개방형 무선 통신망 구조를 위한 복합 보안 프레임워크 설계

김정태*

Design of Integrated Security Framework for Open Wireless Networking Architecture

Jung Tae Kim*

이 논문은 한국연구재단(과제번호 : 2012-0007896)의 연구비를 지원받아 수행된 연구임

요 약

다음은 요약문입니다. 여러 종류의 무선 통신망들에 대한 통합화된 서비스에 대한 수요가 요구되고 있다. 이러한 요구는 기존의 유선망과 무선 통신망의 통합 배치를 통하여 가능하게 되었다. 각각의 무선 통신망들은 기존 망들에 비해 고유의 특징을 가지고 있다. 개방형 무선 통신 환경 하에서의 주요한 문제 중의 하나가 보안성에 관련된 문제이다. 개방형 환경 하에서 통합된 환경의 보안성을 실현하기 위해서는 현실에서 실제적으로 적용 가능한 통합 보안 구조를 개발하여야 한다. 따라서 본 논문에서는 이러한 요구조건을 만족하기 위해서 고려해야 하는 사항들을 분석하였다.

ABSTRACT

The increasing demand of users for various wireless communication services has lead to the development with uniting co-existence of different and wireless networks. Each one of the these wireless networks has its own unique characteristics, as compared to other networks. An integrated security mechanism is one of the key issue in the open wireless network. To realize overall security mechanism in open wireless architecture, we should provide practical workable framework for the realization of the integrated security challenges. In this paper, we analysed integrated security platform and considerations based on the security concept.

키워드

보안 프레임 구조, 무선 통신망, RFID, 통합 보안 기능

Key word

Security Frame Architecture, Wireless Networking, RFID, Integrated Security Mechanism

* 종신회원 : 목원대학교(교신저자, jtkim3050@mokwon.ac.kr)

접수일자 : 2013. 05. 01

심사완료일자 : 2013. 05. 24

I. 서 론

현재 정보통신 기술의 발전으로 인하여 많은 통신 환경이 변화되고 있다. 기존의 정보통신망들은 유선망과 무선망의 분할로 이루어지고 개별 통신망으로 구성되어 발전하였다. 그러나 근래에는 유선망과 무선망 등이 통합되는 단계로 융합되면서 기존의 유선망과 무선망의 구별이 없어지고 있는게 현실이다. 다양한 종류의 특성을 가진 무선 통신망을 위한 사용자들의 요구로 인하여 각각의 통신망들은 각각의 특징에 맞게 발전되고 있다. 사용자의 관점에서 보면 기존의 통신망을 통합하여 사용자 중심의 무선통신 기반의 새로운 특징을 가진 통신망 구조로 발전되고 있다. 사용자의 요구에 따라 무선 및 이동 통신의 특징을 실현하기 위하여 개방형 기반의 무선망 구조를 이용한 형태로 발전되고 있다. 이렇게 구성된 여러 종류의 무선 통신망을 하나의 형태의 개방형 무선망으로 구성하기 위해서는 해결해야 할 문제점들이 많이 있다. 특히 무선 통신망을 기반으로 하기 때문에 이동성에 따른 각각의 시스템을 관리하기 위한 관리 기법, 서비스의 품질, 무선망에서의 고유 문제인 취약성 문제, 서로 다른 시스템의 상호 간의 보안성 연결 문제 등이 아주 중요한 요소로 잡고 있다 [1]. 따라서 본 논문에서는 이러한 개방형 기반의 통합 무선 환경 망에서 요구되는 통신망에서의 특징, 보안성 문제 등에 대하여 살펴본다.

본 논문의 구성은 1장에서는 서론에 대해서 알아보고 2장에서는 관련연구에 대해서 살펴보고, 3장에서는 시스템 보안을 위한 요구사항에 대해서 살펴보고 4장에서는 이중기간의 시스템에서의 보안사항에 대해서 기술하고 마지막 5장에서는 결론을 맺는다.

