의 활용

이 통합프레임워크는 기존의 키 관리기법을 다양한 파라미터의 조합으로 표현할 수 있을 뿐만 아니라, 기존의 키 관리 기법이 가지지 못하는 여러 장점을 보여준다. 첫 번째로 강화된 직접 키 확립 옵션 기법이다. 아래에서는 이 기법의 필요성과 사용 방법을 설명한다.

첫 번째 경우는 노드의 수가 유동적이고 시간이 흐른 뒤 노드가 삽입과 삭제 될 수 있는 경우이다. 네트워크의 크기가 미리 알려지지 않았기 때문에, 각

그룹에 속하는 노드의 수가 m 보다 작게 하는 것은 어렵다. 따라서 이 경우에는 원래의 Polynomial 기반 기법 (RS : Random Subset)과 더불어 강화된 직접 키 확립 옵션을 사용한다.

기본적으로, 통합된 키 분배 프레임워크의 목적은, 두 인접 노드가 세션 키를 직접적으로 설정할 수도 있게 하며 노드 캡쳐 공격도 완벽한 보안성을 유지하도록 하는 것이다. 본 보고서의 통합 프레임워크는 노드를 여러 그룹으로 분할하여 각 그룹 내에 존재하는 노드의 수를 m이하로 유지하기 때문에, 어떠한 캡쳐 공격에도 완벽한 보안성을 유지할 수 있게 된다. 하지만 원래의 RS 기법을 사용하는 경우, 만약 인접하는 두 노드가 공통된 Polynomial key share를 가지고 있지 않으면, 두 노드는 세션 키를 설정 할 수 없게 된다. 예를 들어 P를 키 서버에 존재하는 Polynomial의 수라고 하고, k를 한 센서노드가 가지고 있는 Polynomial share의 수라고 가정한다. 여기서 임의의 두 노드 쌍이 최소한 하나의 공통된 Polynomial share를 가질 확률 p는 다음과 같다.

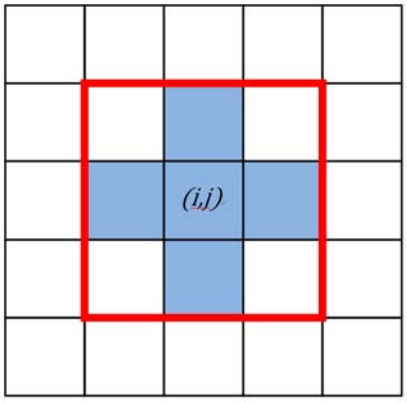
$$p = 1 - \sum_{i=0}^{k-1} \frac{P-k-i}{P-i}$$

t가 Polynomial share의 차수라고 하면 여기서 $k = \frac{m}{t+1}$이다. 이것은 확률 p를 증가시키기 위해서 k를 증가시켜야 하고, 이는 곧 t를 감소시켜야 한다는 것을 보여준다. 따라서 t가 감소하게 되면 Polynomial share의 안전성이 감소하게 되어 t개 이상의 노드가 캡쳐 될 경우에는 Polynomial이 노출될 수 있다. 그러나 통합 프레임워크 상에서는 세션 키가 두 노드에 존재하는 모든 공통된 Polynomial share에 기반을 두기 때문에, 네트워크의 안전성이 완전히 Polynomial 차수(degree)에만 의존하지 않는다. 따라서 보안이 더 향상되는 것이다.

나. 센서 노드 위치 정보의 활용

본 보고서의 제 6장 제 2절에서 분류한 네트워크 형태에 상관없이, 부가적인 정보가 제공되는 경우 이 통합 프레임워크는 더 나은 성능을 발휘할 수 있

다. 예를 들면 센서 노드의 위치 정보가 분배되기 전에 미리 주어진 경우이다. 이 때 추가된 정보를 참조함으로써, 보안성을 높일 수 있다. 첫째로, 지역 정보를 기준으로 노드의 그룹을 나눈다. 여기서 한 가지 제약 사항은 각 노드가 m 키 값만을 유지 할 수 있기 때문에 각 그룹 내에 속하는 노드의 수를 m보다 작게 해야 한다. 그렇지 않으면 특정한 m 개의 노드가 캡쳐 될 경우 같은 그룹 내의 다른 노드들의 통신이 노출 될 수 있다. 하지만 다른 그룹 내의 노드들은 이 경우라도 통신이 노출되지 않아 통신이 가능하게 된다. 또한 서로 다른 그룹에 속하는 노드들 간에 통신이 가능해야 함으로, 한 그룹에 속한 노드들은 인접 그룹의 Polynomial share를 가져야 한다. 인접한 그룹의 수가 증가할수록, 각 노드가 가지는 공유된 Polynomial의 수도 증가한다. 각 노드의 메모리 크기가 m 밖에 되지 않기 때문에, 각 노드가 가질 수 있는 Polynomial shares의 키 값의 수는 m보다 작거나 같을 수밖에 없다는 점을 유의해야 한다.



(그림 6-18) 지리적 위치 정보를 가진 그룹

위에서 설명한 요구사항을 맞추기 위해서, 센서 네트워크 지역을 정사각형으로 나누어서, 각 사각형이 4개의 인접 사각형을 갖게 하였다. 따라서 하나의 사각형에 속하는 노드는 (그림 6-18)에서 볼 수 있듯이 5개의 Polynomial shares를 갖게 되고, 8개의 인접 사각형에 속한 노드들과는 항상 2개의 공유

Polynomial을 갖게 된다(인접 사각형은 (그림 6-18)에서 굵은 선으로 포함되어 있다). 유의할 점은 각각 공유 Polynomial의 차수는 m/5라는 것이다.

남은 문제점은 각 사각형의 크기를 결정하는 것이다. 각 사각형의 Polynomial 차수가 m/5이고 하나의 Polynomial은 주변의 5개 사각형에 속한 노드들이 서로 보유하고 있기 때문에, 각 사각형에 속한 노드의 수는 m/5보다 작게 해야 한다. 이것은 이상적인 상황인 경우다. 하지만 이것은 또한 작은 사각형 크기를 초래할 수 있고, 안전한 통신 링크를 성립할 수 있게 되는 범위가 작아지기 때문에 네트워크가 분할될 수 있다. 따라서 영역을 분할하기 위해 하나의 방법만을 사용하기 보다는 각 사각형에 존재하는 노드의 수를 파라미터 ss로 표시하여 각 그룹에 속한 노드의 수를 ss 이하로 하도록 한다. 이 ss는 센서 네트워크 관리자가 지정할 수 있다.

따라서 키 서버가 각 사각형에 존재하는 노드의 수인 ss보다 같거나 작은 숫자가 되도록 전체영역을 사각형으로 나눈다. 사각형에 들어갈 노드의 적절한 수는 이진 탐색(binary search)을 통해 쉽게 구할 수 있다. 여기서 사각형 한 변의 길이를 r이라고 하자. 보통의 경우처럼 가장 왼쪽 아랫부분을 (0,0)로 정한다. 그렇기에 한 변의 길이가 r일 경우 각 사각형의 가장 아랫부분 왼쪽 좌표는 (rx, ry)가 되며, 여기서 x, y는 정수로 c<=x, y이다.

아래의 표에서 ss 개 보다 적은 수의 센서노드가 센서 네트워크의 각 사각형에 들어가는 알고리즘을 나타낸다.

이 알고리즘은 ss 파라미터와 함께 사각형의 최적 길이를 구해준다. 이미 사각형의 리스트가 있기 때문에 각 사각형에 임의로 Polynomial을 할당한다. 각 그룹(사각형)안의 노드는 속한 그룹과 5개의 인접 사각형에서 공유 Polynomial을 받게 된다. (그림 6-18)는 이러한 예시를 보여준다. (i, j)에 존재하는 노드들은 (i-1, j), (i, j-1), (i, j), (j, j+1), (i+1, j)상에 존재하는 5개의 사각형에서 공유 Polynomial을 받게 된다. 두 인접한 사각형에 존재하는 두 노드는 2개의 같은 Polynomial을 가지게 된다. 이렇게 함으로써 각 노드는 인접한 사각형에 존재하는 다른 노드들과 통신이 가능하게 된다.

[표 6-8] 최적의 사이트 길이(ss) (Optimal Side Length(ss))

1. Find the smallest rectangle that contains all the nodes in the sensor network. Let W be the width of the rectangle and H be the height.
2. Let R be the maximum of W and H.
3 Set L = 0
4. If R < L, stop and return L.
5. r = (L+R)/2.
6. With the given r, we construct the squares with the side length of r as described in the above.
7. If the number of nodes in all the squares are less than ss, L=r.
8. If the number of nodes in any of the squares are more than ss, R=r.
9. Go to step 4.

다. 시간에 따른 노드 교체

여러 가지 이유에 따라 센서 노드의 교체가 필요해 질 때가 있다. 예를 들면, 센서 노드의 배터리가 닳게 되거나, 센서 노드가 폭풍이나 눈사태 등의 자연 재해에 부서질 경우가 있다. 이런 상황에서는 침입자가 센서 네트워크를 장기간 동안 모니터를 하고, 노드를 캡쳐 할 수 있어서 Polynomial을 밝혀낼 가능성이 있다. 이러한 시간차 공격은 시간 변이 Polynomial 할당법을 사용하여 방지할 수 있다. 즉 시간을 슬롯으로 나눈 후 (한 달 이나 일 년) 다른 시간 슬롯에 따라 그룹의 Polynomial 집합이 달라지는 것이다. 따라서 각 노드는 현재 그룹의 과거, 현재, 미래의 세 가지 슬롯에 있어 Polynomial을 받게 된다. 이런 식으로 노드는 Polynomial을 빼앗기는 찬스를 낮춤과 동시에 이전에 배치도니 노드나 후에 배치도리 노드와 통신이 가능하게 된다.

제 7 장 네트워크 형태별 키 관리 모델 성능 분석

본 장에서는 USN 환경에서의 키 관리 기술의 적용 모델 개발을 위해 제시한 통합된 프레임 워크의 사용 성능을 분석하고자 한다. 기존의 기법들의 경우 각 논문에서 이들의 성능을 분석할 때 각 노드는 모든 다른 노드와 통신이 가능함을 가정하고 분석하였다. 하지만 실제 센서 네트워크에서는 통신 범위가 제한되어 있고, 네트워크의 토폴로지도 다르기 때문에 이와 같은 가정이 성립하지 않고, 이에 따라 성능 분석이 비현실적이 될 수 있다. 따라서 1절에서는 센서 네트워크가 가지는 통신 범위에 의해 형성된 센서 네트워크의 토폴로지에 따라 센서 네트워크가 분할 될 수 있음을 보여주어, 키 관리 기법의 성능을 분석할 때 실제적인 통신 범위를 바탕으로 한 토폴로지를 이용해야 함을 보여준다. 2절에서는 통합 키 사전 분배 프레임워크의 여러 파라미터 값을 다양하게 조절하여 그 성능을 분석하는데, 랜덤 키 분배 기법과 원래의 Polynomial 기반 기법인 RS 기법과의 비교 결과도 제시한다.

제 1 절 실제 배치된 센서 네트워크의 특성에 따른 효과 분석

본 보고서에서는 센서 네트워크의 형태나 특성에 따라 다른 키 관리 기법을 사용해야 함을 역설하였으며, 이 절에서 키 관리 기법들의 성능을 분석할 때 센서 네트워크 토폴로지를 고려해야 함을 설명한다. 예를 들어, 스타 토폴로지를 가진 센서 네트워크의 경우 하나의 싱크 노드만을 가지고 있고, 센서 노드는 이 싱크 노드와만 통신을 하면 되기 때문에 각 센서 노드는 단 하나의 키만 가져도 안전한 통신이 성립될 수 있다. 또한 각각의 노드에 대한 인증과 노드 캡쳐 공격에 대한 완벽한 저항력을 보장한다.

또한 모든 센서 노드가 다른 노드들과 통신 범위에 있다는 가정은 실제 배치된 센서네트워크를 조사한 결과 비현실적인 가설이라는 것을 알 수 있다. 따라서 본 절에서는 실제 배치된 센서 네트워크에 대한 특성을 분석한 결과를

바탕으로 기존 키 배포 기법에서 제한된 통신 범위가 미치는 영향을 분석하였다.

1. 통신 범위가 센서 네트워크 토폴로지에 미치는 영향

기존에 제시된 많은 키 관리 기법들은 센서 네트워크의 특성을 간과한 가정을 바탕으로 성능을 분석되었다. 하지만 센서 노드의 통신 범위는 키 분배 기법의 성능에 따라 큰 차이를 보인다.

(그림 7-1)에서는 크기가 P인 키 풀(key pool : Polynomial의 집합)을 가진 RS(Random subset) 키 분배 기법과 특정한 전송 범위의 토폴로지를 통한 성능 분석 결과이다. 이 시뮬레이션을 위해 100개의 노드를 2000×2000 공간에 랜덤하게 생성하였다. 전송 범위는 300과 500으로 정했다. 그리고 특정한 두 노드가 전송 범위 300과 500 안에 있다면 연결 링크를 나타내는 선을 그렸다.

(그림7-1)의 (a)와 (b)에서 볼 수 있듯이, 전송 범위는 노드의 차수와 센서 네트워크의 연결성에 확실한 영향을 미친다. 300인 전송 범위 보다 500인 전송 범위 내에서 더 많은 링크가 연결되었고, 노드의 차수 또한 높다. 반면에 전송 범위가 300인 (b)에서는 많은 수의 노드가 하나의 인접노드만을 갖고 있다는 것을 확인했다.

