USN 서비스 미들웨어 보안 프레임워크

나상호*, 황선민*,신영록*, 허의남*

*경희대학교 컴퓨터공학과
e-mail:{shna | hsunny | shinyr}@icns.khu.ac.kr, johnhuh@khu.ac.kr

USN Service Security Middleware Framework

Sang-Ho Na*, Sun-Min Hwang*, Young-Rok Shin*, Eui-Nam Huh*
*Dept of Computer Engineering, KyungHee University

요 약

다양하고 급속히 개발되는 USN 서비스에 대한 보안 서비스의 요구사항은 USN 서비스의 활성화에 큰 부담으로 작용하고 있다. 다양한 서비스 별 보안 표준기술 개발에는 많은 제약이 따른다. 보안 서비스 관점에서 USN 서비스들의 각 요소 별 추상화를 통해 참조 모델을 통해 USN 서비스에서의 보안 위협 분석을 통한 USN 보안 미들웨어 프레임워크 및 세부 컴포넌트 설계를 제안하고자 한다.

1. 서론

USN 서비스가 다양한 분야에 걸쳐 급속한 개발이 이루어지고 있으나 USN 서비스에 대한 보안 요구사항은 USN 서비스 활성화에 큰 부담으로 작용하고 있다. USN 서비스의 종류와 그 내용에 따라 다양한 보안 요구사항이 제안되고 있으며 센서의 하드웨어적 특성으로 인해 보안 기술의 표준화에 많은 제약이 따른다.

또한 USN 서비스의 특성상 센서 네트워크, IP 네트워크, 그리고 NGN망의 연동을 통한 통합네트워크를 지향하고 있으며, 다양한 컨버전스 단말 기기의 연결을 위해서 보안 서비스 제공에 있어 표준화가 시급하다.

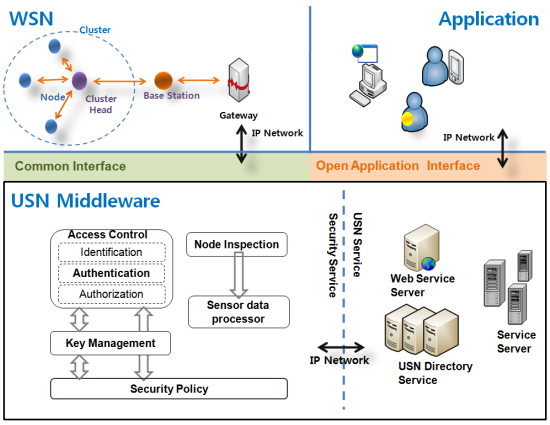
USN 서비스 보안 표준 기술을 위해 USN 서비스를 분류하고 그에 따른 보안 요구 사항 분석을 통해 USN 서비스 보안 프레임워크 설계가 필요하다.

기 발표한 논문 'USN 서비스 분류를 통한 보안 위협 요소 분석'[1]의 결과를 토대로 본 논문에서 USN 서비스 미들웨어 보안 프레임워크를 설계를 제안하고자 한다.

2. USN 서비스 보안 위협과 요구사항

USN 서비스에서 보안 서비스는 USN 미들웨어 계층의 보안 매니저에 의해 이루어지며 그림1은 USN 서비스 미들웨어의 역할을 보여준다. 본 섹션에서는 안전한 USN 서비스 제공을 위해서 센서 네트워크(WSN)와 응용 서비스(Application) 두 요소의 보안 위협 분석하고 센서, USN 미들웨어, 응용 서비스를 다음과 같이 두 구간으로 나누어 보안 요구 사항을 분석한다.

- USN 미들웨어와 센서 네트워크 구간
- 응용 서비스와 USN 미들웨어 구간



(그림 1) USN 서비스 모델

2.1.센서 네트워크에서의 보안 위협

센서 네트워크(WSNs)는 ITU-TX.800, ITU-T X.805 그리고 TD4023에서도 언급하고 있듯이 센서 노드의 하드웨어적인 제약 및 무선 네트워크 특성에 따른 노드 탈취 및 손상, 감청, 서비스 거부 공격 및 라우팅 공격에 취약하다.

