안전한 무선 센서-액터 네트워크를 위한 센서 노드 보안

문미선, 김동성, 박종서*
*한국항공대학교 컴퓨터공학과

A Sensor Node Security for Secure Wireless Sensor and Actor Networks

Misun Moon, Dong Seong Kim, Jong Sou Park*
*Department of Computer Engineering, Hankuk Aviation University

요 약

센서 네트워크 활용의 현실성을 높이기 위해서는 센서 네트워크 보안에 대한 연구는 필수적이다. 현재 진행 중인 센서 네트워크 보안에 대한 연구는 노드 인증, 데이터 기밀성·무결성 제공에 초점이 맞춰지고 있다. 그러나 가용성에 대한 부분은 상대적으로 부족하다. 특히, 센서 네트워크의 구성요소인 센서 노드에 대한 침해는 네트워크 전체의 가용성을 저하시킬 수 있으므로 이에 대한 연구는 더욱 필요하다. 본 논문에서는 센서 노드의 보안을 위해서 Task-Role Based Access Control을 통한 접근제어 방법론을 제안한다.

I. 서론

센서 네트워크는 유비쿼터스(ubiquitous) 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 저전력의 많은 센서들로 구성된 무선 네트워크이다. 현실적이고 안전한 유비쿼터스 컴퓨팅 환경을 구현하기 위해서는 센서 네트워크의 활용 방안 및 센서 기술 개발과 함께 감지된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크상에서의 보안 메커니즘 개발이 반드시 함께 연구되어 적용되어야 한다. 현재 인증기법, 키관리 기법(그룹키 기반), 센서 노드간 Pairwise Key 설정 기법, 보안을 위한 센서 네트워크 구조 연구, 위치 기반 프라이버시 보호 등의 연구가 진행되고 있다[1].

센서 네트워크의 특성상 하나의 센서 노드가 침해되면 침해의 전파를 막기 위해 그 노드 또는 그 주변의 노드들을 block 해야 하는 상황이 발생한다. 침해되는 노드가 많아지면 이와 같은 이유로 네트워크 전체의 가용성이 떨어진다. 따라서 네트워크의 가용성을 위해 센서 노드 자체의 보안도 요구된다.

센서 노드의 보안을 위해서 센서 노드에 접근하려는 다른 노드(베이스 스테이션, 액터 노드 포함)를 제어한다. 본 논문에서는 Task-Role Based Access Control을 적용해 센서 노드 보안을 제안하고자 한다.

본 논문은 제안 방법론을 이해하기 위한 배경 지식을 2장에서 서술하고 3장에서 센서 노드 보안을 위한 접근제어 방법을 제안한다. 4장에서는 제안된 방법론을 보안면에서 분석하고 5장에서 관련연구와 비교하며 6장에서 결론을 맺는다.

II. 배경지식

2.1 키 사전분배

센서 노드 사이에 안전하게 키를 분배하는

키 사전분배에 대한 연구가 진행되었다. 확률적인 키 사전 분배 방법[2], q-composite 키 스킴과 random pairwise 키 스킴[3], 그리드 기반 키 사전분배 스킴[4], 그리드 기반 키 사전분배 스킴에 확률적인 키 사전분배를 합한 스킴[5] 등의 방법론이 제안되었다. 이들의 목적은 센서 노드의 키가 침해당하더라도 침해당하지 않은 나머지 센서 노드들의 안정성을 보장하자는 것이다. 키의 사전 분배가 중요한 또다른 이유는 키 사전 분배 후에 센서 노드간의 공유키 설정, 또한 안전한 라우팅 경로 확보의 전제 조건이기 때문이다.

2.2 SPINs: Security Protocol for Sensor Networks

센서 네트워크의 보안을 위해 설계된 SPINs은 SNEP(Secure Network Encryption Protocol))과 u-TESLA로 구성되어 있다. SNEP은 데이터 기밀성(data confidentiality), 인증(data two-party authentication), 초기성을 제공하고, u-TESLA는 인증된 streaming 브로드캐스팅을 제공한다[6]. SPINs에서 데이터 기밀성을 제공하는 암호화는 대칭키 방식의 알고리즘을 사용하며 이 키는 앞 절에서 설명한 키 사전분배 스킴에 따라 사전분배 되어 사용된다.