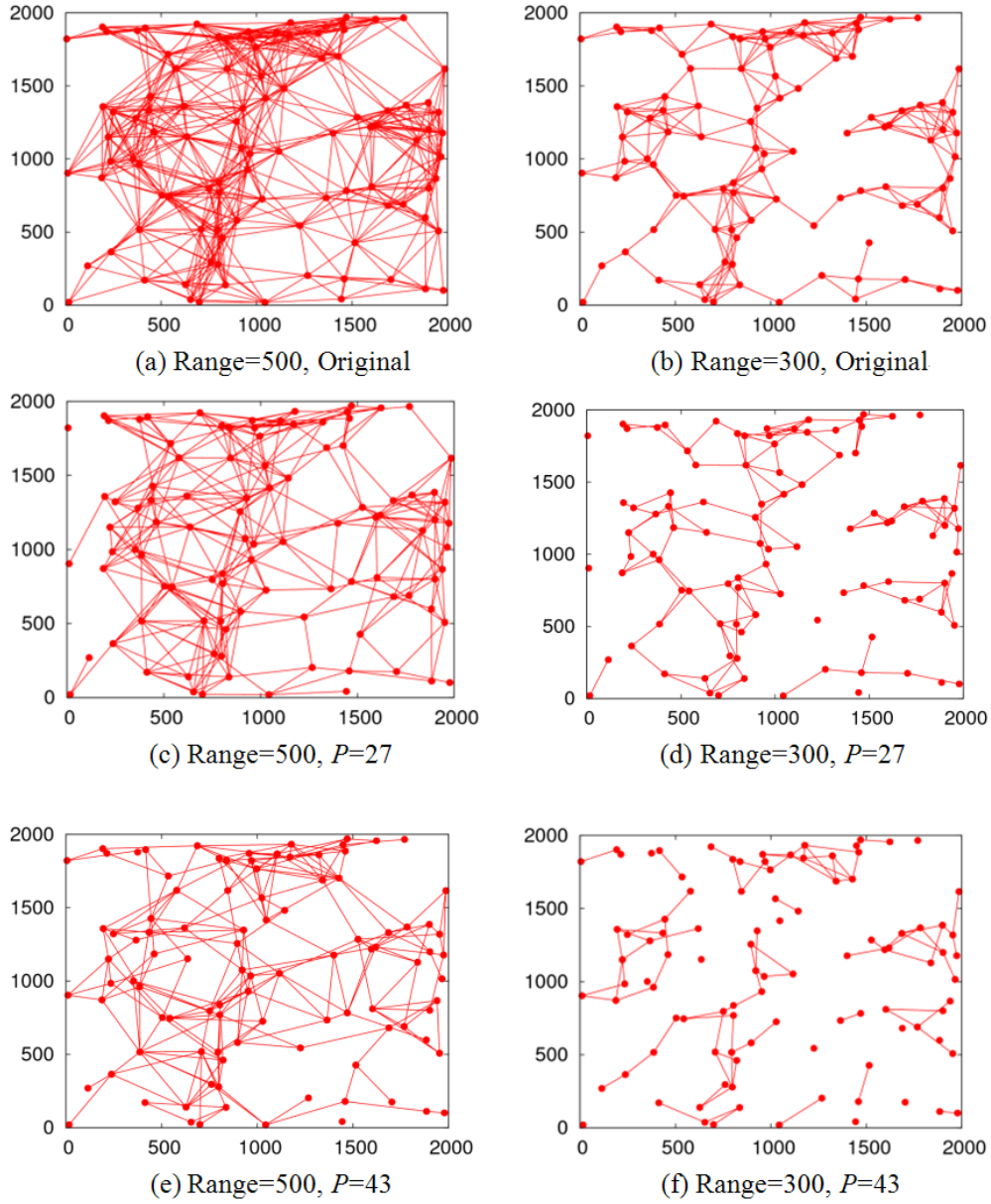
위의 토폴로지(Original Topology : 키 풀이 없는 토폴로지, 통신 범위 안에 존재 하는 모든 노드와 연결한다.)에서 RS 키 분배 기법을 통해 안전한 링크를 만드는 과정을 키 풀의 크기가 27과 43인 경우로 나누어 비교하였다. 각 노드는 200개의 키 값을 유지할 수 있다고 가정하였다. 그리고 Polynomial의 차수는 49로 가정하여, 50개의 계수 (Coefficient)를 저장하여야한다. 따라서 각 노드는 4개의 Polynomial share를 가질 수 있다.

키 풀 사이즈가 27일 때는 0.5의 연결확률(두 노드가 하나의 공통키를 가질 확률)을 보이고, 키 풀 사이즈가 43일 때는 0.33의 연결확률을 보인다. 이 때 이 연결확률이 감소할수록, 앞서 보았던 토폴로지(Original Topology)가 낮은 노드 차수 (degree, 인접 노드의 수)를 갖는 토폴로지로 축소되는 것을 (그림 7-1)의 (c), (d), (e), (f)를 통해 확인 할 수 있다. 그 이유는 0.5와 0.33의 물리

적인 링크만이 공통 Polynomial을 가지게 되어 안전한 통신에 사용될 수 있기 때문이다.

(그림 7-1)의 (d)와 (f)에서 보는 것과 같이 연결확률이 1이 아닌 경우, 센서 네트워크가 여러 개의 component로 분할되어(그래프 이론에서의 components) 다른 그룹과 통신할 수 없게 되는 문제가 발생한다. 이 경우 원래 토폴로지인 (b)에서 보는 것과 같이 여전히 물리적인 네트워크 자체는 연결되어 있기 때문에, 각 분리된 그룹 간에 통신을 하기 위해서는 Key 서버나, Sink Node의 도움이 필요하게 된다.

앞의 결과 토폴로지에서 연결 확률에 대한 효과를 명확히 하기 위해, 키 풀 크기 P를 10에서 50까지 값을 사용해 보았다. 결과적으로 P가 클수록 연결 확률이 낮음을 알 수 있다. 이 실험에서 RS 키 분배 기법에서 P 이외의 다른 값은 앞 실험과 같다.



(a) Range=500, Original (b) Range=300, Original

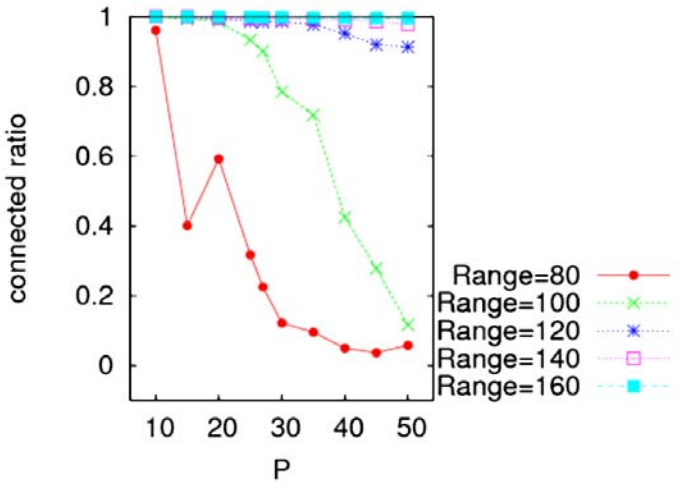
(c) Range=500, *P*=27 (d) Range=300, *P*=27

(e) Range=500, *P*=43 (f) Range=300, *P*=43

(그림 7-1) 다양한 통신 범위와 키 풀 사이즈 P에 대한 토폴로지

o 노드의 수 : 100 개
o 공간 범위 : 2000×2000
o 키 풀(key pool) 사이즈 P : original, 27, 43
o 전송 범위(Range) : 300, 500

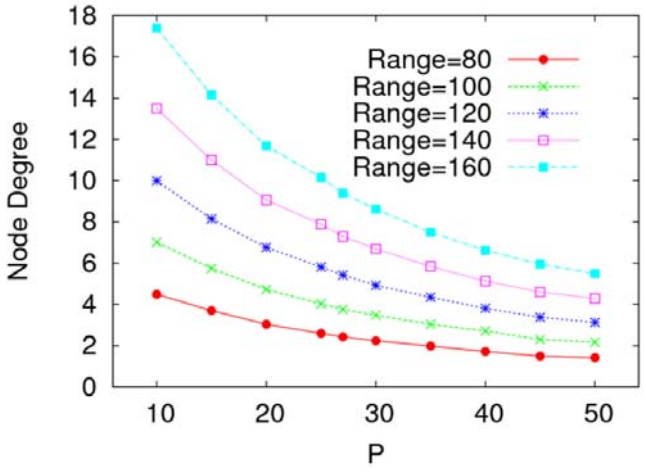
(그림 7-2)는 Original 토폴로지에서 위 파라미터 값들을 적용하여 생성한 토폴로지의 부분 그룹(Components)들 중에서 최대 연결 컴포넌트와 Original 토폴로지의 최대 연결 컴포넌트의 비율을 보여준다. 예를 들면 Original 토폴로지의 최대 연결을 가진 컴포넌트의 노드수가 100개이고, 생성된 토폴로지의 최대 연결을 가진 컴포넌트의 노드수가 80개라면, 이 비율 값은 0.8인 것이다. 이 성능 분석을 위해 1000개의 노드를 2000X2000 공간에 생성한다. 앞의 실험(그림 7-1)보다 노드 밀도가 10배 증가하기 때문에, 통신 범위를 80에서 160까지 변화를 준다. (그림 7-2)에서 키 풀 사이즈가 증가 할수록 연결 비율이 감소하는 것을 보였다. 연결 비율의 감소는 통신 반경이 작을 때(80~100) 더 많이 나타났다. 통신 범위가 작은 Original 토폴로지가 더 작은 노드의 차수(degree)를 가지게 되고, 이 상태에서는 토폴로지의 특정 링크들이 제거되어 토폴로지가 분리되는 가능성이 높아지기 때문이다.



(그림 7-2) 기본 토폴로지가 다양한 통신 범위에서 키 풀 사이즈에 따라 변하는 연결 비율

o 노드의 수 : 1000 개
o 공간 범위 : 2000×2000
o 키 풀(key pool) 사이즈 P : 10, 20, 30, 40, 50
o 통신 범위 : 80, 100, 120, 140, 160

노드 차수(degree)의 감소는 (그림 7-3)에서 나타난다. 키 풀의 크기가 증가하면서 평균 노드 차수(degree)는 감소한다. 통신 범위가 더 커질수록 평균 노드 차수는 18까지 커진다. 그러나 낮은 연결 확률(키 풀 크기 값이 큰) 때문에, 노드의 차수는 2까지 작아지게 된다. 낮은 평균 노드 차수(degree)는 네트워크의 분할을 초래하며, 이는 (그림 7-2)에서 명확하게 볼 수 있다.



(그림 7-3) 키 풀 사이즈 P에 대한 노드 차수(degree)

이와 같은 시뮬레이션 결과를 통해 키 풀 사이즈 P 값을 크게 하여 임의로 연결 확률을 줄이면 안 된다는 것을 확인했다. 하지만 앞의 연구에서 연결 확률이 낮으면 노드 캡쳐 공격에 대항하는 보안성능이 높아짐을 볼 수 있다. 따라서 높은 연결 확률에서도 보안 성능을 향상시킬 방법을 연구해야 한다.

이상의 시뮬레이션의 결과를 통해 알 수 있는 것은, 기존의 Polynomial 기반의 RS 기법에서 보안 성능을 향상시키기 위해 링크의 연결확률을 줄이는 경우가 있는데, 이것은 통신 범위의 제한에 따라 센서 네트워크가 여러 개의 component로 분할되는 결과를 가져올 수가 있게 된다는 것이다. 즉 특정 기법의 성능을 보여줄 경우에 그 성능이 센서 네트워크를 분할하지 않도록 해야 그 성능이 올바르게 도출되었다고 할 수 있다.

위에서 실행한 다양한 실험의 결과를 바탕으로 다음 절에서는 각 센서 네트워크의 성능을 실험할 때 적절한 통신 범위와 연결확률을 유지하면서 성능을 비교하도록 한다.

제 2 절 다양한 센서 네트워크에서의 통합 프레임워크의 성능

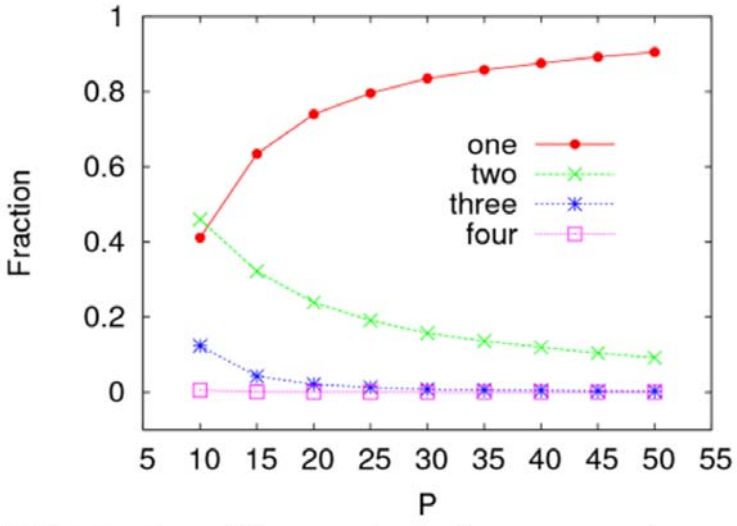
이 절에서는 통합된 키 분배 프레임워크가 다양한 센서 네트워크 상황에서 얼마나 높은 성능으로 적용 되는지를 평가 한다. 통합된 키 분배는 여러 부분에서 RS(Random subset)[168]을 기반으로 하였기 때문에 RS와 통합 프레임워크를 비교한다. 또한 사전 키 분배 기법의 초기 기법인 랜덤 키 사전 분배 기법과도 비교한다.

1. 단일 토폴로지에서의 통합 프레임워크의 성능

첫째로 강화된 직접 키 확립 옵션이 어느 정도 보안을 향상시키는지 살펴본다. 직관적으로 봤을 때 하나의 공통 Polynomial 대신에 복수개의 공통 Polynomial을 사용하여 링크 (세션 키)를 설정하기 때문에 안정성을 높일 수 있음을 알 수 있다. 이 강화된 직접 키 확립 옵션이 얼마나 많은 성과를 올릴 수 있는지 보기 위해서, 우선 각 안전한 링크에 존재하는 공통 Polynomial 수의 분포를 살펴본다. 이 시뮬레이션에서, 150의 전송 범위를 가진 2000×2000 영역에 1000 개의 노드를 생성하고, 파라미터의 값을 P=27, k=4, t=29로 설정한다. 메모리 사이즈 m=200이 된다.

(그림 7-4)은 키 풀 사이즈 P를 변화에 따라 공통 Polynomial의 각각 수의 비율(fraction)을 보여준다. (그림 7-4)에서 볼 수 있듯이 연결 확률이 높을 때 (낮은 키 풀 사이즈 P) 복수 개 공통키의 비율이 하나의 공통키보다 높아졌다. 이것으로 강한 연결성이 필요할 때(즉 두 개의 인접 노드 사이에 세션 키를 설정하는 연결 확률을 높이고자 할 때)는 강화된 직접 키 확립 옵션이 복수개

의 공통 Polynomial을 이용할 수 있기 때문에 더 높은 보안 성능을 보일 가능성이 있음을 알 수 있다.