- 센서 노드 탈취 / 포섭 : 센서 네트워크는 일반적으로 잠재적인 위험이 내재된 지역에 배치되며 공격자로 인해 탈취 되거나 손상을 입게 된다. 일단 손상된 센서 노드는 공격자의 추가적인 공격에 이용된다.
- 감청 : 센서 네트워크의 무선 통신은 공격자의 노드

간 통신 감청에 매우 취약하다. 따라서, 감청에 대한 공격에 대해 데이터 암호화가 필요하며 견고한 키 분배 및 암호화 기법이 요구된다.

• 서비스 거부 공격 : 무선 통신에 대한 서비스 거부 공격에는 jamming attack, collision attack 그리고 denial-of-sleep attack 등이 있다. 이는 센서 노드의 배터리 소모를 일으켜 센서 네트워크 수명을 감소시키며, 서비스 거부 공격을 바탕으로 추가 공격을 시도할 수 있다.

• 라우팅 공격 : 멀티 홉 라우팅 프로토콜을 사용하는 센서 네트워크에서 라우팅 공격은 서비스 거부 상태의 원인이 되며 스푸핑(Spoofing), 셀렉티브 포워딩(Selective Forwarding), 싱크홀(Sinkhole), 웜홀(Wormhole), 시빌(Sybil) 그리고 헬로우 플러딩(Hello Flooding) 공격 등이 있다.

• 프라이버시 침해 : 공격자는 센서 노드 포섭을 통해 감청, 쿼리 공격, 저장된 데이터 접근 등을 통해 개인 정보 수집이 가능하다. 따라서 USN 서비스를 제공함에 있어 개인 정보 보호가 보장되어야 하며 외부 IP 네트워크의 인가된 사용자에 한해 접근이 허가되어야 한다. 접근 제어 및 데이터 암호화는 USN 서비스 보안 정책에서 가장 중요한 요소들이다.

2.2. 응용 서비스에서의 보안 위협과 요구사항

IP네트워크에서의 보안 위협은 ITU-T X.805권고사항에 명시되어 있다. 권고사항의 내용은IP네트워크를 통한 의도적 공격을 막고, 보안 취약점에 의해 발생할 수 있는 위협에 대한 보안 이슈와 요구사항이 포함되어 있다. 본 섹션에서는 ITU-X.805 문서의 내용을 바탕으로 USN 서비스 보안 요구 사항을 살펴보자.

• 접근제어 : USN 서비스는 오직 인가된 사용자 혹은 단말에게만 서비스를 제공한다.

• 인증 : USN 서비스에 접근 하려는 사용자 혹은 단말의 신분 확인을 위하여 커버로스(Kerberos)와 같은 인증 기법이 사용될 수 있다.

• 부인 방지 : USN 서비스 보안 모듈은 USN 서비스나 미들웨어에 접근하려는 사용자 혹은 단말에 대해 부인 방지 서비스를 제공해야 한다.

• 데이터 기밀성 : 데이터의 전송, 가공, 저장에 있어 네트워크 장비의 불법적인 접근, 열람 및 재전송으로부터 보호되어야 한다.

• 데이터 무결성 : 데이터의 전송, 가공, 저장에 있어 네트워크 장비의 허가되지 않은 수정, 삭제, 그리고 복제에 보호되어야 한다.

• 유용성 : USN 미들웨어는 다양한 종류의 DoS 공격에 대해 안전해야 하며, 사용자 정보의 변경, 삭제 등의 수동적 공격(Passive Attack)으로 부터 보호 되어야 한다.

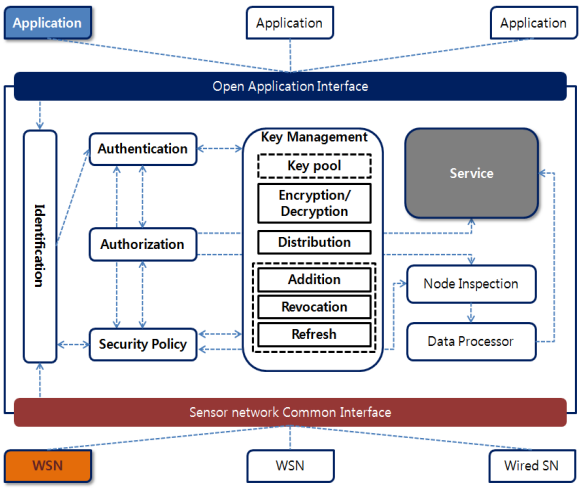
• 안전한 통신 : 사용자와 USN미들웨어 사이에서 USN 서비스 데이터의 전송, 가공, 저장 시 네트워크 장비에 의한 데이터의 우회나 가로채기 공격에 보호되어야 한다.