II. 관련 연구

일반적으로 개방형 무선 통신망의 구조는 기존의 셀룰라망, WLAN, 에드 혹망, 센서 네트워크 망 등으로 구성되어 개별적으로 운영되고 있다. 일반적인 셀룰라망은 기지국을 중심으로 하여 단말기까지 단일 홉 방식의 프로토콜을 사용한 구조의 네트워크이다. 이에 반해 WLAN은 무선 사용자들을 액세스포인트를 사용하는 단일 홉 기반의 네트워크이다. 이러한 무선랜은 유선이

필요 없고 단말기의 재배치가 쉽고 이동 중에도 통신이 가능할 뿐만 아니라, 빠른 시간 안에 네트워크의 구축이 용이하다는 장점을 가지고 있다. 그러나 무선망을 매개체로 사용하여 개방성에 따른 해킹 및 접근이 용이하기 때문에 전자상거래, 전자 메일, 데이터 전송과 같이 데이터 보안의 중요도가 높은 응용 시스템에서 보안성의 요구가 더욱 증가하고 있다. 일반적으로 에드혹 네트워크 구조는 공개된 통신 환경 하에서 주로 사용되며, 네트워크 관리 차원에선 더욱더 복잡한 환경을 제공 한다. 또한 센서 네트워크는 다중 홉 구조의 통신망을 이루고 있으며, 특정한 기능을 위한 폐쇄적인 구조를 가지고 있다. 즉 다시 말하면 하나의 네트워크 망이 형성되면 새로운 센서 노드는 망에 연결될 수 없는 구조로 되어 있다. 최근에는 RFID 시스템을 이용한 자동 인식 시스템 혹은 특정 정보를 인식 교환하고자 하는 개념으로 확장되고 있으나, 무선 통신망의 한계성으로 나타나는 보안상의 취약성을 보여주고 있다.

최근까지 비약적인 기술의 발전으로 인하여 정보기술에 기반한 디지털기술의 융복합화, 개인화로 인하여 유무선 통신 기술을 통합한 유비쿼터스 환경으로 발전되고 있다. 특히 이러한 기술의 발전으로 인하여 인간의 건강을 위한 병원에서의 환자 관찰을 위한 시스템의 발전을 가져오고 있다. 특히 실시간 모니터링을 위해 무선 통신 채널을 통하여 환자와 의사간의 의료 진단을 위한 정보를 가능하게 한다. 특히 센서 네트워크에서의 표준 보안 메카니즘의 성능을 분석한 논문들이 다수 발표되고 있다[2]. Ming Li는 그의 논문에서 헬스케어 시스템에서의 무선센서 네트워크에서의 무결성 문제를 체계적으로 분석 제시하였다 [3]. 또한 Jelena는 IEEE 80.215.4 환경하에서 ECC 알고리즘을 사용하여 무선 센서네트워크 환경하에서 헬스시스템에서의 보안 시스템을 설계하였다 [4]. 따라서 본 논문에서는 이러한 무선 이동 통신망에서의 설계 시 요구되는 보안사항에 대해서 분석하였다.

III. 시스템 보안을 위한 요구사항

본 절에서는 이러한 개별적인 네트워크에 적용하기 위한 표준 보안 알고리즘을 알아보기 전에 무선 통신망에서 사용되는 보안 메카니즘에 대한 기초적인 개념을

알아본다. 무선 통신망의 경우 유선망에 비해 보안적인 위협을 훨씬 더 많이 받는다.

3.1. 보안 요구 사항

일반적으로 요구되는 사항은 다음과 같은 요구 사항을 충족하여야 한다[5].

