센서 네트워크 보안프로토콜에 대한 연구

조남필*, 한영주*, 정태명**
*성균관대학교 컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail : {npcho,yjhan}@imtl.skku.ac.kr* , and tmchung@ece.skku.ac.kr**

A Study for Security Protocol of Sensor Network

Nam-pil Cho*, Young-ju Han, Tai-Myung Chung**
*Dept. of Computer Engineering, Sungkyunkwan University
**School of Information &.Communication Engineering, SungKyunKwan University

요 약

장소에 상관없이 언제 어디서나 네트워크에 접근하여 자신이 원하는 정보를 쉽게 얻을 수 있는 유비쿼터스 컴퓨팅에 대한 많은 연구가 진행되고 있다. 유비쿼터스 환경에서의 센서 네트워크(USN)는 정보를 수집하고 전달하기 위한 가장 기본적인 기반 기술이라고 할 수 있다. 그러나 센서 네트워크는 고유의 특성으로 인하여 기존의 네트워크보다 더 많은 보안 취약성을 가진다. 본 논문에서는 유비쿼터스 환경에서 기반기술인 센서 네트워크에서 안전한 정보의 전달을 위한 보안프로토콜의 작동 원리를 알아보고 개선 사항에 대해서 생각해 보고자 한다.

1. 서론

센서 네트워크는 특정 요청에 의해 원하는 정보를 수집하여 전달해주는 센서로 구성된 일종의 애드 혹(AD-hoc)네트워크이다. 센서 네트워크는 유비쿼터스 센서네트워크(USN)와 무선센서네트워크(WSN)로 구분할 수 있다. 근래에 활발한 연구가 진행되고 있는 유비쿼터스 환경에서의 센서 네트워크는 RFID 기술과 접목하여 사물이나 사람에 이식된 전자 태그에서 센서 노드가 정보를 읽어 들여 이를 사용하는 방식이다. 무선센서네트워크는 수많은 센싱 노드들을 원하는 장소에 넓게 분포 시키고 이중에서 유효한 센싱노드에서 정보를 취하는 방식이다. 이는 군사적인 목적이나 자연재해의 예방뿐이 아니라 실생활의 전반적인 모든 환경에 적용이 가능하다.[8]

유비쿼터스센서네트워크와 무선센서네트워크가 서로 지향하는 점은 다르지만 센서 네트워크의 궁극적인 목적은 모든 사물에 컴퓨팅 능력 및 무선통신 능력을 부여하여 "언제", "어디서나" 사물들끼리의 통신이 가능한 유비쿼터스 환경을 구현하는 것이다.

센서 네트워크는 앞으로 실생활의 많은 부분에서 적용이 될 것이고 많은 정보가 이를 통해서 전달이 될 것이다. 이렇게 전달되는 정보의 신뢰성은 센서 네트워크를 통해 제공되는 서비스의 안정성뿐만이 아니라 개인정보보호에도 중요한 요소이다. 그러나 센서 네트워크는 고유의 특성에 의해 보안상 많은 취약점들을 내포하고 있다.

센서 네트워크에서 센서 노드들간의 통신은 무선통신 방식을 이용한다. 이러한 무선통신 방법은 장소의 제약을 받지는 않지만 보안에 큰 약점을 가진다. 또한 센서 네트워크의 특성상 센서의 수가 매우 많고 센서의 삽입과 제거, 이동이 빈번히 일어나는 특성을 가진다. 따라서 데이터의 도청이나 악의적 노드의 삽입 등이 쉽게 이루어 질 수 있다.[9]

이러한 보안의 중요성을 인식하고 효율적인 환경을 구축하기 위해서는 보안 적용을 후자로 두지 말고 환경구축에서부터 고려 해야 한다.

본 논문에서는 센서 네트워크에서 노드간의 보안에 초점을 맞추어 보안 프로토콜들이 어떻게 보안을 제공하는지 알아보고, 단점이나 개선 가능한 사항에 대해서 살펴본다. 2 장에서는 센서 네트워크가 가지게 되는 제약사항과 센서 네트워크에서 보안에 대한 위협에 대해서 알아보고, 3 장에서는 센서 네트워크에서의 보안 평가 요소를 살펴본다. 4 장은

한글 : 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성·지원사업의 연구결과로 수행되었음

SPINS(Security Protocol for Sensor Network)와 LEAP(Localized Encryption and Authentication Protocol)라는 보안 프로토콜을 분석하고 각각 프로토콜에서의 키 관리의 관점에서 장단점을 비교 해본다. 마지막 5장에서 결론을 맺는다[1], [2].