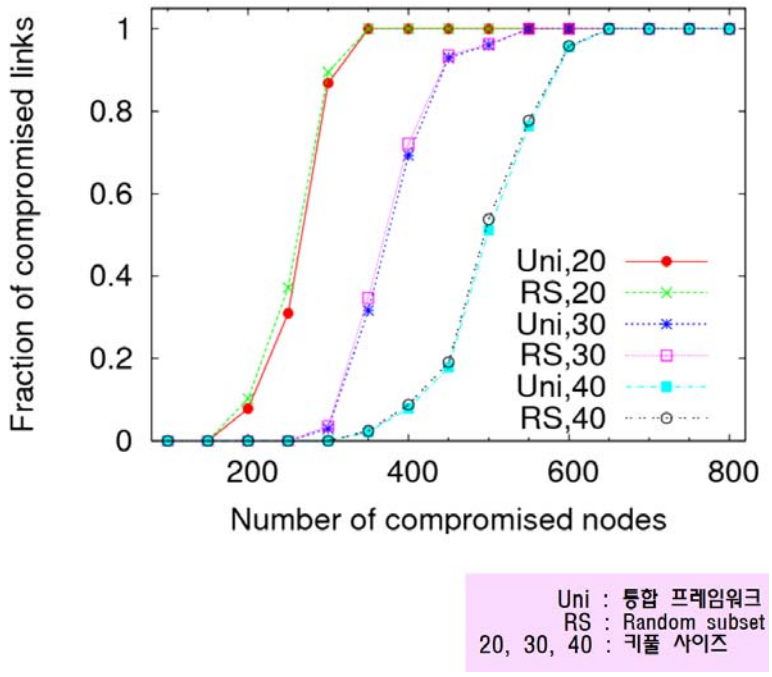


(그림 7-4) 일반적인 polynomial의 수에 따른 분배

o 노드의 수 : 1000 개
o 공간 범위 : 2000×2000
o 전송 범위 : 150
o P(키 풀 사이즈) : 10, 20, 30, 40, 50
o t(degree) : 49
o m(메모리, 센서 노드가 보유 할 수 있는 키의 수) : 200
o k(한 센서 노드 보유하고 있는 polynomial의 수) : 4

이것은 (그림 7-5)에서 정확하게 볼 수 있다. 1000개의 같은 노드를 분배할 때, 다양한 노드들을 랜덤하게 선택하여 캡쳐 한다. 노드들이 캡쳐가 된 후에, 캡쳐가 되지 않은 노드들 간의 링크는 영향을 받지 않아야 정상이지만 Polynomial의 집합이 제한적이기 때문에 이러한 링크들의 세션 키가 노출되는 현상이 발생한다. 따라서 캡쳐 되지 않은 노드들 간의 전체 링크 중에서 캡쳐된 링크의 비율을 계산하여 이 비율이 어느 정도인지를 살펴보도록 한다. 이

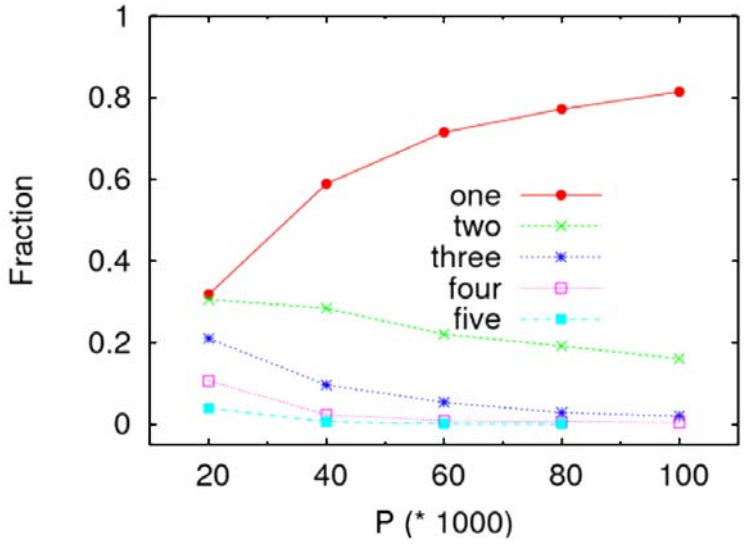
비율이 낮을수록 좋은 보안 성능을 보이는 것이다. 다양한 상황에서의 성능을 비교하기 위해 캡쳐 된 노드의 수는 50에서 800까지 변화를 준다. 키 “Uni"은 본 보고서에서 제안한 통합된 프레임 워크를 의미하고 ”RS"는 RS 시스템을 의미한다. 그림의 키 안의 수는 P 값을 의미한다. 파라미터 k와 t는 이전과 같다.



(그림 7-5) 통합 프레임워크와 RS의 보안 레벨

o 노드의 수 : 1000 개
o 공간 범위 : 2000×2000
o 전송 범위 : 150
o P(키 풀 사이즈) : 20, 30, 40
o t(degree) : 49
o m(메모리, 센서 노드가 보유 할 수 있는 키의 수) : 200
o k(한 센서 노드 보유하고 있는 polynomial의 수) : 4
o 캡쳐 된 노드의 수 : 50 ~ 800

(그림 7-5)에서 보듯이, 본 보고서에서 제안한 통합 프레임워크는 낮은 P 값(높은 연결 확률)에서 RS 시스템의 성능을 5-20% 능가하였다. 그러나 P가 증가할수록 그 성과가 줄어들었다. (그림 7-4)에서 볼 수 있듯이, P 값이 증가할수록 많은 Polynomial shares의 비율이 줄어들었다. 이것으로 높은 연결 확률이 필요하여 작은 P 값을 사용해야 하는 경우 강화된 직접 키 확립 옵션을 사용하는 것이 보안 성능을 향상시킴을 알 수 있다.

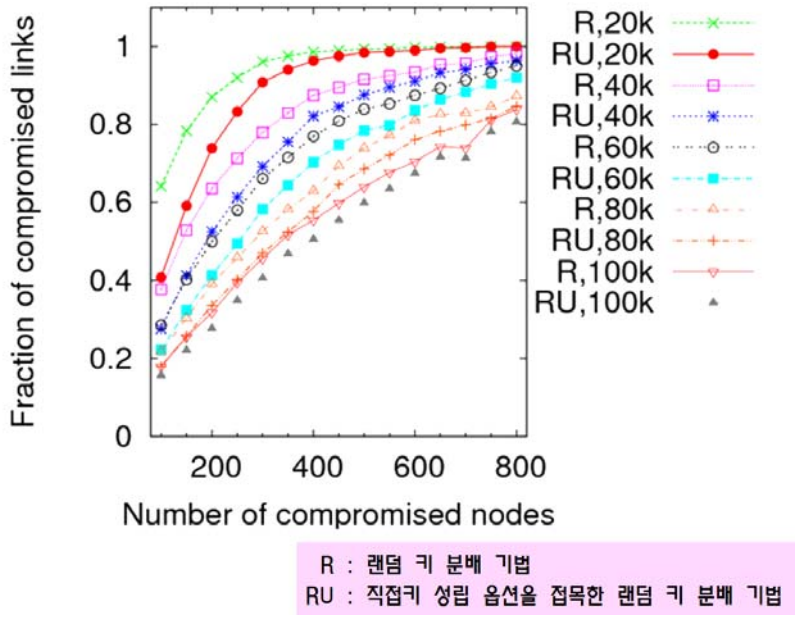


(그림 7-6) 랜덤 키 분배에서 일반적인 polynomial의 수에 따른 분배

o 노드의 수 : 1000 개
o 공간 범위 : 2000×2000
o 전송 범위 : 150
o P(키 풀 사이즈) : 20000 ~ 100000
o t(degree) : 49
o m(메모리, 센서 노드가 보유 할 수 있는 키의 수) : 200
o k(한 센서 노드 보유하고 있는 polynomial의 수) : 1 ~ 5

강화된 직접 키 확립 옵션은 공통키를 기반으로 하여 세션 키를 생성하는 랜덤 키 사전분배 기법에도 적용 할 수 있다. 이 적용의 성과를 예측하기 위해 랜덤 키 분배 시스템 상에서 공통키의 수의 분포를 살펴본다. 풀 사이즈 P는 20,000에서 100,000으로 변화를 주어, 연결 확률이 0.33에서 0.85까지 변하도록 하였다. RS와 마찬가지로 P가 낮을수록 연결 확률이 높아진다.

이 시뮬레이션에서, 캡쳐 된 노드의 숫자를 50에서 800까지 변화시켜 캡쳐되지 않은 노드들 간의 전체 링크 중에서 캡쳐 된 링크의 비율을 계산하였다. 여기서 'R'은 랜덤 키 분배 기법이고 'RU'는 강화된 직접 키 성립 옵션을 접목한 랜덤 키 분배 기법을 의미한다. 20,000 정도의 낮은 P 값의 경우에는 20%의 성능향상을 보여주었다.

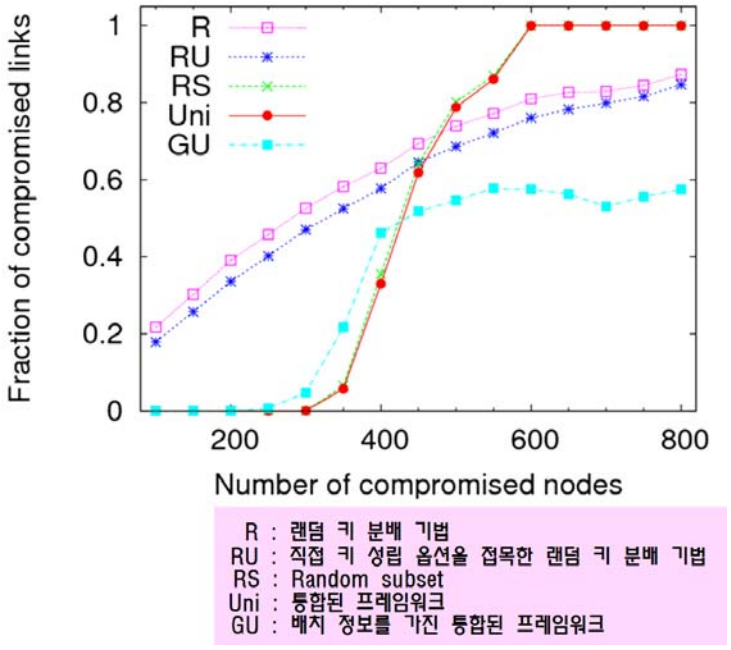


(그림 7-7) 랜덤 기법과 통합 프레임워크의 보안 레벨

o P(키 풀 사이즈) : 20000
o k : 20, 40, 60, 80, 100
o 캡쳐 된 노드의 수 : 50 ~ 800

모든 세팅에서 보듯이 'RU'가 랜덤 기법보다 성능이 더 좋다는 것을 알 수 있다. (그림 7-7)의 키의 숫자는 P의 크기를 의미하는데, k는 1,000을 의미한다. 즉 20k는 20,000이다.

마지막으로 분배 정보가 있을 때 통합 프레임워크의 성능을 관찰하기 위해서 랜덤과 RS 기법에 대한 분배 정보에 대한 경우를 비교하였다. (그림 7-8)은 캡쳐 되지 않은 노드들 간의 전체 링크 중에서 캡쳐 된 링크의 비율을 보여준다. 랜덤 기법('R')에 대한 키 풀 사이즈 P는 80,000으로 맞추었다. RS 기법('RS')과 통합 프레임워크('Uni')에 대한 키 풀 사이즈 P는 35이며, k=4, t=49, m=200에 맞추었다. 분배 정보를 접목시킨 통합 프레임워크('GU')는 k=5, t=39, m=200 그리고 ss=40이다. 이 경우, 키 풀의 사이즈는 영역 내의 사각형의 수와 같다. (그림 7-8)에서 보듯이 강화된 직접 키 확립 옵션 성능이 좋다. 캡쳐 된 노드의 수가 적을 때, "GU" 성능은 "RS"보다 나쁘지만, 캡쳐 된 노드의 수가 400 개 이상으로 올라갈 경우에는 캡쳐 되는 링크의 수의 비율이 거의 일정하다.

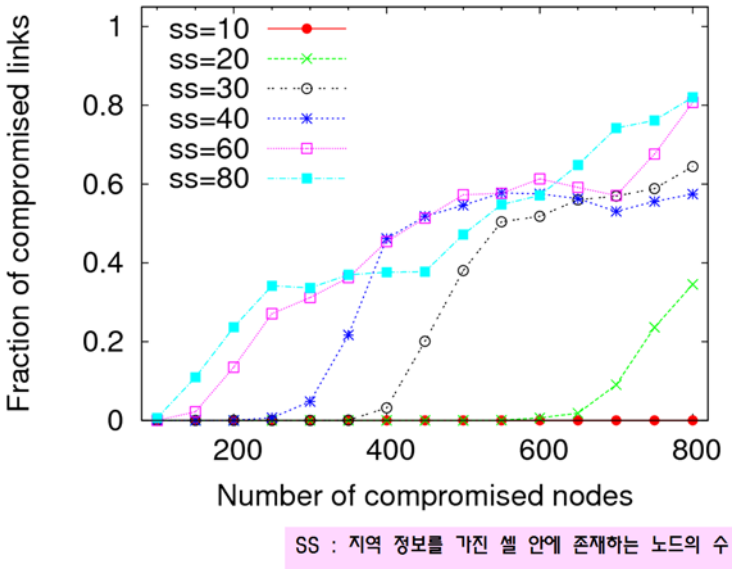


(그림 7-8) 배치 정보를 가진 보안 레벨

o P : R - 80000 / RS, Uni - 35
o k : RS, Uni - 4 / GU - 5
o t : RS, Uni - 49 / GU - 39
o m : 200
o ss(각 사각형 안에 존재하는 노드의 수) : 40

실제로, "GU"의 성능은 같은 사각형 안에 있는 노드의 수에 의존한다. 따라서 ss(배치 정보를 가진 셀 안의 노드의 수) 숫자가 안정성 성능에 미치는 영향을 알아보기 위해서, 다른 파라미터를 그대로 유지한 채 ss를 10에서 80까지 변화시켜서 캡쳐 되지 않은 노드 사이의 캡쳐 된 링크의 비율을 계산한다. (그림 7-9)에서 보는 것과 같이 ss와 캡쳐 된 노드의 수가 증가 할수록 캡쳐 된 링크의 비율이 증가한다. 이것으로 ss=10일 때 캡쳐 된 링크가 없다는 것을 알 수 있다. 그 이유는 ss가 10일 때 최대 50 개의 노드만 하나의 Polynomial을 갖기 때문이다. 하지만 Polynomial의 차수가 40이고 공통 Polynomial의 가장 낮은 수가 2개이기 때문에, 공격자가 하나의 Polynomial을 가지기 위해서 최소 40개의 센서 노드를 캡쳐 해야 한다. 그러나 랜덤 노드 캡쳐 상황에서는 하나의 Polynomial로부터 40개 이상의 센서 노드를 캡쳐 하는 것은 어렵다. 하지만 같은 Polynomial을 가진 노드만을 캡쳐 하는 방식의 공격일 경우에는 캡쳐 되지 않은 노드 간의 통신 링크를 캡처할 수도 있다. 그러나 이러한 공격은 같은 Polynomial을 가진 모든 노드들이 Polynomial의 사각형과 인접한 5개의 사각형 내에 있는 로컬에 국한된다. 따라서 이러한 영향은 오로지 특정 지역으로만 제한된다.