1) 기밀성(Confidentiality)

하나의 시스템과 각 노드 사이의 모든 통신이 공격자에게 도청되더라도 어떠한 의미 있는 정보는 노출되지 않아야 한다. 즉 공격자는 도청을 하더라도 어떠한 정보를 얻을 수 없어야 한다. 일반적으로 이러한 기밀성을 위하여 기존의 수학에 기초한 암호학적인 방법이 요구되고 있으나 단말기 혹은 노드에서의 적은 용량의 메모리, 연산 능력, 면적 등의 제한적인 리소스로 문제로 인하여 기존의 방법으로는 해결되지 않고 있어 다양한 새로운 기법이 요구되어 지고 있다.

2) 익명성(Anonymity)

공격자가 송신자와 단말기 간의 통신을 통해서 단말기의 위치를 추적 혹은 감시할 수 없어야 하는 성질을 말한다. 이러한 익명성을 보장하기 위하여 구별 불가능성(Indistinguishability) 과 전방향 안전성(Forward Secrecy) 을 만족해야 한다. 구별 불가능성은 단말기에서 전송되는 정보를 통해서 어떠한 태그로 부터의 정보인지를 구별할 수 없어야 한다. 또한 전방향 안전성은 단말기의 현재 데이터가 노출되더라도 이전의 데이터가 추적되지 않아야 한다.

3) 상호 인증(Mutual Authentication)

상호 인증은 송신단과 수신 단말기에서 서로 정당한 객체임을 확인하는 절차 과정을 말한다. 어느 한 방향이라도 인증과정을 통과하지 못하면 공격자는 대상자를 통한 공격 등을 통하여 중간에서 획득한 데이터를 통하여 위조 및 변조가 가능하다.

4) 가용성(Availability)

송신단의 시스템이 수신단 까지 통신을 하는 동안 악의적인 코드를 통한 시스템의 사용을 제한 받는 경우를 말한다. 이중 가장 흔한 공격 방법이 서비스 부정 공격이다.

5) 무결성(Integrity)

네트워크를 통하여 송신자가 송신한 데이터가 수신자가 수신하기 전인 중간 과정에서 데이터의 변조가 없이 전달되어야 한다.

일반적인 보안 기술은 보안 알고리즘 및 프로토콜을 실현하기 위해서 요구되는 기술적인 내용을 수학적인 요소로 분석하여 암호학적으로 검증을 하여야 한다. 다음에서 기술하는 사항은 그 대표적인 요구사항이다. 일반적으로 암호학적인 메카니즘을 이용하여 암호 및 복호화 과정을 이루는 두 개의 과정으로 이루어지며 키를 통한 암호화 과정으로 이루어진다. 대칭키 암호화 시스템의 경우, 암호화 및 복호화 과정에서 동일한 키를 사용하며, 공개키 암호 시스템의 경우, 암호화 과정에서 서로 다른 키를 사용한다. 특히 암호화 키를 통하여 복호화 키를 유추할 수 없는 단방향의 해쉬 메카니즘을 사용한다. 이러한 해쉬 알고리즘은 디지털 서명, 난수 발생, 데이터의 무결성을 위해 사용된다.

3.2. 제안되는 이중기기간의 보안 요구 사항

다음의 (그림 1)은 이중기기간의 무선 이동통신망을 통합한 망 구성도의 예이다. 따라서 각각의 개별 통신망에 대한 보안 요구 사항 및 특징에 대해서 분석하였다[6].

그림 1. 유무선 통합 환경 하에서의 시스템 구성도
Fig. 1 Topology of System under Unified with Wire and Wireless Surroundings

3.2.1. 셀룰라 네트워크의 보안

셀룰라망에서 사용되는 대표적인 예로서 3G UMTS를 들 수 있는데, 각각의 서비스 영역은 무선 접근 영역과 기지국 사이에서의 서비스 보안을 위한 보안 메커니즘을 필요로 하고, 사용자의 보안을 위해서는 AAA (Authentication, Accounting, Authorization)에 의해서 생성되는 인증기술을 사용한다. 이때 사용되는 인증 알고리즘은 단일 라운드 교환 방식을 이용한 핸드셰이킹 방식을 사용한다.