2.3 RBAC for Mobile Ad-hoc Network

Sye Loong Keoh와 Emil Lupu[7]는 무선 ad-hoc 네트워크에서 RBAC을 적용해 각 노드와 네트워크 전체의 보안을 강화하는 구조를 제안했다. 이 구조는 TESLA를 통한 보안 브로드캐스팅을 통해 인증서를 교환하고 멤버십을 관리한다. 그리고 이 멤버십을 기반으로 role을 할당하고 접근제어를 하는 RBAC 메커니즘을 사용한다. role은 URA(User-Role Assignment) 정책에 따라 설정된다.

이 방법론은 멤버십 관리를 위해 노드 중에 하나의 cooperator를 선택하고 이 cooperator가 일정 시간마다 인증서와 멤버십 리스트를 네트워크의 노드들에게 브로드캐스트한다. 이를 통해 네트워크에 동적으로 합류 또는 탈퇴도 가능하고 네트워크에 불법적으로 접근하려는 노드를 제한할 수도 있다. 그러나 센서 네트워크는 자원의 제약이 크므로 인증서를 통한 접근제어는 불가능하다. 따라서 센서 네트워크에 적용 가능한 형태로 수정하여야 한다.

Ⅲ. 제안 방법론

3.1 전체 구조

먼저 2.3절에서 설명한 인증서 방식에서 많은 자원을 요구하는 인증서대신 센서 네트워크에서 멤버십 관리에 가장 많이 사용되는 그룹키를 이용한다. 그룹키가 노출되었을 경우 보안이 깨어지지만 2.2절에서 설명한 SPINs를 이용하여 암호화와 인증된 브로드캐스팅을 이용하여 그룹키를 안전하게 네트워크의 멤버에게 전송함으로써 멤버십에 대한 보안을 제공할 수 있다. 또한 앞서 언급한 URA는 cooperator가 가지고 있는 것으로 가정한다.

센서 액터 네트워크는 센서 노드와 액터 노드로 구성된다. 액터 노드는 센서 노드보다 큰 자원과 계산 능력, 에너지를 가지고 더 넓은 영역의 통신 범위를 가진다[8]. 제안하는 방법론은 이 센서 액터 네트워크에서 동작하고 액터는 cooperator가 되는 것으로 가정한다. 액터 노드는 자신에게 속한 센서 노드들에게 같은 그룹에 속한 노드들에 대한 정보(멤버십 리스트)와 암호화된 그룹키를 주기적으로 전송한다. 멤버십 리스트를 전송받은 각 센서 노드는 이 정보를 이용해 T-RBAC(Task-Role Based Access Control) 모듈을 적용한다. T-RBAC은 향상된 RBAC의 형태로 RBAC의 특징을 그대로 수용하지만 더 넓은 환경에서 사용가능한 접근제어 메커니즘이다[9].

그림 1은 센서 노드에서의 T-RBAC의 구성도를 보이고 있다. 각 센서 노드가 가지고 있는 자원과 그 자원을 구동하는 타스크가 있고 각 사용자가 할당받은 역할(Role)에 각 타스크에 대한 접근 권한을 할당한다. 각 역할은 멤버십 리스트에 저장되어 있고 역할에 따른 타스크

접근 권한 정보는 각 센서노드가 가지고 있다.

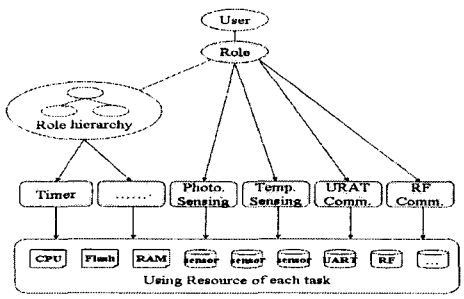

그림 1 T-RBAC 구조

그림 2는 제안하는 방법론의 전체 구조를 보이고 있다.