향상된 성능 외에, 분배 정보를 가진 통합된 프레임 워크는 인접한 사각형의 모든 쌍이 두 개의 Polynomial 공유를 가지고 있기 때문에 기존의 토폴로지를 유지한다. 높은 연결성이 센서 노드부터 싱크 노드까지 복수 개의 경로를 가능하게 했다. 따라서 싱크 노드까지 다양한 경로를 가짐으로써 센서 노드의 에너지를 절약하는데 이용될 수 있다.



(그림 7-9) ss 값에 대한 배치 정보를 가진 노드의 보안 레벨

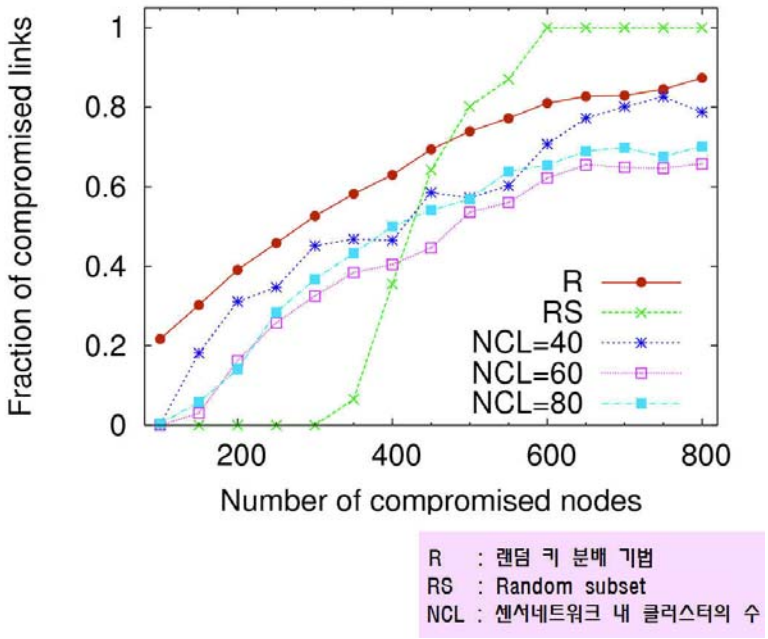
o 캡쳐 된 노드의 수 : 50 ~ 800 o ss : 10, 20, 30, 40, 60, 80

2. 클러스터 토폴로지에서의 통합 프레임워크의 성능

여기서 클러스터 된 토폴로지들에서의 통합 프레임워크의 성능을 분석한다. 여기에서는 클러스터 멤버십(cluster membership) 정보가 주어지기 때문에 클러스터에 속해 있는 노드들을 알 수 있다고 가정한다. 또한 클러스터들 사이에서 이웃의 관계가 주어진다고 가정한다. 이러한 상황을 시뮬레이션 하기 위해, 클러스터링 멤버십과 이웃 클러스터 정보를 생성할 필요가 있다. 센서 네트워크에서 특별한 클러스터링 알고리즘이 많이 있지만 우리는 간단한 클러스터링 알고리즘을 선택한다. 이 알고리즘에서, 직사각형 안에 k개의 포인트(주요 포인트)를 선택한다. 다음으로 직사각형 안에서 노드의 위치를 랜덤하게 발생시킨다. 그리고 각 노드에서 가장 가까운 주요 포인트를 계산한다. 가장 가까운 주요 포인트가 같은 노드는 같은 클러스터에 속한다. 클러스터의 각 쌍

에서, 만약 통신 범위 내에 속한 두 클러스터 안의 두 노드가 있다면 두 클러스터는 이웃 클러스터가 된다. 단 생성되는 클러스터링 정보에 대해서만 노드의 위치를 사용한다.

클러스터의 수는 40, 60, 80으로 설정한다. 또한 노드의 수는 1,000개이며, 통신범위는 150으로 설정한다. (그림 7-10)은 캡쳐 된 노드의 수에 따라 캡쳐된 링크의 비율이 증가함을 보여준다. 키 NCL은 센서 네트워크 내 클러스터의 수를 의미한다.



(그림 7-10) 클러스터의 수에 대한 클러스터링 정보를 가진 보안 레벨

o NCL(센서 네트워크 내의 클러스터의 수) : 40, 60, 80
o 노드의 수 : 1000 개
o 전송 범위 : 150
o 캡쳐 된 노드의 수 : 50 ~ 800
o ss(각 셀 안에 존재하는 노드의 수) : 10, 20, 30, 40, 60, 80

(그림 7-10)에서 볼 수 있듯이, 통합 프레임워크는 기존의 랜덤 키 분배 기법보다 더 좋은 성능을 보인다. 클러스터의 수의 변화는 성능에 크게 영향을 미치지 않는다. 캡쳐 된 노드의 수가 적을 때는, RS 기법이 통합 프레임워크에 비해 더 좋은 성능을 보인다. 지리적으로 위치 정보가 주어진 경우와 다르게 클러스터링 정보는 통합 프레임워크가 그 특성을 활용할 수 있는 여지가 적었음을 알 수 있다. 이 이유는 아마도 이 보고서에서 제시된 클러스터링 정보 활용 기법이 좋지 못하기 때문일 것이다. 또는 클러스터링 정보가 보안 성능에 중요하게 작용하지 않는 것 일 가능성도 있다.

간략하게 정리하면, 클러스터를 가지는 토폴로지의 경우, 캡쳐 된 노드의 수가 작을 때 이 클러스터링 정보를 이용하여 통합 프레임워크를 적용하는 것이 RS 기법에 비해 낮은 보안성능을 보여주었다. 하지만 캡쳐 된 노드의 수가 증가할 경우에는 RS 기법에 비해 높은 성능을 보여줌을 알 수 있다. 이와 더불어 캡쳐 된 노드의 수에 상관없이, 통합 프레임워크는 랜덤 키 사전 분배 기법에 비해서는 더 나은 성능을 보여준다.

제 8 장 결론

이 보고서에서는 센서 네트워크에서 사용하는 다양한 키 관리 기법에 대해 조사하고, 몇 가지 키 관리 기법에 대해서 성능을 정성적 및 정량적으로 비교하였다. 구체적으로 USN 환경에서 사용되는 키 관리 기법 들 중에서 사전키 기반 분배 기법(마스터 키, Pairwise 키(Random Pairwise key), 확률론적 키(Blom's Polynomial, q-합성수, Multi-path), 그룹 키), 공개키 기반 분배 기법(ECC, ECDH)들에 대한 개요와 장단점을 분석하였고, SPIN과 LEAP과 같은 센서 네트워크 보안 프로토콜을 요약하여 기술하였다.

또한 이러한 키 관리 기법이 필요한 요인인 USN에 대한 다양한 공격 형태, 예를 들면 도청, 데이터 위변조, 서비스 거부 공격, 라우팅 공격, 물리적 공격과 같은 여러 공격 형태를 조사하고, 이를 다양한 기준에 의해 분류하여 좀 더 효과적으로 공격을 이해하고, 이를 방어하기 위한 키 관리 기법을 선택할 수 있는 기준을 제시하였다.

이와 더불어 USN 보안 기술 표준화 동향과 u-City 시범 서비스에 대한 조사와 분석을 진행하였는데, 이러한 기반 기술 및 동향에 대한 연구를 바탕으로 이 연구에서는 USN 환경에서 센서 네트워크의 형태 별로 키 관리 기법을 달리하는 것이 보안의 성능을 향상시키는데 필수적임을 지적하였다. 이러한 키 관리 기법 적용 모델을 바탕으로 다양한 키 관리 기법을 하나의 통합된 키 관리 프레임워크에서 구현할 수 있는 통합 키 사전 분배 프레임워크를 제시하였다. 이 통합 프레임워크는 기존의 주요한 키 관리 기법을 표현할 수 있으며, 기존 기법이 가지지 못하는 통합 프레임워크만의 장점을 가지고 있다.

본 보고서에서는 이러한 키 관리 기법 적용 모델의 성능을 통합 프레임워크를 기반으로 시뮬레이션을 통해 분석하고, 이 연구에서 제시한 모델과 통합 프레임워크가 효율적임을 보였다. 향후에는 좀 더 실제적인 토폴로지를 이용한 성능 분석과 구현 시 발생하는 문제점을 검토하고자 한다.

참고문헌

[1] 신수연, 권태경, “센서네트워크의 랜덤 키 설정 기법에 관한 연구”, 2005년도 한국정보과학회 한국컴퓨터종합학술대회 논문집 제32권 제1호(A), pp.118~120, 2005.

[2] 박익수, 오병균, “USN에서 보안 프로토콜에 관한 연구”, 2006년도 한국정보과학회 한국컴퓨터종합학술대회 논문집(C), pp.325~327, 2006.

[3] 조관태, 이화성, 김용호, 이동훈, “유비쿼터스 센서 네트워크에서의 키 분배 프로토콜 구현 및 분석”, 2008년도 한국정보보호학회 하계정보보호학술대회 논문집 제16권 제1호, pp.599~603, 2008.

[4] 이경호, 정석원 오병균, “U-센서네트워크에서의 Pairwise Key 설정 기법”, 2006년도 한국정보과학회 가을 학술발표논문집 제33권 제2호(C), pp. 552~555, 2006.

[5] 곽진, 오수현, “분산 센서 네트워크용 키 분배 프로토콜 연구 동향”, 2007년도 정보통신연구진흥원 주간기술동향 제1307호, pp.1~9, 2007.

[6] 이석준, 오경희, 김호원, 정병호, "USN 공격 기법 및 보안 기술 동향", 한국 인터넷 정보학회, 제9권 제1호, pp.34~43, 2008.

[7] 권태경, 신수연, 박상호, 박태진, “무선 센서 네트워크 보안”, 2006년도 한국통신학회지(정보통신) 제23권 제9호, pp.88~102, 2006.

[8] 김광조, “RFID/USN 정보보호 기술”, TTA저널 95호.

[9] 홍도원, 장구영, 박태준, 정교일, “유비쿼터스 환경을 위한 암호 기술 동향”, 2005년도 ETRI 전자통신동향분석 제20권 제1호, pp.63~72, 2005.

[10] 나재훈, 채기준, 정교일, “센서 네트워크 보안 연구 동향”, 2005년도 ETRI 전자통신동향분석 제20권 제1호 2005.

[11] 박정현, 임선배, 이경준, “이동통신에서 안전성을 위한 키 관리”, 1998년도, 정보통신연구진흥원, 1998.

[12] 오경희, 김태성, 김호원, “공개 암호 키를 사용한 센서 네트워크에서의 키 분배 구현,” 한국방송공학회, 2008, pp.95-98.

[13] 이향진, 이홍섭, “공개키 기반구조와 전자서명”, 2002년도 전자공학회지 제29권 제3호, pp.71~79, 2002.

[14] 한국정보보호센타, “국내 공개키 기반구조 구축방안 연구”, 1998년도IITA 정보통신연구진흥원, 1998.

[15] Wenliang Du , Jing Deng , Yunghsiang S. Han , Pramod K. Varshney, “A Pairwise key pre-distribution scheme for wireless sensor networks”, in Proceedings of the 10th ACM conference on Computer and communications security, October 27-30, 2003, Washington D.C., USA.

[16] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proceedings of the 9th ACM conference on Computer and communications security. Washington D.C., USA: ACM Press, 2002, pp. 41–47.

[17] 이재원, 허준, 홍충선, "WSN 환경에서 논리적 그룹 형성과 키 분배 방법“, 2007년도 정보과학회 논문지 : 정보통신 제34권 제4호, pp.296~304, 2007.

[18] 강지명, 이성렬, 조성호, 김종권, 안정철, “센서 네트워크에서의 쿼럼 시스템을 이용한 키 사전 분배”, 2006년도 정보과학회논문지: 정보통신 제33권 제3호, pp.193~200, 2006.

[19] 정윤수, 김용태, 박길철, 이상호, “무선 센서 노드의 강한 보안 강도를 위해 이중 해쉬 체인을 적용한 키 사전 분배 기법”, 2008년도 한국통신학회 논문지 제33권 제8호(통신이론 및 시스템), pp.633~641, 2008.

[20] 설정환, “홈네트워크 서비스를 위한 인증 서버 설계 및 구현”, 2008년도 인천대 대학원 석사학위논문 pp12~16.

[21] 한국정보보호학회, “현대 암호학 및 응용”, 한국정보보호진흥원, 2002.

[22] R Blom, "An optimal class of symmetric key generation systems", In Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques, pp.335~338, New York, NY, USA, 1985. Springer-Verlag New York, Inc., 1984.

[23] 김장성, 권미영, 김이형, 곽민혜, 한규석, 김광조, “감시정찰 센서네트워크

및 주요 시설물 관리에서의 키관리 기법 비교”, 2008년도 한국정보보호학회 충청지부 학술발표회 논문집, pp.75-83, 2008.

[24] 양대헌, 모하이센 아브델아지즈, “정적 무선 센서 네트워크를 위한 강한 연결성을 가진 계층적 그리드 기반의 키 선분배 기법”, 전자공학회논문지 제43권제7호, pp.14~23, 2006.

[25] 윤미연, “유비쿼터스 센서네트워크에서 에너지효율을 고려하는 비동기적인 키관리 기법”, 2006년도 한국통신학회논문지 제31권 제10C호, pp.1011~1022, 2006.

[26] 조정식, 여상수, 김성권, “무선 센서 네트워크에서의 향상된 키 분배 기법”, 2005년도 한국정보과학회 한국컴퓨터종합학술대회 논문집(A) 제32권 제1호, pp.151153, 2005.

[27] Diffie, W., Hellman, M. E., "New directions in cryptography", IEEE Trans, Inform. Theory, IT-22, pp,.644~654, November 1976.

[28] V. Boyko, P.D. MacKenzie, S. Patel, “Provably secure password-authenticated key exchange using Diffie-Hellman”, in: Advances in Cryptology--Proceedings of EUROCRYPT 2000, in: Lecture Notes in Comput. Sci., vol. 1807, Springer-Verlag, 2000, pp. 156-171.

[29] S. Zhu, S. Setia, S. Jajodia, "LEAP: Efficient security mechanism for large-scale distributed sensor networks", In 10th ACM Conference on Computer and Communications Security (CCS'03), 2003a.