3.2.2. 무선랜 보안

무선랜 보안을 위해서는 인증과 비밀성을 위한 영역으로 나누어진다. 일반적으로 IEEE802.11 표준안은 WEP(Wired Equivalent Privacy)를 통하여 비밀성을 제공한다. 그러나 이러한 방식은 짧은 키와 초기치 값의 충돌로 인하여 보안성에 취약한 면을 가진다. 현재는 IEEE에서 802.11i 프로토콜을 무선랜 보안의 표준으로 제정하고 있으나 그 취약성으로 인하여 지속적인 향상된 알고리즘을 제안하고 있다. 그러나 이 프로토콜은 인증과 키 관리에 국한되어 설명이 되어있어서 다른 공격에는 취약한 상태이다.

3.2.3. 에드홉 네트워크망의 보안

에드홉망은 기존의 유선 및 무선망과 같이 고정된 하부 구조를 필요로 하지 않는 무선 단말기로만 구성된 네트워크이다. 이러한 망구조에서의 보안적인 메커니즘은 에드홉 망에서의 프로토콜의 라우팅 동작을 위한 보안을 제공해야 하며, 특히 키 분배와 안전한 라우팅 프로토콜의 설계가 주된 문제가 된다. 특히 공개키 기반의 알고리즘으로 AODV(Adhoc On-demand Distance Vector) 프로토콜을 사용하며, 개인 키 기반의 대표적인 프로토콜은 SRP(Secure Routing Protocol)이다.

3.2.4. 센서 네트워크 보안

센서 네트워크에서는 센서 노드들이 서비스 영역에 배치된 후 자동적으로 Ad-hoc 네트워크를 구성하는 구조로 이루어진다. 기존의 무선 Ad-hoc 네트워크는 많은 프로토콜과 알고리즘이 연구되고 있지만, 이를 센서 네트워크에 그대로 적용하기에는 많은 문제점을 가지고 있다. 특히 무선, 이동성 및 분산화의 특성을 갖는 센서 네트워크는 센서의 경량화로 인하여 에너지 저장 용량,

컴퓨팅 연산 능력 및 통신 능력 면에서 제한적인 요소를 가지고 있다. 따라서 이러한 문제점 때문에, 기존의 네트워크 환경에서 제공되었던 보안 기술들을 그대로 센서 네트워크에 적용하기에는 많은 문제점이 있음을 예상할 수 있다. 특히 무선 통신 환경 하에서의 키 설정, 통신 기밀성, 중요 정보에 대한 프라이버시, DoS(Denial of Service)에 대한 견고성, 보안 라우팅, 물리적인 공격에 대한 대응, 보안 그룹 관리 및 침입탐지 등의 각각의 요구 조건에 대한 보안성을 만족하여야 한다.

3.2.5. RFID 보안

RFID(Radio Frequency Identification)는 물체의 인식을 위한 매개체로 사용함으로 인해 프로토콜의 취약성을 나타낸다. 프로토콜의 보안성을 강화하기 위하여 기존의 일반적인 연산적인 방법으로서 사용하기에는 태그에서의 적은 용량으로 인하여 기존의 방법이 사용되기 어렵다. 또한 태그에서의 정보를 유출하기 위한 외부의 여러 가지의 공격에 대한 방법을 고려하여야 한다. 이러한 보안적인 취약점 및 위협으로부터 방어하기 위한 기술적 발전이 진전되고 있으나, 암호학적인 측면에서는 저용량, 작은 메모리 영역 및 제한적인 자원으로 인하여 완전히 보안성을 구현하지 못하고 있다. 현재는 저가의 RFID를 위한 보안 기법을 내장한 설계가 많이 연구되고 있으나, 기존의 방법인 단방향 해쉬 함수를 사용한 기법들이 사용되었는데, 이는 저가의 태그 구현에 적합하지 않다. 이러한 연구와는 상반된 개념으로 태그에 해쉬 함수를 지원하는 구조로 설계할 경우, 태그의 저용량 자원으로 인하여 고비도의 암호 알고리즘을 구현하기에는 불가능하다. RFID를 이용한 응용 시스템의 경우, 연산 능력과 저장 능력에 대한 제한적인 요소로서 기존의 공개키 방식이나 대칭키 방식의 암호화 알고리즘을 적용하기는 적절하지 않다. 현재까지 발표된 대표적인 연구결과의 대부분은 태그 내부에서의 실질적인 대칭키 암호 연산을 통한 보안 문제 해결로 접근하는 연구결과와 미약하고 아래와 같은 방법을 주로 연구하고 있다[7-9].

