u-City에서 센서네트워크에 기반을 둔 자녀 안심서비스의 보안요구사항 분석 및 시스템 제안

김장성*, 유명한*, 김광조*

*카이스트 정보통신공학과

A new system and its security requirements for kid's safety care based on sensor network in u-City

Jangseong Kim*, Myunghan Yoo*, Kwangjo Kim*

*Department of Information and Communications Engineering, KAIST.

요 약

최근 아이들에 대한 흉악범죄가 지속적으로 발생함에 따라 자녀안심서비스가 각광을 받고 있다. 이러한 경향은 u-City가 거주민들의 삶의 질 향상, 기업의 생산성 향상, 도시의 효율적인 관리 제공을 위해 제안된 개념이기에 u-City에서도 동일하게 적용될 것으로 기대된다. 그러나 현재 상용으로 운용 중인 자녀안심서비스는 부정확한 위치정보, 개인의 프라이버시 침해, 서비스 제공자 중심인 점에서 u-City에서 활용되기 어렵다. 본 논문에서는 이러한 문제를 해결하기 위해 센서네트워크에 기반을 둔 자녀안심서비스의 보안요구사항을 분석하였고 이에 맞는 새로운 시스템을 제안하였다.

I. 서론

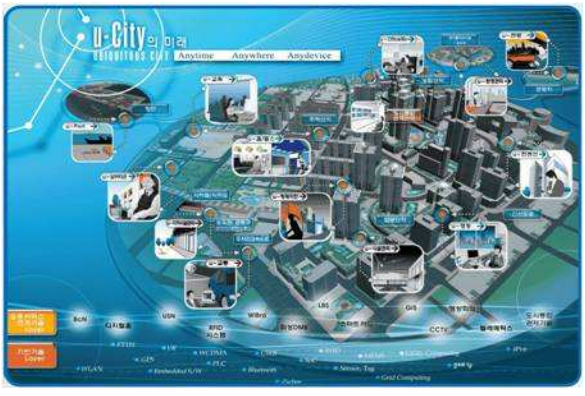

그림 1: u-City가 적용된 미래 도시 [1]

유비쿼터스 기술이 일상생활에 조금씩 들어옴에 따라 우리가 사는 도시도 이러한 유비쿼터스 기술을 적용한 u-City가 각광을 받고 있다. 이는 u-City가 시민에게는 보다 안전하고 풍요로운 생활을, 기업에게는 보다 향상된 기업 경쟁력을, 도시정부에는 효율적인 도시 관리를 제공할 수 있기 때문이다. 그림 1은 u-City가 실생활에 적용될 경우 제공 가능한 다양한 서비스를 보여주고 있으며, 실제로 인천 송도를 비롯해 홍콩, 두바이 등 세계 각국에서 구축 되고 있다 [1].

최근 아이들을 상대로 흉악범죄가 빈번하게 발생함에 따라 대다수의 학부모들은 자신들의 자녀가 안전하게 등·하교하며, 아파트/주택 단지 인근에 위치한 놀이터에서도 안전하기를 희망하고 있다. 현재에는 SKT, KTF, LGT와 같은 통신사 기반으로 자녀 안심서비스가 상용화되어 운용중이며, 가입자는 지속적으로 늘어나고 있다. 더욱이, 서울 강남구청에서는 2009년 5월 현재 유비쿼터스 센서네트워크와 GPS 기술을 활용해 어린이 위치 확인 서비스를 제공하고 있다 [2]. 그러나 이러한 서비스들은 부정확한 위치정보 [3] 혹은 개인의 사생활을 침해하는데 악용될 소지가 있다.

이런 측면에서 봤을 때, 현재의 서비스는 점점 커져가고 있는 시민들의 자녀 안전에 대한 요구사항을 만족시키지 못하는 실정이다. 따라서 u-City에서는 이러한 시민들의 요구를 만족시켜줄 수 있으면서도 앞서 제기된 문제들을

해결해주어야 한다.

본 논문에서는 센서네트워크 기반의 자녀안심서비스의 효용성 및 해당 서비스의 보안요구사항에 대해 다루고자 한다. 이를 위해 2장에서는 현재 서비스되고 있는 자녀안심서비스의 특징 및 문제점에 대해 살펴본 다음, 3장에서는 센서네트워크 기반의 자녀안심서비스의 장점, 시스템 모델 및 보안요구사항을 분석하고자 한다. 4장에서는 제안된 시스템 모델에 대해 분석하며, 5장에서는 간략한 맺음말과 앞으로의 연구방향에 대해 언급한다.