2. 관련 연구

2.1 센서 네트워크의 정의 및 의미

센서 네트워크를 정의 하자면 간단한 작업을 수행하는 센싱 기능을 갖는 초소형 디바이스(프로세서)를 일반사물에 장착하고 무선 송/수신기능을 탑재하여 서로간에 무선 네트워크로 센싱 정보를 주고 받아 호스트나 인터넷상으로 정보를 전송하여 원격지 상에서 전체상황을 감시/제어하는 시스템이라고 말할 수 있다[3]. 이는 과학 기술의 발달로 인한 소형화 된 네트워크 디바이스와 컴퓨팅 디바이스가 일반 사물에서부터 심지어 사람에게 까지 이식된다는 것을 의미한다.

유비쿼터스 환경에 관한 연구가 활발히 진행되면서 센서 네트워크는 기반 기술로 자리를 잡았고 현재 활발히 연구가 진행되고 있다. 센서 네트워크는 우리의 실생활에 다가올 큰 변화의 핵심 기반 기술이면서 IT 선진국인 우리나라의 성장을 책일 질 IT839 전략의 핵심 기술이다.

2.2 센서 네트워크의 제약사항

센서 네트워크에서의 센서 노드들은 무선 환경의 통신을 하고 전력을 공급받지 못하는 컴퓨팅 디바이스 들이다. 이들간의 보안을 적용하기 위해 많은 연구가 진행되고 있지만 센서 네트워크의 제약사항은 연구에 많은 어려움을 주고 있다.

센서 네트워크에서의 기본적인 제약사항은 다음과 같다.

- 전원 공급의 제약
- 프로세싱 능력의 제약
- 메모리의 공간의 제한
- 유선망에 비해 적은 전송 대역폭
- 무선환경으로 인한 보안 취약성 및 전송 거리의 제한

앞에서 언급했듯이 센서 네트워크는 일종의 애드 혹네트워크이다. 그러므로 애드 혹 네트워크가 가지는 제약사항도 가지게 되고 이는 다음과 같다[4].

- 잦은 네트워크 토폴로지 변경
- 잦은 라우팅 변경
- 데이터 전송속도/패킷 사이즈
- 채널 에러/지연

기존에 제안되어왔던 많은 암호화 기법이나 보안 기법들은 큰 컴퓨팅 파워와 메모리를 요구하기 때문에 센서 네트워크에 보안을 적용하기 위해서는 위에 열거한 제약 사항들을 고려한 새로운 암호화 기법 및 보안 기법이 필요하다.

2.3 센서 네트워크에서의 보안위협 유형

센서 네트워크에서는 일반적인 네트워크 환경에서의 위험 요소와 더불어 무선 전송 환경 및 애드 혹 네트워크가 가지는 보안 위험 요소까지 가지게 된다.

다음은 일반적인 센서 네트워크에서 자주 언급되는 보안위협의 유형들이다[4].

- 센서노드 공격
- 도청공격(Eavesdropping)
- 센싱 된 데이터의 프라이버시
- 서비스거부(DoS) 공격
- Sybil 공격

3. 센서 네트워크에서의 보안 평가 요소

3.1 데이터 인증

데이터 인증은 센서 네트워크에서 가장 중요한 보안 평가 요소이다. 센서 노드와 노드, 혹은 노드와 기지국(Base Station)간의 데이터의 전달이 일어날 때 공격자에 의해 메시지가 쉽게 삽입이 될 수 있으므로 잘못된 메시지를 수신하지 않기 위해 데이터 인증이 필요하다.

일반적인 상황에서는 공개키 방식을 취해서 데이터의 인증을 적용한다. 하지만 공개키 방식은 큰 자원의 소모를 동반함으로 센서 네트워크 제약사항에 위배된다고 할 수 있다. 결국 비밀키를 사용하는 MAC(Message Authentication Code)을 적용하여 데이터 인증을 하게 된다. 하지만 비밀키 방식을 사용해서 브로드캐스팅이 이뤄질 경우 수많은 노드 중 하나가 악의적인 노드라면 보안에 구멍이 생길 수 밖에 없다.