[30] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler, "SPINS: security protocols for sensor networks," Wireless Networks, Volume 8, Issue 5, pp 521 - 534, 2002.

[31] 이동훈, "USN 정보 보호 기술 동향", [IITA] 정보통신연구진흥원 학술정보 - 주간기술동향 1212호.

[32] 박용수, 김일희, 김희문, “USN 환경에서의 분산형 인증체계 연구”, 한국정보보호진흥원.

[33] 이주영, 권대성, “센서 네트워크에서의 키 사전 분배”, 2008년도, Springer Science+Business Media, LLC 2008.

[34] 정성은, 염희운, “안전한 그룹 키 분산 기법에 관한 연구” 2001년도 한국정보과학회 가을 학술발표논문집 제28권 제2호(1), pp.748~750, 2001.

[35] 김신효, 강유성, 정병호, 정교일, “U-센서 네트워크 보안 기술 동향,” 전자통신동향분석 제20권 제1호, pp.93-94, 2005.

[36] 이신경, 이해동, 정교일, 최두호, “안전한 USN을 위한 정보보호기술 동향”, 전자통신동향분석 제 23권 제 4호, 2008.

[37] 신 승 수, 최 승 권, 지 홍 일, 신 동 화, 조 용 환, “무선 PKI에서의 블러킹 확률 분석,” 한국통신학회논문지 ’05-5 Vol.30 No.5A.

[38] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K. Varshney, “A key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge”, in Proc. IEEE INFOCOM 2004, vol. 1, pp. 586-597, 2004.

[39] Felix Freiling, Zinaida Benenson, "Attacker Models for Wireless Sensor Network", Summer School "Protocols and Security for Wireless Sensor Actor Networks" Schloss Dagstuhl, 2008.

[40] Chung Kei Wong, Mohamed Gouda, and Simon S. Lam, "Secure Group Communications Using Key Graphs," in IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 8, NO. 1, FEBRUARY 2000.

[41] Yun Zhou, Yanchao Zhang, and Yuguang Fang, "LLK: A Link-Layer Key Establishment Scheme for Wireless Sensor Networks," in the Proceedings of IEEE Wireless Communications and Networking Conference, 2005, March 2005.

[42] Kyung-suk Lhee, "Memory-Efficient Hypercube Key Establishment Scheme for Micro-Sensor Networks," ETRI Journal, Volume 30, Number 3, June 2008.

[43] H. Chan and A. Perrig, “PIKE: Peer Intermediaries for Key Establishment in Sensor Networks,” Proc. INFOCOM, pp. 524-535, 2005.

[44] Scott C.-H. Huang and Ding-Zhu Du, "New Constructions On

Broadcast Encryption and Key Pre-Distribution Schemes," in Proc. of INFOCOM 2005, March 2005.

[45] Zeen Kim, Jangseong Kim, Kwangjo Kim, "Key Predistribution Scheme for Wireless Sensor Networks with Higher Connectivity," in Proc. of SCIS 2007, Sasebo, Japan, Jan. pp23-26, 2007.

[46] Donggang Liu and Peng Ning, "Improving key predistribution with deployment knowledge in static sensor networks," ACM Transactions on Sensor Networks (TOSN), Volume 1, Issue 2, November 2005, pp 204 - 239.

[47] H. Harney and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture," RFC 2094.

[48] Seung Bae Park, Moon Seol Kang, and Sang Jun Lee, “Authenticated Key Exchange Protocol Secure against Offline Dictionary Attack and Server Compromise,” GCC 2003, LNCS 3032, pp. 924.931, 2004.

[49] Jooyoung Lee, and Douglas R. Stinson, “Deterministic Key Predistribution Schemes for Distributed Sensor Networks,” in Proc. of SAC 2004, LNCS 3357, pp. 294-307, 2005.

[50] Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," in Proceedings of 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 1992.

[51] 윤종호, “윈도우 서버와 프로토콜 분석기를 활용한 네트워크 보안 프로토콜”, 교학사, 2004.

[52] Bergriyz A. Forouzan 저, 손승원, 이재관, 임종인, 전태일 역, “Cryptography and Network Security, 암호학과 네트워크 보안”, McGraw-hill(한국 맥그로힐), 2008.

[53] William Stallings 저, 소우영, 이재관, 이임영 역, “Cryptography and Network Security., 컴퓨터 통신보안”, Prentice Gall(도서출판 그림), 2003.

[54] H.X.Mel, Doris Baker 저, 정재원, 류대걸, 강한 역, “Cryptography

Decrypted, 보안과 암호화 모든 것”, Addison wesley(인포북), 2001.

[55] Mark Stamp 저, 안태남, 손용락, 이광석 역, “정보보안 이론과 실습”, 한빛미디어, 2006.

[56] 이문구, “정보보호개론”, 이한출판사, 2008.

[57] 한국정보보호학회, “차세대 네트워크 보안 기술”, 한국정보보호진흥원, 2002.

[58] 남상엽, 정교일, 김성동 저, “유비쿼터스 센서 네트워크 구조 및 응용”, 상학당, 2006..

[59] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu and M. Galloway, “A survey of key management schemes in wireless sensor networks”, Comput. Commun., vol. 30, pp. 2314~2341, 2007.

[60] 박익수, 오병균, "USN에서 보안 프로토콜에 관한 연구", 2006 한국컴퓨터종합학술대회 논문집 Vol.33,No.1(C), 2006.

[61] 정용진, 김종만, 김영필, 김성두, 이석용, 전신우 “스마트카드용 타원곡선 암호 알고리즘 (ECC) 하드웨어 설계에 관한 연구”, 정보통신연구진흥원, 2001.

[62] 위키백과 “http://ko.wikipedia.org"

[63] 김태호, 김창훈, 권순학, 홍춘표, :타원곡선 키 교환 프로토콜 응용을 위한 마이크로소프트 COM 소프트웨어 모듈 구현“, 2006년도, 한국통신학회, 2006년 하계종합학술발표회 논문 초록집 Vol.33, 6D-32 pp618, 2006.

[64] 최두호, 이신경, 이해동, 오경희, 이석준, 박남제, “안전한 USN을 위한 정보보호 현황”, 월간 정보보호21c 통권 제103호, 보안뉴스 (www.boannews.com)

[65] 이승혁, “타원곡선 암호알고리즘을 이용한 효율적인 디지털 컨텐츠 암호화 기법 연구”, 2004년도, JOURNAL OF INFORMATIION TECHNOLOGY APPLICATIONS & MANAGEMENT, 2004.

[66] 김호원, 이석준, 오경희, "센서네트워크 보안 기술 개발 동향", 한국정보보호학회지 제 18권 제 2호, 2008.

[67] 신순자, 임진수, “유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향

연구”, 한국 정보 사회 진흥원, 2004.
[68] 조영섭, 조상래, 유인태, 진승헌, 정교일, “유비쿼터스 컴퓨팅과 보안요구사항 분석”, 한국정보보호학회, 정보보호학회지 pp 21-~34, 2004.
[69] 강희조, 방기천, "유비쿼터스 컴퓨팅과 센서 네트워크 보안 기술에 관한 연구", 한국디지털정책학회 06 추계학술대회 pp387-395, 2006.
[70] 이웅용, 박광진, "USN 활성화를 위한 정보보호 요구사항", 한국통신학회. 한국통신학회지(정보와통신)제 21권 9호 pp132~142, 2004.
[71] 임채훈, "유비쿼터스 센서 네트워크 보안", 한국통신학회지 V.22.no.8 pp.35-50, 2005.
[72] 김윤진, 권혁태 공저, "유비쿼터스 개론", 문운당.
[73] 한국 RFID/USN협회, "*유비쿼터스 지식능력검정*", 영진미디어
[74] 김호원, 오희국, "유비쿼터스 보안 기술", 한국정보과학회 정보통신 소사이어티, 정보통신 기술 제 19권 제 2호, pp.59~73, 2005.
[75] 조현숙, 정교일, 최두호, 강유성, "RFID/USN 보안 기술 개발 동향", 한국전자파학회, 전자파기술 제19권 제6호, pp. 60 ~ 71, 2008.
[76] 김학범, "IP-USN 최신 기술 동향 및 보안 요구사항 분석", 한국정보보호학회, 정보보호학회지 제16권 제6호, pp. 64 ~ 73, 2006.
[77] C.Karlof and D.Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proc. 1st IEEE Int'l., Wksp. Sensor Network Protocols and Applications, May, 2003.
[78] 이동훈, "개인정보보호의 중요성과 보호 기술", 2007.
[79] 노선식, 김광현, 박기배, 박재선, 강철구, “RFID/USN 확산 저해요인 및 개선 대책 연구” 한국전산원, 2005.
[80] 정병호, 강유성, 김신효, 정교일, 양대헌, “RFID/USN 환경에서의 정보보호 소고”, 한국통신학회, 2004.
[81] 정태명, 엄정호, 한영주, 박선호, “사이버 공격과 보안 기술”, 홍릉과학출판사.
[82] 최원준, 노병희, 휴승희, 오영철, “랜덤화된 트리워킹 알고리즘에서의 RFID 태그 보안을 위한 백워드 채널 보호 방식”, 한국통신학회논문지 제

30권 5C호, 2005.

[83] 안해순, 부기동, 윤은준, 남인길, “RFID/USN 환경을 위한 개선된 인증 프로토콜”, 전자공학회.

[84] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks", IEEE comp, pp 54-62, 2002.

[85] 김영기, 이화성, 김용호, 이동훈, "무선 센서 네트워크에서의 라우팅 보안 기법 비교 분석", 한국 방송공학회 학술발표대회 논문집, 2008.

[86] 정우진, 홍종욱, 이우주, 박영태, 윤동원, "센서 네트워크의 보안 라우팅 연구 동향", 대한전자공학회 2007년도 하계종합학술대회 논문집II(반도체/컴퓨터/시스템 및 제어) 제30권 제 1호, 2007.

[87] 최병구, 조응준, 홍충선, "무선 센서 네트워크 환경에서 링크 품질에 기반한 라우팅에 대한 효과적인 싱크홀 공격 탐지 기법", 정보과학회논문지, 컴퓨팅의 실제 및 레터 제 14권 제 9호, 2008.

[88] 이규호, 이건희, 김동규, 서정택, 손기욱, “애드 혹(Ad Hoc) 네트워크에서의 위치정보 기반의 웜홀(Wormhole) 탐지 기법”, 한국정보과학회 2006 가을 학술 발표논문집 제 33권 제 2호(D), 2006.

[89] 정석원, "부채널 공격법과 이의 대응법에 대한 연구 동향", 정보보호학회지 제16권 제4호, 2006.

[90] 염홍열, "글로벌 USN 보안 표준화 동향", 2009. http://www.tta.or.kr/data/weekly_view.jsp?news_id=2579,

[91] 한국정보통신기술협회, "USN에서의 센서 노드 간 인증 및 키 분배 프로토콜", 정보통신단체표준(국문표준) TTAK,KO-12.0092, 2008.

[92] 유승화, “RFID/USN 표준화 추진방향”

[93] 김진희, "ETRI, RFID/USN 분야 국제 표준화 이끈다", IT DAILY, 2009.

[94] 최두호, 이해동, 강유성, 최용제, 한동국, 박남제, 월간 정보보호 21c 통권 제 104호, 보안뉴스(www.boannews.com), 2009.

[95] http://www.boannews.com/media/view.asp?idx=11578&kind=1

[96] 나선웅, 김동균, 최영길, 이상정, “무선 센서 노드 데이터를 이용한 홈 네트워크 서비스”, 한국정보과학회 2006 가을 학술발표논문집 제33권 제2호

(D), 2006.
[97] http://blog.naver.com/bskim682/140012624147
[98] 윤종호, 이현우, “전문인을 위한 정보통신일반-파워IT 시리즈7”, 교학사(컴퓨터), P.228, 2007.
[99] http://web.yonsei.ac.kr/AIM/Research.htm
[100] “USN 기반의 교량 모니터링 시스템”, 한국정보사회진흥원 RFID/USN 현장시험 연구과제
[101] “희망한국 실현을 위한 u-City 구축 활성화 기본계획”, 정보통신부, 2006.
[102] http://www.jdlsolutions.com/images/PlantFloor.jpg
[103] http://www.hankyul.in/hw/img/img5.gif
[104] Firetide, "무선 MESH Solution 응용 Service 및 MESH network 구축 고려 사항"
[105] www.netdts.com/govt.html
[106] "MERL", http://www.merl.com/
[107] NIA홈페이지, u-City 정의
[108] 조병선, 정우수, 조향숙, "u-City 사업 전개와 추진동향", 전자통신동향분석 제21권 제 4호, 2006.
[109] 한국정보사회진흥원, "u-City 서비스 모델 확대 발전 방안연구", 2007.
[110] 양단희, 김연수, "u-City의 서비스, 인프라, 기술",한국인터넷 정보학회(제10권 제1호), 2009.
[111] 전자신문,최정훈, "IT유토피아 u시티를 현실로-(2)도시생활 변화 가져올 u-서비스, 2007.
[112] 임춘성, 전남주, 최종화, 송기보, 신현규, "USN 서비스 모델 실태조사 및 개발 방법론 연구", 정보통신연구진흥원, 2005.
[113] 박석지, "미래 RFID/USN 전망", ETRI 주간기술동향, 2006.
[114] 한국 정보 사회진흥원, "유비쿼터스 사회 전망 및 해외사례", IT산업 전망 컨퍼런스 2007 발표 자료
[115] 한국정보사회진흥원, "2006년도 국내외 USN산업 동향 분석 연구", 2006.