II. 관련연구

2.1 자녀안심서비스

통신사에서 제공하는 자녀 안심서비스는 매 1시간 간격으로 아이의 위치를 부모의 휴대폰으로 알려주는 서비스이며, 사전에 설정한 지역을 벗어날 경우 즉시 부모에게 통보된다. 또한, 그림 2와 같이 부모는 자녀의 위치를 수시로 확인할 수 있다. 그러나 이러한 서비스는 사용자가 소지하고 있는 휴대폰 종류에 따라 위치정보의 정확성이 다르며, 부정확한 위치정보를 전송하는 문제를 야기 한다 [3]. 이는 자녀가 소지한 휴대폰이 수신한 기지국의 위치를 중심으로 상대적인 거리를 파악하는 방법이며, 실제사례를 통해 확인된 오차 반경은 4km정도이다 [4]. 따라서 범죄가 발생했을 때 효과적으로 대처하기 어려우므로 부모가 자녀들의 위치를 보다 정확하게 확인하기 위해서는 위치보정용 하드웨어가 필요하다.

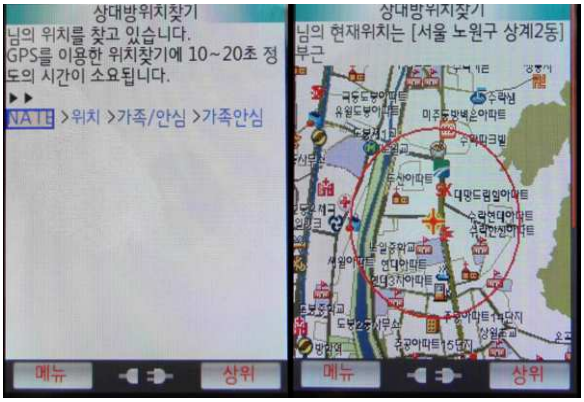

그림 2: S 통신사의 가족/안심서비스 [5]

서울 강남구에서는 그림 3과 같이 유비쿼터스 센서네트워크와 GPS를 기반으로 하여 위치정보를 확인하고 위치관제시스템에 전송해 보호자가 어린이, 치매노인, 지적 장애인의 위치를 실시간으로 PC 혹은 휴대폰을 통해 확인하도록 해주는 서비스 [2]를 제공하고 있다. 그러나 해당 서비스는 인권침해 혹은 프라이버시를 침해하는데 악용될 우려가 있다.

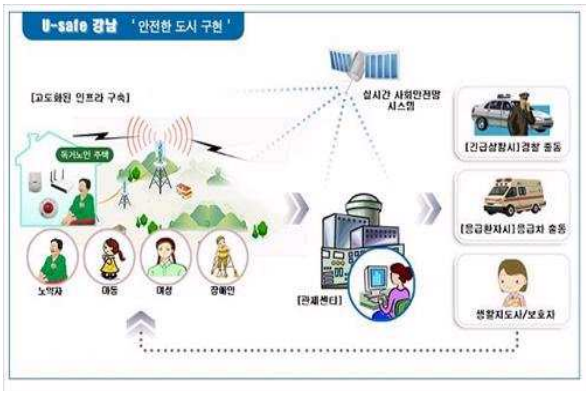

그림 3: U-safe 강남에서 위치 확인 서비스

KT에서는 교육기관의 차별화 및 학부모의 안심을 위해 어린이 안심서비스를 제공하고 있다 [6]. 해당 서비스는 그림 4와 같이 교육기관에 ZigBee 기반의 카드리더기를 설치하면 학부모들은 자녀들의 등·하교 정보를 휴대폰을 통해 전송받을 수 있다. 그러나 해당 서비스는 학교에 등·하교 과정에서 발생하는 범죄에 대해서는 대처하기 어렵다. 이를 해결하기 위해 단말기에 GPS 기능을 추가하고 유비쿼터스 센서네트워크 위치 기술을 활용해 등·하교 과정에서도 자녀들의 위치정보를 전송할 수 있도록 개선할 예정이다.