이를 예방하기 위해 SPINS 에서는 지연된 키의 노출과 단 방향 함수 키 체인을 제안하고 있다.

3.2 데이터 기밀성

키 교환 메시지 같은 중요한 메시지의 경우는 데이터의 기밀성이 꼭 지원 되어야 한다.

센서 노드간의 통신은 무선 통신 방식 임으로 도청에 취약하다는 큰 단점을 가지게 된다. 즉, 원하던 원하지 않던 노드 주변에 위치를 하게 되면 통신 내용을 볼 수 있게 된다. 그러므로 노드간의 메시지 교환 시 비밀키를 사용하여 암호화 하고 이를 보내는 방식을 사용한다.

3.3 데이터 무결성과 객체 무결성

센서 네트워크에서 무결성은 노드간의 전송되는 메시지에 대한 무결성과 객체간의 무결성을 말한다.

데이터의 무결성은 일반적인 보안에서 말하는 무결성과 같은 의미를 가진다. 이는 메시지 인증 코드인 MAC을 사용 함으로서 쉽게 적용 할 수 있다.

객체에 대한 무결성은 노드 자체를 공격자가 다른 것으로 변경 시킬 수 있다는 것을 말한다. 비밀키 위주로 보안을 적용하는 센서 네트워크에서 노드가 악의적으로 변경이 되었다는 것은 비밀키의 노출 등에서 큰 위협에 처할 수 있게 된다. 노드에 대한 물리적인 공격으로 가능한 이러한 위협에 대처 할 수 있는 연구가 더 진행 되

어야 한다.

3.4 데이터 신선성

데이터 신선성은 구 데이터의 대한 재사용을 방지하는 것을 말한다. 데이터의 신선성은 Count 값을 사용하여서 데이터가 전에 사용되었는지를 구별해 낸다.

일반적으로 약한 신성성과 강한 신선성의 2 가지 기술이 있다. 약한 신선성은 count 값만을 사용하고, 강한 신선성은 임의의 난수 값을 사용하여 요청과 응답 메시지를 비교하여 신선성을 제공한다.

4. 센서 네트워크의 보안 프로토콜

4.1 SPINS (Security Protocol for Sensor Network)

SPINS 는 SNEP (Sensor Network Encryption Protocol)와 μTESLA (the "micro" version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol)의 2 가지 보안 요소로 구성되어 있다.

4.1.1 SNEP

SNEP 는 다음의 보안 요소들을 제공한다.

- 데이터 기밀성
- 양단간 데이터 인증
- 재사용 방지
- 신선성(freshness)
- 무결성

SNEP 은 양 노드간의 공유된 키를 기반으로 생성되는 MAC 값을 가지고 서로의 인증을 제공한다. 기밀성을 제공하기 위해서는 Count 값을 메시지와 포함하여 암호화를 한다. 이는 같은 메시지를 암호화 하더라도 변하는 Count 값에 의해 매번 다른 값으로 암호화가 되기 때문이다. 또한 MAC 값은 재사용 방지와 무결성에도 유용하게 쓰인다.

$A \rightarrow B : N_A, R_A$

$B \rightarrow A : \{R_B\}_{<k_{encr,C}>}, MAC(k_{mac}, N_A | C | \{R_B\}_{<k_{encr,C}>})$

K_{encr} : 암호화 키
K_{mac} : MAC 키
C : counter, initialization vector
N_A : nonce

[그림 1] SNEP Message

SNEP 은 낮은 통신 오버헤드를 발생시키고 Count 값이 양단간에 공유되므로 전송 양을 줄일 수 있으며 RC5 같은 비밀키 암호화 알고리즘을 사용하여 보안을 제공함으로 자원의 소모를 줄일 수 있다는 장점을 가지고 있다.

4.1.2 μTESLA

일반적인 브로드캐스팅의 인증은 공개키 알고리즘을 사용하여서 보안을 제공한다. 하지만 센서 네트워크에서 공개키 알고리즘을 이용한 인증 서비스는 제약사항에 위배 된다.