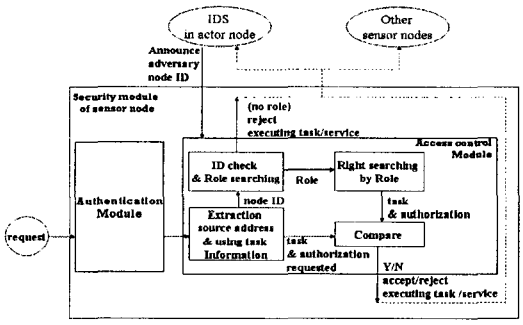

그림 2 제안 방법론의 시스템 전체 구조

타스크 수행에 대한 요청이 발생하면 보안 프로토콜인 SPINs을 통해 데이터 암호화가 이루어지고 안전한 브로드캐스팅으로 요청 메시지가 전송된다. 요청 메시지는 네트워크를 통한 인증 과정을 거친 후 요청을 받는 센서 노드에게로 전달된다. 메시지를 받은 센서 노드는 전달된 요청 메시지로부터 일련의 과정을 통해서 필요한 정보만을 추출한다.

추출된 정보는 요청을 발생한 노드의 ID, 요청한 타스크 정보와 요청 권한에 대한 내용이다. 추출된 정보에서 노드 ID를 'N1'이라하고 실행하고자 하는 타스크를 'T1', 요청 권한을 'A1'라 하자. 먼저 노드 ID 'N1'으로 'Role'을 검색한다. 만약 'N1'이 멤버십 리스트에 존재하지 않는 ID이거나 적절한 'Role' 정보가 없을 경우 T-RBAC 모듈은 이 요청에 대해 거부한다. 이 외의 경우 'Role'에 따른 타스크 실행 권한과 요청 메시지에 포함되어 있던 실행 요청 타스크와 그에 대한 권한 'T1'과 'A1'이 일치하는지를 검사한다. 이 결과가 일치하면 타스크를 실행하고, 일치하지 않으면 요청에 대해 거부한다.

또한 요청에 대한 거부를 할 때에는 'N1'이 허가되지 않은 동작을 수행하려고 한다는 것을 액터 노드와 다른 노드들에게 알려주게 된다. 이에 따라 액터 노드는 이 사실을 반영하여 미리 정해진 규칙에 따라 다음 멤버십 리스트 작성시 적용한다. 또한, 다른 노드들은 액터로부터 새로운 멤버십 리스트와 그룹키를 받을 때까지 전달받은 정보를 통해 'N1'이 허가받지 않은 동작을 시도했다는 사실을 알고 있으며, 'N1'로부터의 요청을 임시적으로 거부하게 된다. 이러한 방법으로 하나의 노드가 침해되었을 경우 침해의 확산을 막을 수 있다.

3.2 설계 및 구현

하나의 네트워크 내에는 여러 개의 액터 노드가 존재할 수 있다. 본 논문에서는 하나의 액터 노드가 관할하는 범위의 네트워크만을 생각한다.

액터 노드는 주기적으로 센서 노드들에게 멤버십리스트와 같은 네트워크의 멤버임을 증명하는 그룹키를 전송한다. 그룹키는 액터 노드가 랜덤하게 생성하며 멤버십리스트는 표 1과 같은 형태로 구성되어 있다.

표 1 멤버십리스트 내용

Node ID(pid)	Role ID(rid)
0x0001	0x01
0x0002	0x02
0x0003	0x01
0x0004	0x02
0x0005	0x03
0x0006	0x00
0x0007	0x03
0x0008	0x03
0x0009	0x02
0x000A	0x01
.....	.....

표 1에서 Node ID는 2바이트 16진수로, Role ID는 1바이트 16진수로 표현하였다. Node ID는 2^{16}개, Role ID는 2^{8}개의 표현이 가능하여 Role의 확장도 용이하다. 또한, 각각의 노드는 Role

ID를 가지며, 본 논문에서는 4가지 레벨의 Role ID(0x00, 0x01, 0x02, 0x03)를 정의한다.

한 노드가 타스크 수행을 요청할 때에는 타스크 정보와 권한 정보를 함께 전송하여야 하는데 이 정보는 표 2와 표3과 같이 정의한다.