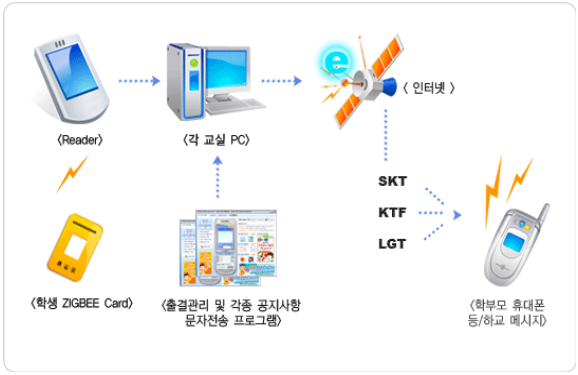

그림 4: KT의 어린이 안심서비스

2006년 K. Takata는 자녀안심서비스와 유사하게 야외활동에서 발생 가능한 다양한 사고로부터 자녀들을 안전하게 하기 위한 대처방안을 알려주는 시스템 [7]을 제안하였다. 제안된 시스템은 그림 5와 같이 자녀가 소지한 단말이 주변 환경으로부터 받은 위치정보를 홈네트워크 서버에 전송하면, 홈네트워크는 자녀의 위치가 위험지역으로 등록되어 있는 경우 해당지역에

서의 안전수칙을 자녀가 소지한 단말에 전송한다. 또한, 부모는 이러한 정보는 GUI로 확인할 수 있다. 그러나 제안된 방법에서는 자녀가 소지한 단말기가 가정의 홈네트워크에 연결될 수 있어야 하지만, 자녀의 위치 정보가 홈네트워크 서버에 직접적으로 전송되기 때문에 개인의 프라이버시를 보호할 수 있다.

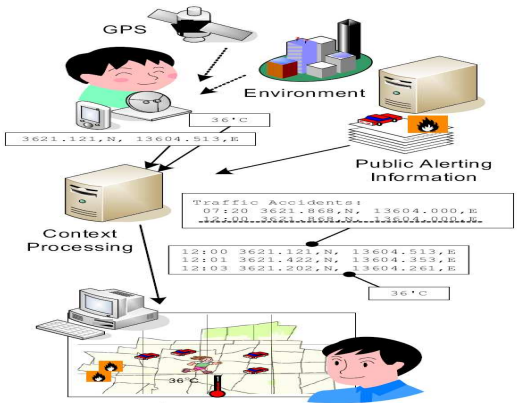

그림 5: K. Takata의 자녀안심서비스 시나리오

2.2 위치측위기술 (Location Determination Technology)

위치측위기술은 위치기반서비스 (Location Based Service)의 필수조건으로 사람 혹은 사물의 위치를 정확하게 파악하는 기술이다. 이에 따라 다양한 방식의 측위기술들이 개발되었으며, 그 정확도와 활용분야별로 측위기술이 활용되고 있다.

현재 활발하게 사용되고 있는 실외 측위기술들은 A-GPS (Network-assisted GPS), GPS (위성측위시스템), DGPS (Differential GPS)가 있다 [8]. 먼저, GPS는 3개 이상의 인공위성을 이용해 위치를 측정하는 방식이다. 위치정확도는 10~30m이며, 단말이 소형이고 설치가 간단하지만, 시내 및 터널 등의 음영지역이 존재한다.

A-GPS는 이동통신 기지국 활용 방식 (e.g., Angle Of Arrival, Time Of Arrival, Time Difference Of Arrival 등)에 GPS 방식을 결합한 방식으로, GPS 방식에 비해 음영지역 및 정확도를 보완할 수 있다. 또한, 인공위성과의 통신에 사용되는 비용을 줄일 수 있다. 현재 상용으로 운용되고 있는 자녀안심서비스는 A-GPS 기반으로 운용된다.

DGPS는 기존의 GPS가 갖는 위성의 위치에 따른 오차를 보정해 정확도를 높이기 위해 지상의 위치를 정확히 알고 있는 기준 수신기를 설치해 해당 수신기를 통해 보정하는 방식이다.

실내위치측위기술은 사용하는 무선통신 기술의 차이에 따라 적외선 기반 측위기술, 초음파 기반 측위기술, RF 기반 측위기술, UWB (Ultra-WideBand) 기반 측위기술로 구분할 수 있다 [9]. 적외선 기반 측위기술은 실내 곳곳에 부착된 적외선 센서가 고유 ID 코드를 가진 적외선 장치를 인식하는 방식이지만, 형광 또는 직접적인 태양광이 비치는 장소에서는 사용하기 어렵다.