• 프라이버시 보호 : 사용자와 미들웨어 사이에 인증과 암호화를 통해 USN 서비스 데이터의 불법적인 이용 대해 안전성을 보장 받아야 한다.

3. USN 서비스 미들웨어 보안 프레임워크

USN 서비스에서 미들웨어는 이 기종 센서 네트워크와의 연동으로 데이터 수집과 센서 네트워크 관리, 수집된 데이터의 가공과 의미화 과정을 통한 정보 및 서비스의 생산, 그리고 개방형 인터페이스를 통한 응용 서비스로 제공한다. 또한 USN 미들웨어는 USN 서비스의 보안 서비스를 통해 USN 서비스의 신뢰성을 보장해 줄 수 있어야 한다.

전술한 바와 같이 USN 서비스는 크게 Sensor Network, Service, Application의 세 가지로 구성되고, USN 서비스의 통합 관리 역할을 수행하는 미들웨어의 중요한 기능 중의 하나는 보안 매니저로서의 역할이다. 이는 USN 서비스 전반적인 보안 정책을 수립하고 센서 네트워크 및 USN 응용서비스 인증, 공격 탐지, 키 관리 등 보안 프레임워크로서 기능을 담당한다. 본 섹션에서는 다음 그림2와 같이 USN 미들웨어 보안 컴포넌트를 제안하고, USN 미들웨어의 보안서비스(Security Service)의 내부 컴포넌트를 정의하고 그 기능을 간략히 제시 한다.



(그림 2) USN 미들웨어 보안 프레임워크

3.1. 컴포넌트 정의 및 기능

3.1.1. 보안 정책(Security Policy)

보안 정책 컴포넌트는 센서 네트워크의 센서 노드 및 응용 서비스와 미들웨어 간 인증 및 인가, 센서 네트워크 노드 탐지 등 보안 서비스 전반에 관련된 정책을 담당한다. 주요 보안 정책은 다음과 같다.

• Network Security - 네트워크상의 어떠한 자원을 보

호할 것인가를 다룬다. 보안 평가 요소로는 access control, firewall, remote access, directory service 그리고 Internet Services 등이 있다.

• Access Control – 누가(who) 어떠한 자원(what)에 접근할 수 있는가를 결정한다.

• Authentication – USN 서비스에 접근하기 위한 센서 혹은 유저 등의 인증에 대한 정책을 담당한다. 응용 서비스의 종류와 센서 네트워크의 특성에 따른 인증 정책을 결정한다.

• Key Management – 암호화와 관련하여 가장 중요한 정책으로 센서 네트워크의 형태에 따라 키의 길이, 키 변경, 키 생성, 키 분배 그리고 갱신에 대한 보안 정책을 결정한다.

3.1.2. 액세스 제어(Access Control)

센서 네트워크의 센서 노드와 응용 서비스의 인증 및 서비스 접근 권한을 통제를 통해 액세스 제어를 수행하며, 다음과 같이 세 가지 컴포넌트를 포함한다.

• Identification Component : 센서 노드 혹은 응용 서비스가 USN 서비스에 접근을 시도할 때, Identification 컴포넌트는 접근하려는 주체 식별하고 정보를 보안정책(Security policy) 컴포넌트에 전달하여 접근 주체에 적당한 보안 정책이 결정된다.

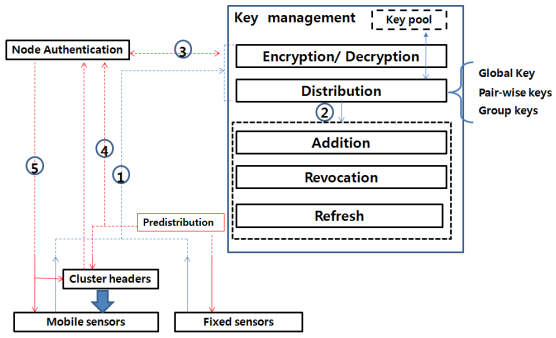
• Authentication Component : 보안 정책에서 결정된 정책에 맞추어 인증 과정이 수행된다. 센서 노드와 응용서비스 두 가지 인증을 수행하기 위해 센서 인증 컴포넌트와 응용서비스 인증 컴포넌트로 구성된다. 따라서 USN 서비스에서 인증 과정은 앞서 정의한 바와 같이 크게 센서 네트워크 – USN 미들웨어, USN 미들웨어 – 응용서비스 두 구간으로 나누어져 센서 네트워크와 응용 서비스에 대한 인증을 수행한다.