TESLA[5]를 변형시킨 μTESLA 는 대칭 키 시간 지연 메커니즘을 사용한 단 방향 키 체인을 통해 공개키 메커니즘에서 제공하는 인증 효과를 제공한다. [6]

기지국에서는 마지막 키 Kn 을 랜덤하게 생성하고 단 반향 함수를 사용하여 나머지 키를 생성한다. 이렇게 나눠진 키는 특정시간에 특정 키만이 공개 된다. 해당 시간에 공개된 키를 노드가 받아서 단 방향 함수를 통해 키를 검증하게 되어 자신이 받은 메시지의 인증을 받을 수 있게 된다.

$M \rightarrow S : N_M$

$S \rightarrow M : T_S | K_i | T_i | T_{int} | \delta$
$MAC(K_{MS}, N_M | T_S | K_i | T_i | T_{int} | \delta)$

Ts : current time
Ki : one-way key chain using past interval i
Ti : starting time
Tint : time interval
δ : disclosure delay

[그림 2] μTESLA Message

μTESLA 는 기지국에서 전달되는 브로드캐스팅 메시지의 인증을 가능하게 해준다. 하지만 시간 동기화를 해야 하며, 노드의 수가 증가할수록 각 노드별 시간 할당이 증가함으로 기지국에서 말단 노드까지의 인증에 상당한 시간이 소요된다는 단점을 가진다. 또한 노드에서 브로드캐스팅을 하게 될 경우는 노드가 기지국에 SNEP 를 사용하여 메시지를 보내고 기지국에서 다시 μTESLA 를 사용해서 메시지의 전달이 이뤄지게끔 작동해야 한다. 이는 노드가 제한된 저장공간과 프로세싱 파워를 가지기 때문에 단 방향 키 체인과 모든 노드와 공유되는 키를 저장하지 못하며, 키 체인을 저장한다 하더라도 브로드캐스팅이 일어날 때마다 키 체인을 계산할 수 있는 능력을 가지지 못하기 때문이다.

4.2 LEAP

LEAP 는 4 개의 암호키를 가지는 센서 네트워크를 위한 키 관리 프로토콜이다. SPINS 의 경우 특정 노드가 자신과 비슷한 환경에 위치하는 근접 노드들에게 메시지를 전달할 경우 기지국에 메시지를 보내고 기지국에서 브로드캐스팅 하여 메시지를 전달한다. 하지만 LEAP 의 경우 노드 자체 적으로 One-hop 브로드캐스팅 인증을 단 방향 키 체인을 사용하여 가능하게 한다. 이는 μTESLA 의 지연 키 공개 기술과는 다르다.

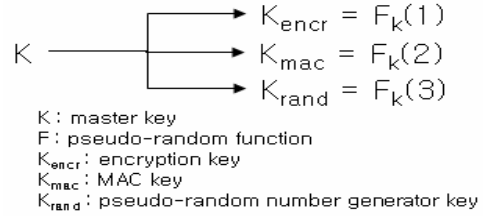
다음은 LEAP 서 사용 되는 암호키 들이다.

- 개인키: 모든 노드는 기지국과 공유하는 노드만의 키를 가지고 있다. 이 키는 노드와 기지국간에 보안통신에 사용된다.
- 그룹키: 기지국이 브로드캐스팅 메시지를 암호화 하여 네트워크의 모든 노드에 전송 할 때 사용하는 키이다.
- 클러스터 키: 하나의 노드와 그 노드에 이웃하는 모든 노드들이 공유하는 키이다. 이 키는 지역적인 브로드캐스팅을 할 때 주로 사용된다.
- 쌍 공유키(Pairwise Shared key): 모든 노드는 그

들의 직접적인 이웃들과 쌍 공유키를 공유한다. 이 키는 프라이버시 혹은 원천지 인증의 통신에서 안전한 통신을 위해서 사용된다. 예를 들면 클러스터 키를 자신의 이웃 노드들에게 분배를 할 때 쌍 공유키를 사용하여 안전하게 분배 한다.