초음파 기반 측위기술은 RF와 초음파의 전송 속도차를 이용해 위치를 파악하는 방식으로 매우 정확하게 측위할 수 있으나, 초음파를 송·수신하기 위한 별도의 모듈이 필요하고 설치환경별 전송 속도차가 사전 측정되어야 하는 점에서 어려움이 발생한다.

반면에 RF 기반 측위기술과 UWB 기반 측위기술은 단말이 수신한 신호의 강도를 통해 위치를 파악하는 방식으로 초음파 기반 측위기술에 비해 상대적으로 정확성은 떨어지지만, 저렴한 단말 및 긴 인식거리 측면에서는 효과적이다.

III. u-City에서의 자녀안심서비스

u-City에서의 자녀안심서비스 및 보안요구사항을 다루기 전에 u-City 구성에 대해 살펴보고자 한다.

3.1 u-City의 특성

◇SK그룹이 그리는 u시티의 모습

그림 6: SK그룹이 그리는 u-City 모습 [10]

u-City는 그림 6과 같이 도시 곳곳에 설치된 센서 및 CCTV를 통해 획득된 정보(e.g., 도로상황, 기상정보, 주변 조도, 화재여부 등)를

유·무선 네트워크를 통해 도시종합정보센터에 전송하고 이를 가공해 거주민들에게 다양한 서비스를 제공하는 형태로 구성되어 있다. 따라서 u-City에서 원활한 정보 수집을 위해 센서네트워크는 필수적으로 설치 및 운용되어야 한다.

그러나 센서네트워크는 연산 능력, 저장 공간, 배터리 측면에서 제한된 리소스를 가진 센서 노드들로 구성되기 때문에 일반적인 네트워크에 비해 상대적으로 많은 보안 취약점 (DoS 공격, Sinkhole / Wormhole / Sybil 공격, 탈취된 노드를 통한 키 정보 획득, 메시지 위·변조, 트래픽 분석 등)을 내포하고 있다 [11][12]. 따라서 u-City 환경에서 이러한 보안 취약점들이 우선적으로 해결되어야 한다.

3.2 센서네트워크 기반의 자녀안심서비스의 장점

자녀안심서비스를 센서네트워크 기반으로 제공할 경우 다음과 같은 장점을 얻을 수 있다.

① **비교적 정확한 위치 측정**: GPS 수신 혹은 초음파 송·수신과 같은 별도의 위치측정용 장비 없이도 오차범위가 수 cm에서 수 m이내의 비교적 정확한 위치를 측정할 수 있다.

② **저렴한 비용 및 다양한 암호연산 지원**: 센서노드는 PDA / 휴대폰 / 무선 AP 에 비해 저렴하면서도 충분한 연산능력을 가지고 있다. 즉, RFID (Radio-Frequency IDentification) tag에서는 수행하기 어려운 다양한 암호연산 (대칭키/공개키 암호화 등)을 지원할 수 있어 RFID 기반의 시스템에 비해 다양한 보안요구사항을 만족시킬 수 있다.

③ **기존 인프라 재활용**: u-City에서는 도시 주변 곳곳에 센서네트워크가 온도, 습도, 도로 노면 상태, 조명 상태, 화재 여부 등을 목적으로 운용되고 있기에 별도의 인프라 구축 비용이 발생하지 않는다.

3.4 u-City에서 센서네트워크 기반의 자녀안심서비스 보안요구사항

① **개인의 프라이버시 침해**: 상용으로 운용중인 자녀안심서비스는 개인이 서비스 가입과 동시에 서비스 해지 할 때까지 지속적인 위치 추적이 가능한 점과 고정된 사용자 ID로 인해 익명성이 보장되지 않는 점으로 인해 발생한다.

② **센서네트워크 자체의 보안취약점**: 위치측위를 위해 센서네트워크를 활용하기에 발생 가능한 센서네트워크 자체의 보안취약점 (DoS 공격, Sinkhole / Wormhole / Sybil 공격, 탈취된 노드를 통한 키 정보 획득, 메시지 위·변조, 트래픽 분석 등)이 선결되어야 한다.

③ **센서 노드의 이동성 지원**: 센서네트워크 보안에 관련된 대다수의 연구는 센서 노드의 이동성을 고려하지 않기 때문에 이에 대한 연구가 필요하다. 예를 들어, 센서 노드의 인증 메시지가 공격자가 전송하는 메시지로 오인될 수 있으며, 재인증 과정에 인해 추가적인 배터리 소모가 발생한다.