• Authorization Component : Identification 컴포넌트에서 전달 받은 주체 식별 정보에 따라 접근 권한을 부여한다.

3.1.3. 키 관리(Key Management) 컴포넌트

USN 미들웨어의 Key Management 컴포넌트는 IP 호스트 혹은 센서 노드 사이에 안전한 통신을 위하여 사용되는 모든 키를 관리하며 센서 노드를 위한 키 데이터베이스뿐만 아니라 IP 호스트를 위한 키 데이터베이스도 가진다. 센서 네트워크 및 응용 서비스 액세스 제어 및 데이터의 무결성, 기밀성 보장을 위해 암호화에 사용할 키 생성과 분배, 업데이트 등을 담당한다.

센서 네트워크 인증을 위해 그림 3과 같은 USN 미들웨어의 중앙 집중식 사전 키 분배를 위한 키 관리 컴포넌트를 제안하며 그 세부 내용은 다음과 같다.



(그림 3) 센서 노드 키 관리 컴포넌트

• 키 풀(Key pool) : 센서 노드의 배치 전 각 센서 노드는 세션의 확보를 위해 몇 개의 키를 생성하고 메모리에 적재되어 USN 미들웨어와 센서 노드 간 인증 및 통신 메시지 암호화에 사용하며, 키 생성과 관리를 위한 키 풀이 있다.

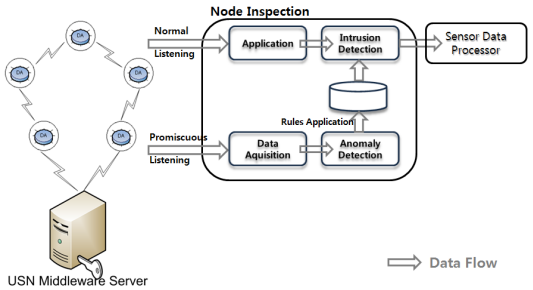
• 키 관리 컴포넌트의 기능 : 제안한 키 관리 컴포넌트는 센서를 위해 다음과 같은 세 가지 기능을 수행하는데, 세부 내용은 다음과 같다.

– 노드 추가 : 새로운 센서 노드가 네트워크에 추가될 때, Addition 모듈은 인증 함수를 알려 준다.(Step 1&2) WSN의 토폴로지가 고정되어 있다면, USN 미들웨어는 분배 함수를 이용해 정보를 교환(Step3)을 통해 WSN에 배치된다.(Step 4)

– 노드 삭제 : USN 미들웨어의 노드 탐지 컴포넌트가 악의적인 공격 노드를 탐지 했을 때, 해당 노드는 클러스터 헤드와 싱크 노드에 의해 WSN에서 제거된다.(Step 5)

– 갱신 : USN 서비스 미들웨어가 네트워크 내 센서 노드들의 갱신이 필요하다 판단되면, 네트워크 내 센서 노드들에게 재인증을 요청한다.

3.1.4. 노드 탐지(Node Inspection)



(그림 4) 노드 탐지 컴포넌트

USN 서비스에는 IP 네트워크로부터 다양한 공격 위협에 노출되어 있으며, 센서 네트워크는 무선 통신이 가지는 취약점으로 인한 위협이 존재한다. 노드 탐지 시스템은

DDoS, 바이러스 및 허가되지 않은 응용 서비스의 접근을 탐지, 차단한다. 또한 센서 네트워크에서 센서 노드는 공격자에 의한 탈취 및 포섭에 취약하고 이는 추가적인 공격의 발판이 되므로 신속한 탐지가 필요하다. 노드 탐지 컴포넌트(그림 4)의 기능은 다음과 같다.