[116] 김관중, 김선진, 김내수, 표철식, "USN 서비스 및 시장 동향", 정보과학회지 제 25권 제 12호, 2007.
[117] DARAE, "국내외 최신 USN 비즈니스 모델 및 응용 사례] IT벤처기업연합회.
[118] Ji Luo, Oian Zhang, Dan Wang, “Delay Tolerant Event Collection for Underground Coal Mine using Mobile Sinks",
[119] Guillermo Barrenetxea, Francois Ingelrest, Gunnar Schaefer, Martin Vetterli, "The Hitchhiker’s Guide to Successful Wireless Sensor Network Deployents",
[120] 양단회, 김연수, “u-City의 서비스, 인프라, 기술”, 인터넷정보학회지 제10권 제1호, 2009.
[121] “u-City It 인프라 구축 가이드라인 V1.0", 한국정보사회진흥원, 2008.
[122] “2005년 USN 현장시험 결과 보고서”, 한국전산원, 2006.
[123] “2006년 USN 현장시험 결과 보고서”, 한국정보사회진흥원, 2007.
[124] 안순신, "IPv6기반 센서 위치정보 관리 연구", 한국정보사회진흥원, 2006.
[125] 송주석, “방송통신망 기반 센서네트워크 보안 전담반”, 연세대학교 컴퓨터과학과.
[126] “첨단 지능형 사회의 기능 인프라 USN 현장시험”, 한국정보사회진흥원.
[127] “세브란스병원 RFID/USN을 이용한 혈액 및 항암제관리 시스템”, 2006.
[128] 정부만, “USN 추진 현황 및 계획”, 한국전산원 RFID/USN 팀, 2006.
[129] 김종보, “홈네트워크의 설치 및 관리를 위한 법적 검토”, 경제규제와 법 제1권 제1호, 2008.
[130] “홈네트워크 시범사업 및 융자사업 계획”, 정보통신부 정보보호산업과, 2005.
[131] 이덕규, 김도우, 한종욱, “홈네트워크 보안 기술 및 표준화 동향”, 전자통신동향분석 제23권 제4호, 2008.
[132] “USN 기반 기상/해양 관측 시스템 구축”, KT 미래기술연구소, 2007.
[133] 정정우, “USN을 이용한 도시기반시설 관제 시스템”, KT컨소시엄, 2006년도 한국정보사회진흥원 USN 현장시험 연구과제, 2007.

[134] 엄희석, “미래 구방을 위한 IT융합 핵심기술”, ITC Kaist IT 융합 연구소, 2009.
[135] 고영훈, “현장 구축을 통한 USN의 활용과 전망”, 임베디드 월드, 2008.
[136] 조수형, “국내 홈네트워크서비스 시장동향”, 전자부품연구원, 2005.
[137] “희망한국 실현을 위한 u-City 구축 활성화 기본 계획”, 정보통신부, 2006.
[138] 정의영, “홈 네트워크 시범사업 1차년도 결과”, 한국전산원.
[139] 온더넷 http://www.ionthenet.co.kr," 국내 USN 추진 현황과 향후 계획" 2008년 2월호.
[140] "Design U-World u-IT projects", 한국정보사회진흥원.
[141] 김강묘, 오석호, 김기형, 유승화, “U-GEMS : USN based Underwater Monitoring System", 정보통신 설비 학술대회 논문집, 2008.
[142] “07년도 RFID/USN 사업 추진현황”, 2007.
[143] 2008 국가정보보호백서 제2장 정보보호 기술 개발 분야.
[144] "농산물 품질향상을 위한 USN 기반의 재배환경 모니터링 시스템", 동부정부기술, USN 응용 서비스 모델 발굴을 위한 현장시험 연구과제, 2006.
[145] "주차정보 관리 서비스를 위한 응용 요구사항 프로파일", 한국정보통신기술협회, 2007.
[146] 인프라밸리, "지능형 주차관제시스템", SOA/u-City/RFID/USN/VSE 성공사례구축 Solution Forum, 2006.
[147] "USN기반의 소양강 상류천 수질관리를 위한 정보수집 시스템 구축", 현대정보기술, 유비쿼터스 서비스 모델발굴을 위한 USN 현장시험 연구과제.
[148] 김형석, "u-기술로 대전 3대 하천 생태복원", 대전일보, 2007년 7월 13일 5면기사.
[149] "USN기반의 불국사 문화재 관리 시스템", 삼성 에스원 컨소시엄, 2007.
[150] “부산시,부산 U-방재시스템 전략수립 및 설계용역 추진”, 부산 뉴스 와이어, 2007.
[151] 곽진, 고웅, 이동법, “u-City 서비스 기술 및 국내외 추진현황”, 주간기술동향 통권 1351호, 2008.

[152] “삼성전자 홈네트워크 사업 추진방향”, 삼성 전자 디지털 솔루션 센터, 2005.
[153] http://lgezeni.co.kr/page14.htm
[154] http://www.hyundaitel.co.kr/business/hn_define.asp
[155] 김진형, 황준, "u-City에서의 서비스 보안", 한국 인터넷 정보학회제10권 제1호, P.99~103, 2009.
[156] 고웅, 이동범, 곽진, "u-City 서비스 분류에 따른 적용 사례와 보안 고려사항", 한국정보보호학회, 정보보호학회지 제18권 제2호, P.49~66, 2008.
[157] “첨단센서 기반의 대형 건설현장 실시간 시공관리 기술 개발 기획보고서”, p41.
[158] http://www.zigbeeforum.or.kr/index.html
[159] 김장성, 권미영, 김이형, 곽민혜,한규석,김광조, "감시정찰 센서 네트워크 및 주요 시설물 관리에서의 키 관리 기법 비교", 2007.
[160] "u-IT 기반 지능형 스키장 모니터링 서비스를 위한 응용 요구사항 프로파일", 한국정보통신기술협회, 2007.
[161] "2008년도 u-서비스 지원사업 사업계획서, u-IT 기반 터널 통합관제 시스템", 부산광역시, 2008.
[162] 정재훈, "대학, ‘u-캠퍼스’ 변신 너도나도", 전자신문, 2009.
[163] 안길섭, "서원대, 무선랜 캠퍼스 구축-노텔, 이세정보 통해 서원대에 ‘와이어리스 메시 네트워크’ 솔루션 공급", 디지털 테일리, 2005.
[164] "부산시, 부산 U-방재시스템 전략수립 및 설계용역 추진", 부산 뉴스 와이어, 2007.
[165] 정종인, 김창성, 김의정, 강신천, 이경남, 이정환, "초/중등학교 RFID/USN 구축 방안 연구". 한국교육학술정보원, 2006.
[166] "첨단센서 기반의 대형 건설현장 실시간 시공관리기술 개발 기획보고서", p72.
[167] 엄의석, “미래 국방을 위한 IT융합 핵심기술”, ITC KAIST IT 융합연구소, 2009.
[168] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor

networks" in Proceedings of the 10th ACM conference on Computer and communications security. Washington D.C., USA: ACM Press, pp. 52~61, 2003.

[169] 표철식, "USN 기술과 응용", 한국전자통신연구원, 2005.

[170] 전호인, "u-City 및 Home Network 서비스와 연계한 RFID/USN의 표준화 전망", http://cafe.naver.com/ttapr/338

[171] http://math88.com.ne.kr/crypto/text/chap10/10-1.htm

[172] D. Liu, P.Ning, "Location-Based Pairwise Key Establishments for Static Sensor Networks", SASN '03 First ACM Workshop on the Security of Ad Hoc and Sensor Networks, 2003.

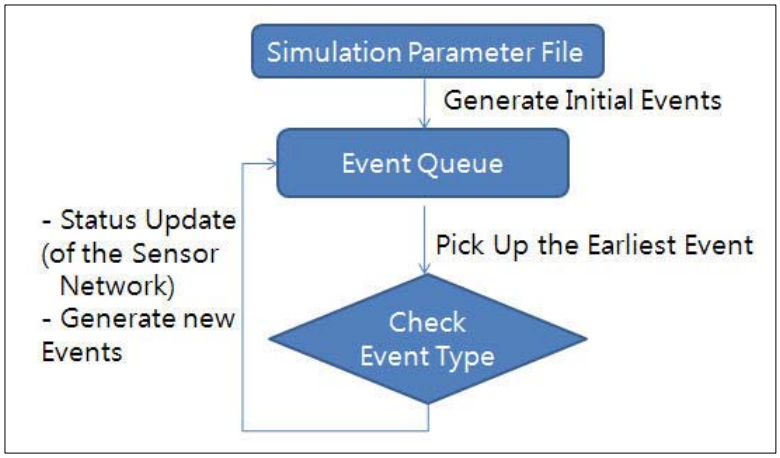
<부록1>

센서 네트워크에서 키 분배에 대한 시뮬레이션 설명

1. 전반적인 시뮬레이션 방법론

가. 개별 이벤트 시뮬레이션

- o 이벤트로 센서 네트워크에서 모델의 모든 활동
- o 이벤트의 결과를 기반으로 시스템(센서 네트워크) 상태 업데이트
- o 필요하다면 새로운 이벤트 발생



(그림 1)시뮬레이션 이벤트

나. 시뮬레이션 파라미터 파일

- o 시뮬레이션 파라미터 열거
  - 노드의 수
  - 무선 범위

- 노드 포지션(랜덤 또는 규칙적)
- 토폴로지
- 키 분배 기법
- 메모리 크기
- etc

다. 초기 이벤트

o 노드 발생
- 주어진 노드의 수를 가져오다.
- 노드 데이터 구조를 형성한다.

o 사전 분배 키 정보
- 키 정보를 분배한다.
- 키 분배 기법에 의존한다.

o 노드 공격
- 공격되어진 주어진 노드의 수를 랜덤하게 선택한다.

라. 이벤트 큐

o 우선 순위 기준으로써 시간을 우선 순위 큐로(Priority Queue with time as the priority criteria)

마. 4가지 이벤트 타입

o 노드 발생
o 사전 분배 키 정보
o 노드 공격
o 메시지
- 노드들 사이의 메시지 교환

```
enum EventType {NODE_GEN = 1, PREDIST, NODECOMP, MSG
};
#typedef Event struct {
  int currenttime // the time that the event occurs
  EventType type;
  char data[MAXSIZE]; // Other Information, depends on event
type
};
```

바. 센서 네트워크의 상태

o 센서 네트워크의 상태를 나타낸다.
o 2가지 중요한 데이터 구조
  - Sink Node (Key Server)
  - Sensor Node

```
#typedef Sensor_Node struct {
  int id;  // ID of the node
  int x, y;  // node's position (x, y)
  char keyring[MAXMEM]; // Key information, depends on key
distribution type
};
```

사. 시뮬레이션의 수행

o Language : C
o OS : LINUX

o TinyOS 환경에서 이동을 위해서만 특정 운용 프로그램에 내재된 C 함수를 사용한다.

2. 시뮬레이션 시나리오

o 센서 네트워크 크기와 다양한 토폴로지를 통한 키 분배 방법의 성능 비교
o 파라미터
  - Size : Small & Large
  - Topology : Star & Mesh
  - Fraction of compromised nodes : 0 to 1
  - 각 노드의 메모리 크기 : Homogeneous, Heterogeneous % Different parameters will be tested.
o Performance metric : 노드 캡쳐 되지 않은 노드들 사이에서 나타난 키들의 수
o 키 분배 기법 후보 : Random 키 기법, Pairwise 키 기법, Polynomial Base 키 기법, Unified key Distribution 기법(현존하는 기법의 성능을 기반으로 통합된 키 분배 프레임워크)

<부록2>

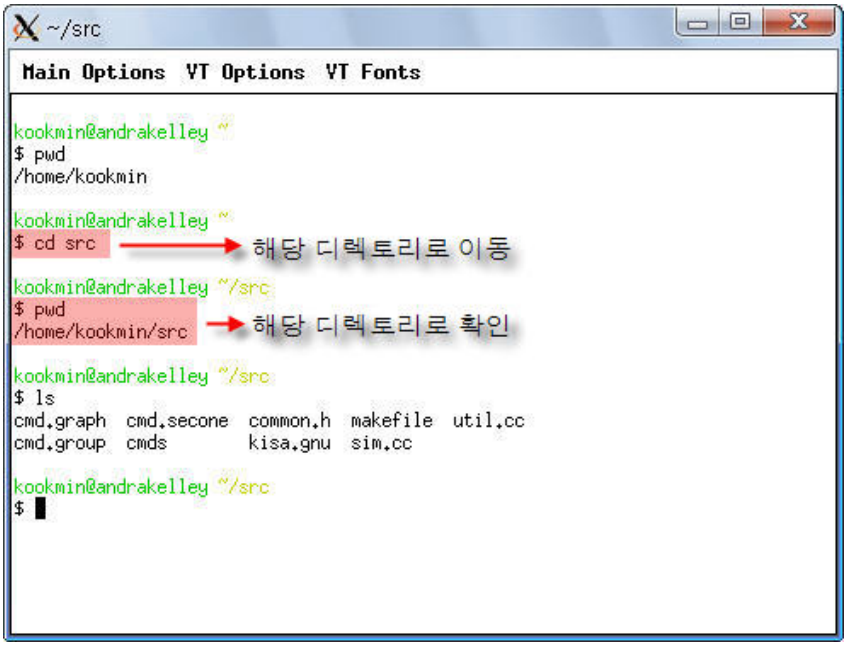
시뮬레이션 방법

1. 모든 파일을 하나의 디렉토리로 복사한다.

2. 리눅스에서 수행한다. cygwin 상에서 수행해도 무방하며 본 보고서는 cygwin에서 수행한 모습이다.

3. cygwin의 xwin Server를 수행하여 파일이 있는 디렉토리로 이동한다. 본 보고서에서 시뮬레이션 수행 시 해당 디렉토리는 /home/kookmin/src 이다.

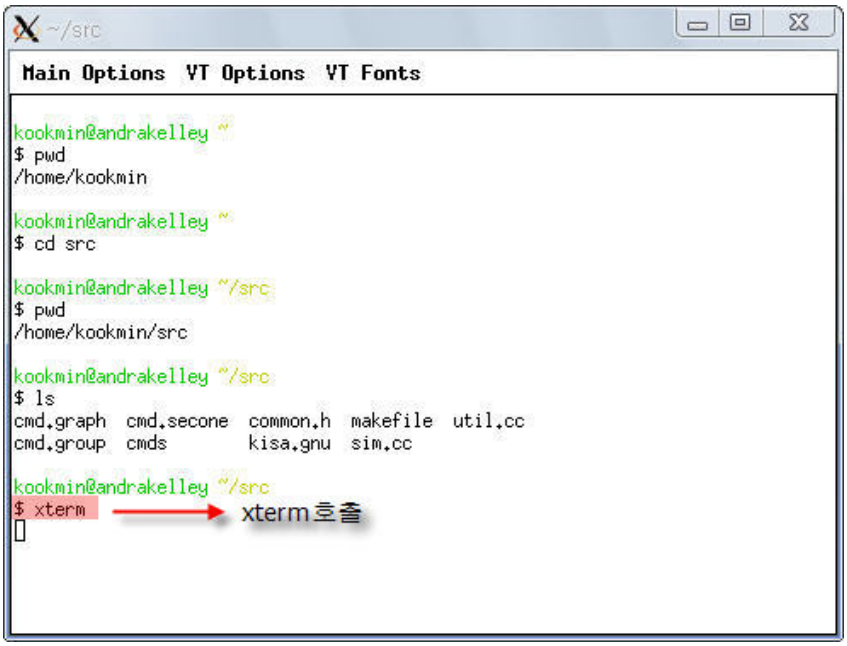
$ cd src



(그림 1) 해당 디렉토리로 이동 및 확인

4. 해당 디렉토리에서 xterm을 호출한다.