④ **확장성**: 다수의 사용자 인증 및 적절한 접근 제어가 필요하기 때문이다.

⑤ **인증 키 합의 / 기밀성 / 무결성**: 사용자와 센서네트워크간의 인증 키 합의 / 통신 채널의 기밀성 / 메시지 무결성이 제공되어야한다.

3.5 제안된 센서네트워크 기반의 자녀안심서비스 시스템

본 논문에서 제안하는 센서네트워크 기반의 자녀안심서비스 시스템은 그림 7과 같다. 여기서 sink 노드는 특정 지역에서 센싱된 정보를 모아서 베이스 스테이션에 전송하는 역할을 담당하며, 외부 전력이 제공될 수 있다.

① **서비스 가입단계:** 자녀안심서비스를 제공받기 위해서 부모들은 자녀안심서비스에 가입한다. 여기서 자녀안심서비스에 가입을 하기 위해서는 기존의 자녀안심서비스와 동일하게 자녀와 부모간의 상호동의가 필요하며, 일련의 과정은 오프라인에서 이루어진다.

② **서비스 등록단계:** 서비스 제공자는 베이스 스테이션에 자신의 가입자 정보를 암호화하여 등록한다. 베이스 스테이션은 등록된 정보를 이용해 추후 서비스 가입자들이 특정 대상에 대한 위치측위를 요청할 때 해당 사용자가 요청한 서비스의 가입자 유무 확인에 판별에 사용한다.

③ **서비스 운용단계:** 부모는 자녀가 외출할 때마다 사용할 센서 노드를 베이스 스테이션에 등록한다. 자녀는 주변 센서 노드에게 소지한 센서 노드를 인증한 다음 자신의 위치를 측정하고 이를 베이스 스테이션에 전송하면, 베이스 스테이션은 해당 정보를 가정

의 홈네트워크로 전송한다. 전송된 정보는 홈네트워크와 센서 노드와 사전에 공유한 키를 통해 암호화해서 전송한다. 게다가 센서 노드를 등록할 때 익명성이 보장하면, 베이스 스테이션은 자녀가 소지한 센서 노드가 속한 sink의 위치를 통해 대략적인 위치만 파악할 수 있다.

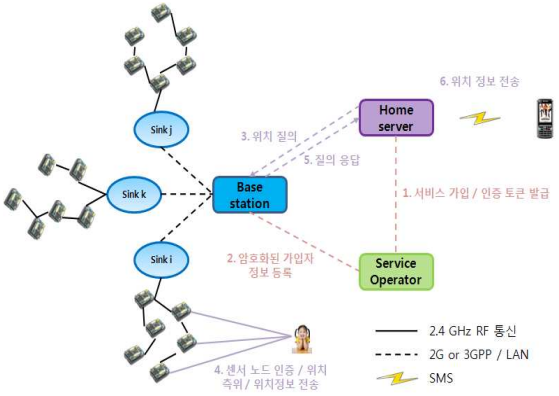

그림 7: 센서네트워크 기반의 서비스

IV. 제안된 서비스 시스템 분석

본 논문에서 제안하는 센서네트워크 기반의 자녀안심서비스 시스템은 다음과 같은 특징을 가진다.

첫째, u-City에서 센서네트워크는 공공시설이므로 현재의 자녀안심서비스 구조와는 달리 위치정보를 측정을 위해 사용되는 네트워크가 서비스 제공자에 속한다고 볼 수 없다. 더욱이, 기존의 서비스 모델에서는 서비스 제공자가 개인별 안심지역, 보호자 연락처, 측정된 위치정보 등을 저장하고 있어 개인의 프라이버시 침해 우려가 발생한다. 하지만 제안된 모델에서는 이러한 정보는 개인의 홈네트워크 서버에 저장되기 때문에 프라이버시 침해 우려를 줄일 수 있으며, 서비스 제공자 측면에서도 잘못된 운영으로 인한 민·형사상 고소로 발생할 수 있는 경제적 손실을 줄일 수 있다. 더욱이, 개인이 원할 때에만 서비스 위치 추적을 할 수 있으며, 자신의 ID 정보를 숨기기 위해 익명성 기법이 적용가능하다.