1) Full-fledged 방법 : 전자여권과 같은 분야에 응용되고 있으며 기존의 암호학적 방법인 단방향 해쉬함수 등을 사용한 방법이나 하드웨어적인 구성 요소가 많이 증가되는 단점을 가진다.

- 2) 난수 발생 방법 : 태그에 단방향 해쉬함수를 사용하거나 의사유도난수 발생기를 이용한 방법으로서 태그에서의 저용량 메모리를 고려할 때 현실적인 대안이 되지 못하고 있다.
- 3) 경량화 방법 : 의사난수 발생기, CRC(Cyclic redundancy code) 등을 사용하여 하드웨어적인 구성요소를 줄이는 방법을 개선한 방법이다.
- 4) 초경량화 방법 : XOR, AND, OR 과 같은 비트 연산을 사용한 단순한 방법을 사용하여 저가격의 RFID 시스템에 적용가능하나 보안상의 취약성을 가진다[10].

IV. 이기종간의 단말기간의 보안 분석

4.1. 보안 요구 사항

이기종 통합 무선망에서 각각의 망구조에 적합한 통합 환경의 보안적인 구조에 대해 분석하면 다음과 같은 사항을 고려해서 설계해야 한다.

- 1) 송신단에서 목적지까지의 다중 환경의 보안 메커니즘이 구현되어야 한다.
- 2) 단일의 최적화된 보안 메커니즘의 문제점으로 인하여 각 단계의 시스템에 대한 다중의 보안 메커니즘이 제공되어야 한다.
- 3) 트랜스포트 층에서 각각의 보안성을 구현하기 상위 레벨의 구현이 적합한 구조로 설계되어야 한다.
- 4) 이기종간에 서로 독립적인 상호 보안 인증 과정을 제공해야 한다.
- 5) 상위 계층에서 여러 종류의 보안 메커니즘을 사용하기 위하여 유연성을 제공해야 한다.

4.2. 보안 요구 사항

(그림 1)에서 보는 바와 같이 통합 환경 하에서 각각의 네트워크에 접근하기 위해 요구되는 보안 절차 구간은 다음과 같다.

- 1) 사용자와 노드간의 인증을 위한 절차
- 2) 센서 네트워크 환경 하에서의 Sink에 대한 센서 디바이스의 인증 절차

- 3) 에드 홉 네트워크와 각각의 센서 네트워크 간의 인증 절차
- 4) 에드 홉 망과 무선랜 사이의 인증 과정
- 5) 무선랜과 셀룰라 망과의 인증 절차

<표 1>은 일반적인 WSN(Wireless sensor network)과 RFID 시스템과의 특징을 나타내고 있다[6].

표 1. WSN과 RFID 시스템의 비교
Table. 1 Comparison of WSNs and RFID systems

특징	WSN	RFID
목적	부착된 물체의 조건에 대한 센서 파라미터 인식	태그가 장착된 물체를 인식
구성 요소	센서 노드, 릴레이 노드, 싱크	태그, 리더
프로토콜	지그비, WIFI	RFID 표준
통신	멀티 홉	단일 홉
이동성	센서 노드는 정적임	태그는 부착된 물체에 의해 동적임
전원	배터리 장착	능동적 혹은 태그에 부착
프로그램 가능	프로그램 가능	불가능
가격	센서 노드가 고가	리더는 고가, 태그는 저가
배치	이동 혹은 고정	고정형