$xterm



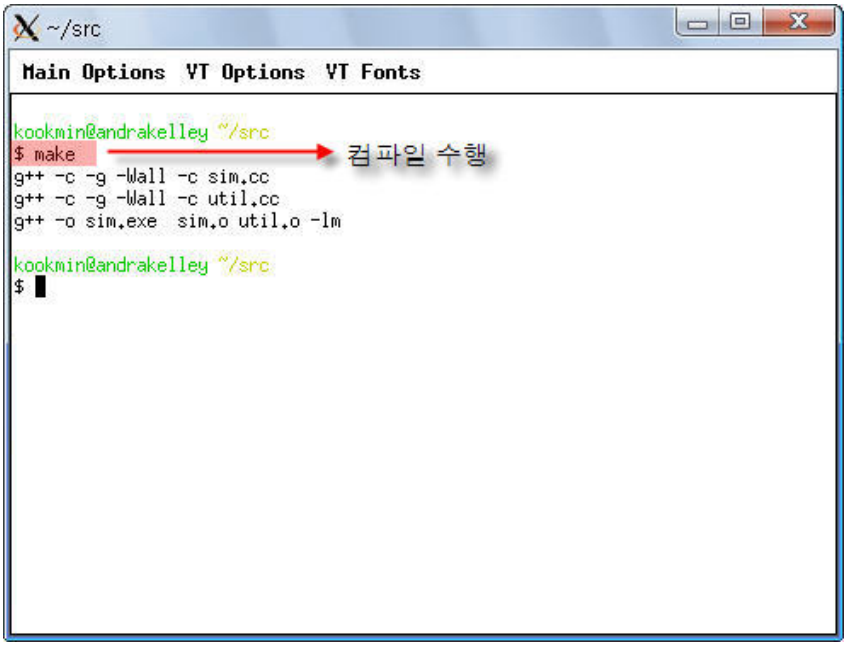
(그림 2) xterm 호출

5. 호출된 xterm에서 소스 코드를 컴파일 시킨다. 해당 폴더에 sim.exe 파일이 생성된다. (그림 3)

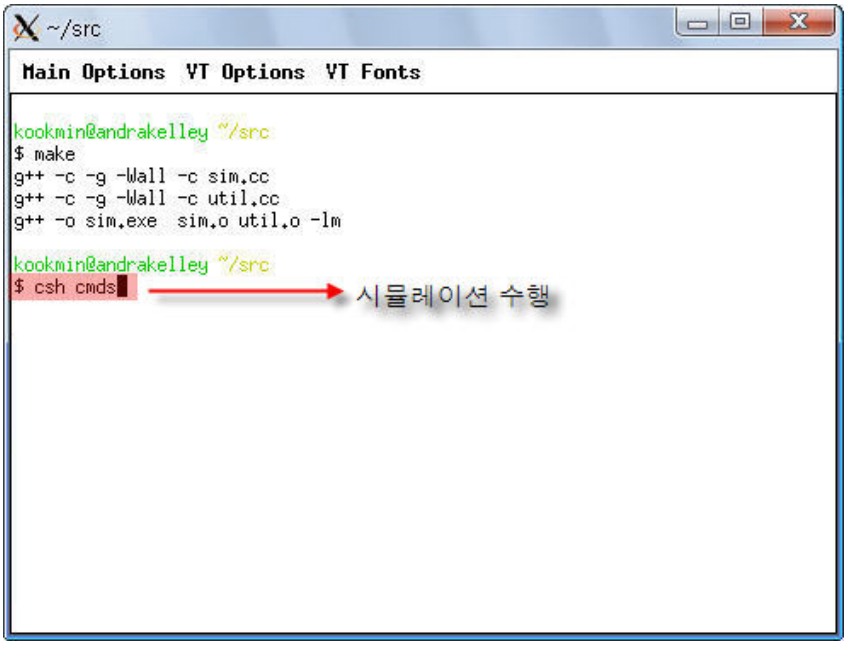
$make

6. 시뮬레이션을 수행한다. 시뮬레이션 수행 결과로 .eps 확장자를 가진 그래프 파일들이 생성된다. (그림 4)

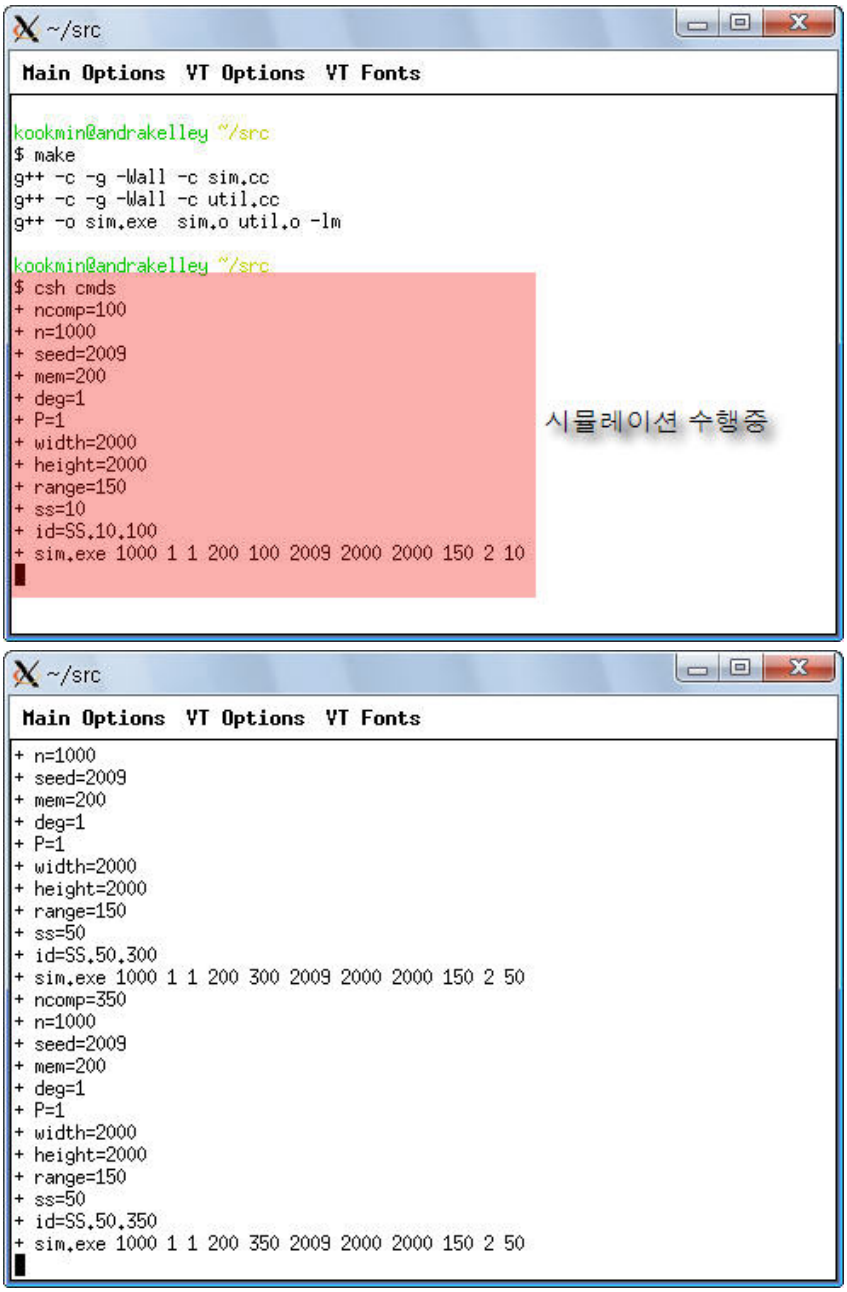
$ csh cmds



(그림 3) 컴파일 수행

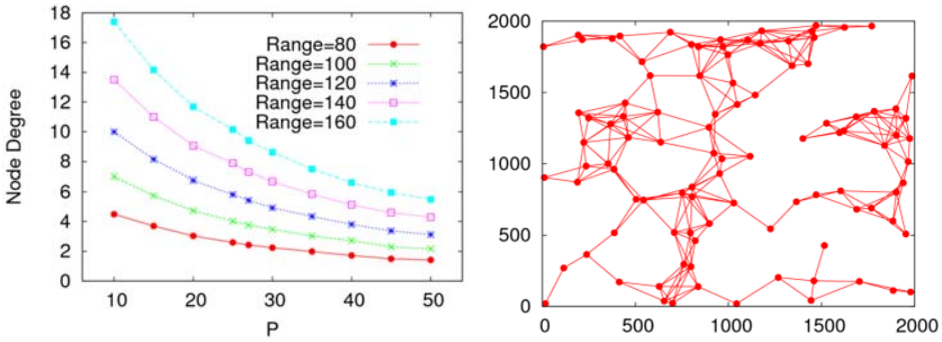


(그림 4) 시뮬레이션 수행



(그림 5) 시뮬레이션 수행 중

7. 시뮬레이션 결과 다음과 같은 그래프가 그려진 파일들이 생성된다.



(그림 6) 시뮬레이션 결과 그래프

※ 그래프에 대한 자세한 내용 및 설명은 제출 논문과 본 보고서를 참조한다.

- 논문 : A Unified Key Distribution Scheme for Ubiquitous Sensor Network
- 제출 : AD HOC & SENSOR WIRELESS NETWORKS(AHSWN)

<부록3>

시뮬레이션 소스코드

1. sim.cc

o main()함수 존재
o 시뮬레이션 시작

```
#include "common.h"



int main(int argc, char *argv[])
{
  int n = atoi(argv[1]); // number of nodes
  int t = atoi(argv[2]); // degree + 1, i.e., the number of coefficient
  int P = atoi(argv[3]); // number of groups
  int m = atoi(argv[4]);// number of memory
  int ncomp = atoi(argv[5]);  // number of compromised nodes
  int seed = atoi(argv[6]);  // seed
  int WIDTH = atoi(argv[7]); // width
  int HEIGHT = atoi(argv[8]);  // height
  double RANGE = atof(argv[9]); // wireless communication range
  int orig = atoi(argv[10]); // original scheme, with one common
  int ss = 0;
  if(argc == 12)
    ss = atoi(argv[11]); // the number of nodes in a square


  int *comppoly;// count of the compromized node with the
Polynomials
```

```
  int i, j;
  int cntcommons = 0; // count of links with common Polynomials
  int cntcomplinks = 0;  // count of the compromised links
  int cntlbncomp = 0; // number of links between non compromised
nodes
  int numofwirelesslinks = 0; // number of wireless links
  int numofsecurewirelesslinks = 0; // number of secure wireless links
  int ***commons; // set of common Polynomials
  int **inrange;  // check whether two nodes are in range


  NODE *nodes = (NODE *) malloc(n * sizeof (NODE));
  memset(nodes, 0, n * sizeof (NODE));

  srand48(seed);

  // ========= Generate Nodes and Key Predistribution
================= //
  // randomly assign coordinates
  assigncoordinates(nodes, n, WIDTH, HEIGHT);

  // randomly assign ni Polynomials to each node
  if(orig == 2)
  {
    P = assignGroupPoly(nodes, n, m, WIDTH, HEIGHT, ss);
    t = m / 5;
  }
  else
  {
    int ni = m/t;  // number of groups that a node belongs to
    assignRandompoly(nodes, n, ni, P);
```

```
  }

  for (i = 0; i < n; i++)
  {
    showvalues(nodes, i);
  }
  // ========= End of Generate Nodes and Key Predistribution
================= //



  // ================= Wireless Link Status ============= //
  // if two nodes are within RANGE, they have a link
  inrange = (int **)malloc(n * sizeof(int*));
  memset(inrange, 0, n * sizeof(int*));

  for (i = 0; i < n; i++)
  {
    inrange[i] = (int *)malloc(n * sizeof(int));
    memset(inrange[i], 0, n * sizeof(int));
  }

  // check each pair of nodes whether they are within RANGE
  numofwirelesslinks = checkinrange(nodes, inrange, n, RANGE);

  // ================= End of Wireless Link Status =============
//



  // ============ Check Secure Links =============== //
```

```
//  printf("hi all\n");

  // find the common Polynomials
  commons = (int ***)malloc(n * sizeof(int **));
  for(i = 0; i < n; i++)
  {
    commons[i] = (int **)malloc(n * sizeof(int *));
    memset(commons[i], 0, n * sizeof(int *));
  }

  for(i = 0; i < n; i++)
  {
    for(j = (i + 1); j < n; j++)
    {
      // find the count of common Polynomials of each pair of links
      int cntcm = 0;
      if((cntcm = commoncount(nodes, i, j, commons)) > 0)
      {
        inrange[i][j] += 2;  // set secure bit
        inrange[j][i] += 2;  // set secure bit

        if(orig == 1) // original schemes, Random and RS
        {
          cntcm = (i + j) % cntcm; // choose one Polynomial
          commons[i][j][0] = commons[i][j][cntcm];
          commons[i][j][1] = -1;  // use only the first Polynomial
        }
      }
    }
  }
```

```
  // count the number of secure wireless links
  cntcommons = 0;
  for(i = 0; i < n; i++)
  {
    for(j = (i + 1); j < n; j++)
    {
      if((inrange[i][j] & 0x3) == 0x3)  // in range and have commons
        numofsecurewirelesslinks++;
      if((inrange[i][j] & 0x2) == 0x2)  // have commons
        cntcommons++;
    }
  }

  printf("count of secure links %d %.3f\n",
    cntcommons, (double)(cntcommons) * 2 / n / (n - 1));

  for(i = 0; i < n; i++)
  {
    for(j = (i + 1); j < n; j++)
    {
      showcommons(commons, i, j, inrange[i][j]);
    }
  }
  // ============ End of Check Secure Links =============== //


  //    ==============  Show the properties of the graph
==============//

  // check connectivity
```

```
  i = checkConnectivity(inrange, n, 1);// wireless connectivity
  j = checkConnectivity(inrange, n, 3);// secure connectivity
  double wdeg = averageDegree(inrange, n, 1);  // wireless degree
  double sdeg = averageDegree(inrange, n, 3); // secure degree

  printf("LCG %5d %.0f %5d %5d %f  %.3f %.3f %f\n",
    P, RANGE, j, i, (double)j/i, sdeg, wdeg, (double)sdeg/wdeg);



  // draw the graph by specifying the edges
  drawgraph(nodes, n, RANGE, inrange, commons);

  // ============== End of Show the properties of the graph
==============//




  // =============== Attack Scenario ============= //

  printf("number of compromized nodes %d\n", ncomp);
  // now select ncomp compromised nodes.
  comppoly = (int *)malloc(P * sizeof(int));
  memset(comppoly, 0, P * sizeof(int));

  // select the compromized nodes
  selectrandomcompnodes(nodes, ncomp, n, comppoly);

  // show the list of compromised Polynomials
  showcompromisedpolylist(comppoly, t, P);
```

```
  // ================ End of Attack Scenario ============= //




  //====================          Show          the          Result
============================ //
  // check whether the secure link is compromised
  cntcomplinks = 0;
  cntlbncomp = 0;
  for(i = 0; i < n; i++)
  {
    if(nodes[i].bcomp == 1)
      continue
    for(j = (i + 1); j < n; j++)
    {
      if(nodes[j].bcomp == 1)
        continue
      if(inrange[i][j] != 3) // not inrange and not secure
        continue
      cntlbncomp++;
      if(checkcompromized(commons, i, j, comppoly, t))
        cntcomplinks++;
    }
  }
  printf("CCL %5d %2d %5d %5d %5d %.0f %5d %5d %f %5d %5d
%.3f\n",
    n, t, P, m, ncomp, RANGE,  // simulation parameters
    cntcomplinks, cntlbncomp, (double)(cntcomplinks) / cntlbncomp,
    numofsecurewirelesslinks, numofwirelesslinks,
```

```
    (double)numofsecurewirelesslinks / numofwirelesslinks );

  //==================== End of Show the Result
========================== //


  return 1;
}
```