4.3 SPINS 와 LEAP 에서 키의 의미

센서 네트워크 보안 프로토콜에서 가장 많이 언급되고 있는 SPINS 와 LEAP 에 대해서 간략하게 살펴보았다. SPINS 는 키 관리를 기지국에서 실행하고 노드는 단지 기지국과 공유하는 초기의 Master 키만을 가지고 있고 이 키를 중심으로 Pseudo-random function 을 실행하여 암호키와 MAC 키 그리고 Random 키를 만들어 낸다. [7]



[그림 3] SPINS 의 키 생성 과정

LEAP 는 보안의 핵심인 키와 관련된 키 관리 프로토콜이다. 각각의 노드는 자신의 주변 이웃 노드의 변화에 따라 스스로 키를 생성한다는 점이 SPINS 와 가장 큰 차이를 보인다.

SPINS 에서의 키들은 보안을 제공하기 위한 키로서 사용된다. 마스터 키를 사용하여 생성되는 부수적인 키들은 보안의 요소들을 제공할 때 쓰이는 역할만을 할 뿐이다. 하지만 LEAP 의 경우는 보안의 요소를 제공하는 키이면서 더불어 지역적인 개념을 추가 하고 있다. 클러스터 키나 쌍 공유키는 주체가 되는 노드의 주변에 위치하고 있는 이웃 노드들 간 공유되는 키이다.

이러한 위치의 개념을 적용한다면 SPINS 의 μTESLA 가 가지는 단점을 상당수 완화시킬 수 있다. 특정 노드가 자신과 비슷한 환경에 위치하는 근접한 이웃 노드들에게 브로드캐스팅을 하기 위해서 기지국에 메시지를 전달 할 필요 없이 클러스터의 개념을 적용한 One-Hop 브로드캐스팅을 적용한다면 자원의 효율성과 강한 보안성을 둘 다 제공해 줄 수 있다.

다음은 SPINS 와 LEAP 를 비교한 표이다.

	SPINS	**LEAP**
키의 개수	4 개	4 개
키 생성 위치	기지국, 노드	기지국, 노드
키의 관리	기지국에 의존적	노드에 의존
키의 특징	보안적 측면 고려	보안적인 측면과 더불어 위치 개념 적용

[표 1] SPINS 와 LEAP 의 키 비교

5. 결론 및 향후 계획

현재 센서 네트워크의 기반 기술에 대한 연구가 활발히 진행 중이며 보안에 관한 기술 개발도 같이 진행 되고 있다. 하지만 연구 및 개발 과정은 초기 단계에 있는 실정이다. 센서 네트워크가 가지는 제약 사항을 고려 하면서 더 효율적인 보안 프로토콜의 개발이 이뤄 져야 한다.

본 논문에서는 센서 네트워크 보안 프로토콜인 SPINS 와 키 관리 프로토콜인 LEAP 에 관하여 살펴보고 키 관리의 관점에서 서로를 비교해 보았다. SPINS 에서 LEAP 의 클러스터 모델을 적용한다면 μTESLA 에서 가지는 단점을 보완 할 수 있을 것이다. 향후 이 부분에 대한 연구를 진행 할 계획이며 성능 평가를 진행 하여 좀더 효율적인 보안 프로토콜의 설계에 대한 연구를 진행할 것이다.

참고문헌

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar. “SPINS: Security Protocols for Sensor Networks.” In Proc. of Seventh Annual ACM International Conference on Mobile Computing and Networks(Mobicom 2001), July 2001.

[2] Sencun Zhu, Sanjeev Setia, Sushil Jajodia “LEAP: Efficient Security Mechanisms for LargeScale Distributed Sensor Networks” CCS’03, Aug 2004

[3] 강석철 “센서 네트웍 시대의 미래", 전자정보센터, 2004.

[4] 전길수 ”홈센서 네트워크 보안 프레임 워크", 홈네트워크 시큐리티 포럼, July.2004.

[5] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song. Efficient authentication and signing of multicast streams over lossy channels. In IEEE Symposium on Security and Privacy, May 2000.

[6] L. Lamport. Constructing digital signatures from a one-way function. Technical Report CSL-98, SRI International, Oct 1979.

[7] O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions. Journal of the ACM, Vol. 33, No. 4, pp 210-217. 1986

[8] 신순자, 임진수 “유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향연구” 한국전산원, Oct.2004

[9] 나재훈, 채기준, 정교일 “센서 네트워크 보안 연구 동향” 전자통신동향분석 제 20 권 제 1 호, Feb 2005