둘째, 베이스 스테이션 기반의 키 설정 기법[13]을 통해 센서네트워크 자체의 보안취약점을 해결할 수 있다. 베이스 스테이션 기반의 키 설정 기법은 랜덤 사전키 분배 혹은 마스터 키 기반의 방식에 비해 노드 탈취에 내성을 가지며, 센서 노드 주변에 대한 사전 정보 없이도 노드 인증이 가능하기 때문에 센서 노드의 이동성 지원이 용이하다. 게다가 동일 Sink 내에서 이동할 경우 인접 노드들로부터 재인증을 필요하지 않기 때문에 노드 이동성을 어느 정도 지원해 줄 수 있다.

셋째, 베이스 스테이션으로부터의 정보누출의 줄이기 위해 베이스 스테이션은 위치 질의를 요청하는 사용자가 서비스 제공자의 서비스 가입자 유무를 파악하며, 가입자인 경우에 한해 질의 대상 센서로부터 받은 정보를 개인의 홈네트워크 서버에 전송하는 것으로 기능을 제한하였다. 이때 전송되는 정보는 홈네트워크와 센서 노드가 공유된 키를 통해 암호화되어 있어 베이스 스테이션은 해당 정보를 획득할 수 없다.

넷째, 자녀는 소지한 센서 노드를 통해 위치정보를 부모에게 위치정보를 알려주는 방식이기 때문에 본인이 원할 경우 일시적으로 위치정보 전송을 제한할 수 있기 때문에 개인의 사생활 보호가 가능하다. 따라서 제안된 시스템은 u-강남서비스와 같이 다양한 목적으로 운용될 수 있다.

V.결론

본 논문에서는 u-City 환경에서 센서네트워크 기반의 자녀안심서비스의 장점 및 보안요구사항을 살펴보았고, 이를 바탕으로 새로운 서비스 모델을 제안하였다. 그 결과 개인의 프라이버시 침해에 대한 우려를 줄일 수 있으며, 센서네트워크 자체의 보안취약점을 해소할 수 있다.

하지만, 서비스 시스템에 대해 개괄적인 기능 및 특징만 기술하였기 때문에 보다 세부적인 프로토콜을 설계하고자 한다. 또한, 센서 노드의 이동성을 반영한 효과적인 재인증 과정이 추가적으로 연구되어야 한다. 이를 통해 배터리 소모를 줄여 센서네트워크의 운영시간을 늘릴 수 있기 때문이다. 더욱이,

[참고문헌]

[1] u-City 개요, www.ucitycenter.org

[2] u-Safe 강남 시스템, http://usafe.gangnam.go.kr/u-safe_01.html

[3] 조선일보, 통신사의 엉터리 자녀안심서비스, http://www.chosun.com/site/data/html_dir/2008/03/31/2008033101613.html

[4] S사의 자녀안심서비스 믿을수 없다, http://bbs3.agora.media.daum.net/gaia/do/st

ory/read?bbsId=S103&articleId=37888

[5] 가족, 자녀, 연인이 어디에 있는지 궁금하다면? 네이트 가족/안심 서비스, http://pustith.tistory.com/455

[6] KT, 어린이 안심 서비스, http://www.iamhere.co.kr/

[7] K. Takata, J. Ma and B. O. Apduhan, A Dangerous Location Aware System for Assisting Kids Safety Care, in 20th International Conference on Advanced Information Networking and Applications, Vol. 1., April 18-20, 2006,pp. 657-662.

[8] 이성호, 민경욱, 김재철, 김주완, 박종현, 위치기반서비스 기술 동향, 전자통신동향분석, 20권, 3호, 2005년 6월, pp. 33-42.

[9] 조영수, 조성윤, 김병두, 이성호, 김재철, 최완식, 실내외 연속측위 기술 동향, 전자통신동향분석, 22권, 3호, 2007년 6월, pp. 20-28.

[10] 아이뉴스, u-City 우리가 만든다 ③, http://itnews.inews24.com/php/news_view.php?g_serial=371623&g_menu=020200

[11] Y. Law and P. Havinga, How to Secure a Wireless Sensor Network, in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '05), IEEE Computer Society Press, 2005, pp. 89-95.

[12] D. R. Raymond and S. F. Midkiff, Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses, in Pervasive Computing, IEEE, Vol. 7, Issue 1, Jan. - Mar. 2008, pp. 74-81.

[13] J. Kim, K. Han, N. Lee and K. Kim, A Lightweight Key Establishment for Critical Condition Monitoring Applications, submitted to ETRI journal.