4.3. RFID 시스템에서의 위협 요소 분석

일반적인 RFID 시스템을 구현했을 경우 보안적인 취약성으로 인하여 발생할 수 있는 위협 요소들은 현재 많이 제시되고 있으며, 이에 대한 많은 연구가 진행되고 있다. 현재까지 알고리즘의 취약성으로 인하여 그 해결책은 아직 해결되지 못하고 있는 실정이며, 그 주요 내용으로는 물리적 공격, 서비스 부인 공격, 위조, 스푸핑, 릴레이 공격, 도청 등이 있다[11-14].

V. 결 론

최근에는 유선망과 무선망의 통합 환경으로 인하여 유선망과 통신망의 구분이 없이 통합되는 구조의 환경

으로 발전하고 있다. 따라서 기존의 유선망에서 사용하는 보안 알고리즘을 무선망에서 공통적으로 사용하기에는 무선 환경 하에서의 통신망의 취약성으로 인하여 동일한 방식으로 접근할 수가 없다. 따라서 본 논문에서는 이기종간의 통합 환경 하에서의 고려해야 하는 보안 메커니즘을 분석하였다.

참고문헌

- [1] Di Ma and Gene Tsudik, "Security and Privacy in Emerging Wireless Networks", IEEE Wireless Communication, Oct 2011, pp.12-21
- [2] Lenka Lhotska, "Security Recommendation for Implementation in Distributed Healthcare System", ICCST 2008, pp.76-83
- [3] Ming Li, etc, "Data Security and Privacy in Wireless Body Area Networks", IEEE Wireless Communication, 2010, pp.51-58
- [4] Jelena Masic, "Enforcing Patient Privacy in Healthcare WSAs Using ECC Implemented on 802.15.4 Beacon Enabled Clusters", 6th Annual IEEE International Conference on Pervasive Computing and Communications, 2008, pp.686-690
- [5] Jung Tae Kim, "Privacy and Security Model for RFID Healthcare System in Wireless Communication Network", vol.16, no.6, 2012, pp.1223-1128
- [6] Hai Liu, etc, "Taxonomy and Challenges of the Integration of RFID and Wireless Sensor Networks", IEEE Network, 2008, pp.26-32
- [7] Faouzi Kamoun. "RFID System Management: State-of-the Art and Open Research Issues" IEEE Transactions on Network and Service Management, vol.6, no. 3, pp.190-205, Sep. 2009
- [8] George Pouloupoulos, Konstantinos Markantonakis, Keith Mayes, "A Secure and Efficient Mutual Authentication Protocol for Low-Cost RFID Systems", pp.706-p.711, 2009 International Conference on Availability, Reliability and Security
- [9] S.A.Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Comp., volume 2802 of LNCS, pages 201-212, 2004.
- [10] H.-Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 4, 2007, pp.337-340.
- [11] A. Juels, "RFID Security and Privacy: A research survey", Selected Areas in Communications, IEEE Journal, pp.104-112, 2006
- [12] Faouzi Kamoun, "RFID System Management: State-of-the Art and Open Research Issues", IEEE Transaction on Network and Service Management, vol.6, no.3, Sep, p.190-1205, 2009
- [13] A. Bongdanov, etal, "Hash Functions and RFID Tags: Mind the Gap," Proc. of the CHES08, vol. 5154 of LNCS, p.283-299, 2008
- [14] M. Feldhofer, etal, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. of the CHES04, vol.3156, p.85-140, 2004

저자소개

김정태(Jung Tae Kim)

2001년 8월 : 연세대학교 대학원
전자공학과 박사
1991년 8월 ~ 1996년 2월 : 한국전자
통신연구원(ETRI)
선임연구원

2002년 10월 ~ 현재 : 목원대학교 전자공학과 교수
※ 관심분야 : Network Security, 보안 컨설팅, RFID & USN Security, ASIC Design.