2. util.c

o 시뮬레이션에 필요한 함수 정의 및 구현

```
#include "common.h"

int intcomp(const void *x, const void *y)
{
  return *(int*)x - *(int*)y;
}



int findcongrp(int **inrange, int i, int *visited, int n, int stat)
{
  int count = 0;
  int j = 0;

  visited[i] = 1;
  count++;
  for(j = 0; j < n; j++)
```

```
    {
        if(i == j)
            continue
        if(visited[j] == 1)
            continue
        if((inrange[i][j] & stat) == stat)  // all the required bits are there
        {
            count += findcongrp(inrange, j, visited, n, stat);
        }
    }
    return count;
}

    // check connectivity
int checkConnectivity(int **inrange, int n, int stat)
{
    int i = 0;
    int maxsize = 0;
    int size = 0;
    // find out the maximal connected component in original graph
    // find out the maximal connected component in secure graph

    int *visited = (int *)malloc(n * sizeof(int));
    memset(visited, 0, n * sizeof(int));

    for(i = 0; i < n; i++)
    {
        if(visited[i] == 0)
        {
            size = findcongrp(inrange, i, visited, n, stat);
            if(size > maxsize)
```

```
            maxsize = size;
        }
    }

    free( visited);
    return maxsize;
}

double averageDegree(int **inrange, int n, int stat)
{
    int i = 0, j;
    int degree = 0;

    for(i = 0; i < n; i++)
    {
        for(j = 0; j < n; j++)
        {
            if(i == j)  continue
            if((inrange[i][j] & stat) == stat)  // all the required bits are there
                degree++;
        }
    }

    return (double)degree/n;
}
double distance(NODE *nodes, int i, int j)
{
    double dist = 0;
    dist = (nodes[i].x - nodes[j].x) * (nodes[i].x - nodes[j].x);
    dist += (nodes[i].y - nodes[j].y) * (nodes[i].y - nodes[j].y);
    return sqrt(dist);
```

```
}

int checkcompromized(int ***commons, int i, int j, int *comppoly, int t)
{
  int *temp = commons[i][j];
  int k = 0;

  while(temp[k] != -1)
  {
    if(comppoly[temp[k++]] < t)
      return 0;
  }
  return 1;
}

int showcommons(int ***commons, int i, int j, int inran)
{
  int k = 0;
//  printf("commons %4d %4d : ", i, j);
  if (commons[i][j][0] == -1)
  {
//    printf("empty\n");
    return 0;
  }

  k = 0;
  while(commons[i][j][k] != -1)
  {
//    printf("%d ", commons[i][j][k]);
    k++;
  }
```

```
  printf("\nsecure%d  %d\n\n", inran, k);

  return 1;
}



int commoncount(NODE *nodes, int i, int j, int ***cms)
{
  int a, b;
  int cnt = 0;
  int poly[MAXP];

  a = b = 0;
  while((a < nodes[i].ni) && (b < nodes[j].ni))
  {
    if(nodes[i].grp[a] == nodes[j].grp[b])
    {
        poly[cnt++] = nodes[i].grp[a];
        a++; b++;
    }
    else if(nodes[i].grp[a] < nodes[j].grp[b])
      a++;
    else if(nodes[i].grp[a] > nodes[j].grp[b])
      b++;

  }

  cms[i][j] = (int *)malloc((cnt + 1) * sizeof(int));
  memcpy(cms[i][j], poly, cnt * sizeof(int));
  cms[i][j][cnt] = -1;
  cms[j][i] = cms[i][j];
```

```
//  fprintf(stderr, "hi %d %d\n", i, j);
  return cnt;
}


int addpoly(NODE *nodes, int i, int poly)
{
  int j = 0;

  for(j = 0; j < nodes[i].ni; j++)
  {
    if(nodes[i].grp[j] == poly)
    {
    //  fprintf(stderr, "duplicate\n");
      return 0;
    }
  }
  nodes[i].grp[nodes[i].ni++] = poly;

  return 1;
}

int showvalues(NODE *nodes, int i)
{
  int j = 0;

  printf("node %d %.3f %.3f %d\n", i, nodes[i].x, nodes[i].y, nodes[i].ni);
  for(j = 0; j < nodes[i].ni; j++)
  {
    printf("%d ", nodes[i].grp[j]);
```

```
  }
  printf("\n\n");

  return 1;
}

int assigncoordinates(NODE *nodes, int n, int WIDTH, int HEIGHT)
{
  int i = 0;

  // randomly assign coordinates
  for (i = 0; i < n; i++)
  {
    // assign coordinates
    nodes[i].x = drand48() * WIDTH;
    nodes[i].y = drand48() * HEIGHT;
  }

  return 1;
}

int assignRandompoly(NODE *nodes, int n, int ni, int P)
{
  int i;
  // randomly assign ni Polynomials to each node
  for (i = 0; i < n; i++)
  {
    int cnt = 0;
    while (cnt < ni)
    {
      int poly = (int)(drand48() * P);
```

```
        if(addpoly(nodes, i, poly))
        {
          cnt++;
        }
        qsort(nodes[i].grp, nodes[i].ni, sizeof(int), intcomp);
      }
    }

    return 1;
}

// get the number of nodes in a square
int getnumnodesinsq(NODE *nodes, int n, double x, double y, double r)
{
    int i = 0;
    int cnt = 0;

    //printf("start with r %f %f %f\n", r, x, y);
    for(i = 0; i < n; i++)
    {
      if( (nodes[i].x >= x) &&
        (nodes[i].x < (x + r)) &&
        (nodes[i].y >= y) &&
        (nodes[i].y < (y + r)))
        cnt++;
    }

    return cnt;
}

// divide the area into squares
```

```
// each square does contain no more than ss nodes.
int assignGroupPoly(NODE *nodes, int n, int m, int WIDTH, int
HEIGHT, int ss)
{
  double R = WIDTH > HEIGHT ? WIDTH : HEIGHT;
  double L = 0;
  double r = 0;
  int maxnum = 0;
  double x, y;

  printf("Start assignGroupPoly\n");

  // determine the size of the square
  while(L < (R - 1))
  {
    r = (R + L) / 2;
    x = 0;
    maxnum = 0;

    while(x < WIDTH)
    {
      y = 0;
      while(y < HEIGHT)
      {
        // check the number of nodes inside (x,y) and (x+r, y+r)
        int cnt = getnumnodesinsq(nodes, n, x, y, r);

        if(cnt > maxnum)
          maxnum = cnt;
        y += r;
      }
```

```
        x += r;
    }
    printf("one step %f %f %d\n", L, R, maxnum);
    if(maxnum > ss)
        R = r;
    else
        L = r;
}

r = L;// choose the smaller one
printf("Final %f %d\n", r, maxnum);

// randomly assign ni Polynomials to each node
x = -r;
y = -r;

int xcnt = (int)ceil(WIDTH / r) + 2;
int ycnt = (int)ceil(HEIGHT / r) + 2;

int i, j, k;
for(i = 0; i < xcnt; i++)
{
    x = i * r;
    for(j = 0; j < ycnt; j++)
    {
        y = j * r;

        // now find all the nodes in this range
        for(k = 0; k < n; k++)
        {
            if( (nodes[k].x >= x) && (nodes[k].x < (x + r)) &&
```

```
            (nodes[k].y >= y) && (nodes[k].y < (y + r)))
          {
            int di, dj;
            // assign 5 Polynomials
            for(di = -1; di < 2; di++)
            {
              for(dj = -1; dj < 2; dj++)
              {
                if((di * dj) != 0)
                  continue
                int poly = (i + 1 + di) * (xcnt + 2) + (j + 1 + dj);
                printf ("poly %d\n", poly);
                addpoly(nodes, k, poly);
              }
            }
            qsort(nodes[i].grp, nodes[i].ni, sizeof(int), intcomp);
          }
        }
      }
    }

    int P = (xcnt + 2) * (ycnt + 2) - 1;
    printf("maxP %d\n", P);

    return P;
}




int drawgraph(NODE *nodes, int n, double RANGE, int **inrange, int
```

```
***commons)
{
  int i, j;

  for(i = 0; i < n; i++)
  {
    printf("EDGE%d%.0f %f %f\n", n, RANGE, nodes[i].x, nodes[i].y);
    printf("EDGE%d%.0f %f %f\n", n, RANGE, nodes[i].x, nodes[i].y);
    printf("EDGE%d%.0f\n", n, RANGE);
    printf("ESDGE%d%.0f %f %f\n", n, RANGE, nodes[i].x, nodes[i].y);
    printf("ESDGE%d%.0f %f %f\n", n, RANGE, nodes[i].x, nodes[i].y);
    printf("ESDGE%d%.0f\n", n, RANGE);

    for(j = (i + 1); j < n; j++)
    {
      // print the edges
      if((inrange[i][j] & 0x1) != 0)// in range
      {
        printf("EDGE%d%.0f %f %f\n", n, RANGE, nodes[i].x, nodes[i].y);
        printf("EDGE%d%.0f %f %f\n", n, RANGE, nodes[j].x, nodes[j].y);
        printf("EDGE%d%.0f\n", n, RANGE);

        if(commons[i][j][0] != -1)
        {
          printf("ESDGE%d%.0f %f %f\n",
            n, RANGE, nodes[i].x, nodes[i].y);
          printf("ESDGE%d%.0f %f %f\n",
            n, RANGE, nodes[j].x, nodes[j].y);
          printf("ESDGE%d%.0f\n", n, RANGE);
        }
      }
```

```
    }
  }

  return 1;
}


int selectrandomcompnodes(NODE *nodes, int ncomp, int n, int
*comppoly)
{
  int i = 0, j = 0;
  while(i < ncomp)
  {
    int cnode = (int)(drand48() * n);
    if(nodes[cnode].bcomp == 1)
      continue
    nodes[cnode].bcomp = 1;
    i++;

    // increase the count of the compromized Polynomials
    for(j = 0; j < nodes[cnode].ni; j++)
    {
      comppoly[nodes[cnode].grp[j]]++;
    }
  }

  return 1;
}

int showcompromisedpolylist(int *comppoly, int t, int P)
{
```

```
  // compromised lists
  int cntcomppoly = 0;      // count of fully compromised Polynomial
  int i = 0;

  printf("compromized list\n");
  for(i = 0; i < P; i++)
  {
    if(comppoly[i] > 0)
    {
      printf("comppoly %4d %d\n", i, comppoly[i]);
      if(comppoly[i] >= t)
      {
        cntcomppoly++;
        printf("fully comppoly %4d %d\n", i, comppoly[i]);
      }
    }
  }
  printf("cntcomppoly %d\n", cntcomppoly);

  return 1;
}

int checkinrange(NODE *nodes, int **inrange, int n, double RANGE)
{
  // when node i and j are within the RANGE, set to 1
  int i, j;
  int cntinrange = 0;

  for (i = 0; i < n; i++)
  {
    for(j = (i + 1); j < n; j++)
```

```
    {
      if(distance(nodes, i, j) <= RANGE)
      {
        inrange[i][j] = 1;
        inrange[j][i] = 1;
        cntinrange++;
      }
    }
  }

  return cntinrange;
}
```

3. common.h

o 시뮬레이션에 필요한 함수 열거

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <string.h>

#define MAXNUM (1024)
#define MAXP (1024)

typedef struct {
  int ni;
  int grp[MAXNUM];
  double x;
```

```
  double y;
  short bcomp;
} NODE;

int intcomp(const void *x, const void *y);

int findcongrp(int **inrange, int i, int *visited, int n, int stat);
int checkConnectivity(int **inrange, int n, int stat);
double averageDegree(int **inrange, int n, int stat);
double distance(NODE *nodes, int i, int j);
int checkcompromized(int ***commons, int i, int j, int *comppoly, int t);
int showcommons(int ***commons, int i, int j, int inran);
int commoncount(NODE *nodes, int i, int j, int ***cms);
int addpoly(NODE *nodes, int i, int poly);
int showvalues(NODE *nodes, int i);

int assigncoordinates(NODE *nodes, int n, int w, int h);
int assignRandompoly(NODE *nodes, int n, int ni, int P);
int assignGroupPoly(NODE *nodes, int n, int ni, int WIDTH, int
HEIGHT, int ss);

int drawgraph(NODE *nodes, int n, double RANGE, int **inrange, int
***commons);
int selectrandomcompnodes(NODE *nodes, int ncomp, int n, int
*comppoly);
int showcompromisedpolylist(int *comppoly, int t, int P);

int checkinrange(NODE *nodes, int **inrange, int n, double RANGE);
```

USN 환경에서의 키 관리 기술의 적용 모델 개발

2009 년 09 월 인쇄
2009 년 09 월 발행

- 발행인: 김 희 정
- 발행처: 한국인터넷진흥원
  서울시 송파구 중대로 135
  IT벤처타워(서관)
  Tel: (02) 4055-114
- 인쇄처: 정우 제본사
  Tel: (02) 929-4456

<비매품>

1. 본 연구보고서는 정보통신진흥기금으로 수행한 정보통신연구개발사업의 연구결과입니다.
2. 본 연구보고서의 내용을 발표할 때에는 반드시 한국인터넷진흥원의 정보통신연구개발사업의 연구결과임을 밝혀야 합니다.
3. 본 연구보고서의 판권은 한국인터넷진흥원이 소유하고 있으며, 당 진흥원의 허가 없이 무단 전재 및 복사를 금합니다.