- Promiscuous Listening 모드에서 쌓인 데이터는 Anomaly Detection 모듈을 위한 정상적인 데이터 샘플을 만든다.
- 센싱 된 데이터는 Anomaly Detection 모듈에 의해 체크되고 센서 네트워크에서 악성 노드 판단 규칙을 생성한다.
- 정상적인 데이터는 Application 모듈을 거쳐 침입탐지(Intrusion Detection) 모듈에서 확인 후 데이터 가공을 위해 USN 미들웨어로 전달된다.

4. 결론

다양한 USN 서비스가 개발되는 현 시점에서 미들웨어 보안 인증 프레임워크 표준화를 통해 USN 서비스 보안 연구의 기반을 마련 앞으로의 USN 보안 연구 방향을 제시해 줄 것으로 기대한다. 또한 각종 네트워크의 통합 및 이 기종 기기 간 연동에 있어 보안 프레임워크 및 보안 파라미터 제시는 사업자들의 USN 서비스를 위한 네트워크 기술 개발 및 기기 개발에 가이드라인을 제시해 USN 산업 활성화를 이끌 것으로 예상한다.

Acknowledgment

본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터지원사업의 연구결과로 수행되었음"
(IITA-2009-(C1090-0902-0002))

참고문헌

[1] 나상호, 황선민, 허의남, “USN 서비스 분류를 통한 보안 위협 요소 분석”, 한국인터넷정보학회, 2008
[2] A. Perrig, R. Szewczyk, V Wen, D.Culler, J. Tyger, "SPINS : Security Protocols for Sensor Networks." Wireless Network Journal, 2002.
[3] L. Eschenauer, V. D. Gligor, "A key-management scheme for distributed sensor networks." In Proceeding of the 9th ACM conference on Computer and communications security, page 41-47, November 18-22, 2002.
[4] 권태경 신수연 박상호 박태진, 무선 센서 네트워크 보안, 한국통신학회지, Vol.23 No.9, 2006.
[5] 이주영, 박소영, 이상호, “정보보안 : 계층적 센서 네트워크에서 안전한 통신을 위한 키 갱신 프로토콜”, 한국정보처리학회, 2006.
[6] 곽진, 오수현, “분산 센서네트워크용 키 분배 프로토콜 연구동향”, 정보통신연구진흥원 주간기술 동향, 통권 1307호, 2007.
[7] Sencun zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP : Efficient Security Mechanisms for Large-Scale Distributed Sensor Network", In Proc. of the 10th ACM CSS, '03, Oct. 2003s
[8] 이재광, 류옥현, 노성호, “USN 응용 서비스 요구사항 분석을 위한 응용 서비스 모델 분류 체계 및 활용 방안”, 『한국전자거래학회 학술대회 발표집』, 2007
[9] 정병호, 강유성, 김신효, 정교일, 양대현, "RFID/USN 환경에서의 정보보호 소고“, 『한국통신학회지』, 제21권 6호, 2004
[10] 이응용, 박광진, “USN 활성화를 위한 정보보호 요구사항”, 『한국통신학회지』, 제21권 9호, 2004
[11] 이준섭, 김은숙, 김형준, “USN과 BcN과의 연동 고찰”, 『한국통신학회지』, 제24권 8호, 2007
[12] 정보통신단체표준, TTAS_KO-06_0170, "USN 미들웨어 플랫폼 참조 모델“
[13] A. Liu and P. Ning. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In IPSN'08 : Proceedings of the 2008 International Conference on Information Processing in Sensor Networks(ipsn2008) ,USA,2008.
[14] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. Tinypk: securing sensor networks with public key technology. In SASN'04 : Proceeding 2nd ACM workshopon Security of adhoc and sensor networks, pages59~64, NewYork, NY, USA, 2004.
[15] S. Zhu, S. Setia, and S. Jajodia, LEAP: efficient security mechanisms for large-scale distributed sensor networks. Proceeding sof the 10th ACM conference on Computer and communications security, pp. 62 - 72, USA, 2003.
[16] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, SPINS: Security protocols for sensor networks, Wireless Networks ,2001.
en/index.asp
[17] L. Eschenauer and V. D. Gligor, A key-management scheme for distributed sensor networks. In ACM Conference on Computer and Communications Security, pages41~47,2002.
[18] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, A Survey of Key Management in Ad Hoc Networks. In IEEE Communications Surveys & Tutorials, 3rd Quarter, 2006.