표 2 타스크 정보

Task	Used Resource	tid
Timer	CPU Clock	0
Computation	CPU	1
	Memory	2
Store data	Flash Memroy	3
Photo Sensing	Photo sensor	4
Temp. Sensing	Temp. sensor	5
URAT Comm.	UART	6
RF Comm.	RF	7
Output	LED	7

표 3 권한정보

s	r	w	x	aid
1	0	0	0	8
0	0	0	0	0
0	0	0	1	1
0	0	1	0	2
0	0	1	1	3
0	1	0	0	4
0	1	0	1	5
0	1	1	0	6
0	1	1	1	7

표 2의 타스크와 자원은 크로스보우사의 Mica2와 MTS310을 기준으로 작성한 것이다. 각 타스크는 센서 노드의 자원을 사용하며 타스크 ID를 갖는다. 또, 표 3의 권한 정보는 리눅스 사용자의 권한 설정과 유사하다. 그러나 중요한 정보는 쉽게 노출되어서는 안 되므로 's'와 같은 super 권한을 따로 두어 이 권한을 소유할 수 있는 노드, Role을 제한한다. 표 2와 표 3의 tid와 aid는 16진수 값이며, tid는 상위 4비트, aid는 하위 4비트의 값으로 표시한다.

표 4 센서 노드의 접근제어 정보

Access control info. on one of nodes
0x0008, ……,
0x0100, 0x0115, 0x0186, ……,
0x0256, 0x0276, ……, 0x0367, ……

표 4는 하나의 센서 노드가 가지고 있는 접근제어 정보로 하나의 정보는 2바이트로 상위 8비트는 역할 정보를, 다음 4비트는 타스크 정보를, 마지막 4비트는 권한 정보를 나타낸다.

위에서 설명한 내용을 기반으로 예를 들어본다. Node ID 0x0001인 노드가 빛 감지(tid : 4) 수행(aid : 1)을 요청하기 위해서는 <0x0001, 0x41>의 쌍으로 메시지를 전송한다. 이 메시지를 받은 노드는 패킷에서 이 정보를 추출해내고 표 4에서 보인 접근제어 정보를 토대로 올바른 요청인지 판단한 후 요청을 수락할 것인지, 거부할 것인지를 결정한다.

Ⅳ. 보안 분석

3장에서 제안한 방법론이 도청에 따른 그룹키 노출, 몇 가지 DoS 공격에 대응하는 방법을 설명한다.

4.1 도청 - 그룹키 노출

외부 노드가 네트워크 패킷의 도청으로 'nid'를 획득했을 경우로, 이후 침입 노드의 ID 정보로 역할 테이블을 검색하여 역할을 할당받은 유효한 ID인지 검사한다. 침입 노드는 역할을 할당받지 못하였으므로 요청은 거부된다. 또는 우연의 일치로 적절한 'uid'를 참조하여 전송하였을 때 'uid'에 알맞은 자원에 대한 권한을 요청하는 것은 어려우므로 접근에 제한된다.

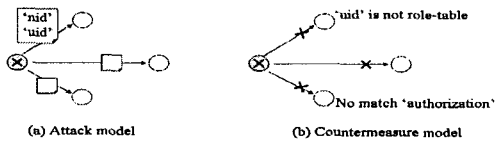

그림 3 도청에 따른 그룹키 노출의 모델과 대응 모델

4.2 DoS 공격 - Misdirection

네트워크에서 전송되는 패킷을 공격 노드가 정상적인 라우팅 경로가 아닌 다른 노드로 포워딩하여 데이터 전송을 방해하는 공격이다. 이 공격은 같은 공격 노드로 전송하여 네트워크의 데이터를 외부로 유출시킬 수도 있고, 특정 노드로 네트워크 트래픽을 집중시켜 특정 노드와 그 주변의 노드를 마비시켜 통신을 마비시킬 수도 있다. 그림 15의 (a)는 공격 모델을, (b)는 대응 모델을 보여준다. 각 노드는 공격 노드로부터의 패킷을 수신하지 않고 네트워크 라우팅 재설정시 이 공격노드를 제외시켜 방어할 수 있다.

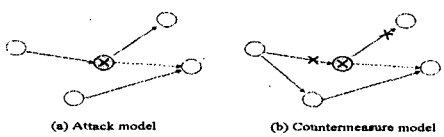

그림 4 Misdirection 공격 모델과 대응 모델

4.3 DoS 공격 - Flooding

연결 지향 방식의 통신에서 주로 발생하는 공격으로 'SYN packet'과 같은 패킷을 계속 전송하여 특정 노드를 마비시키는 공격방식으로 센서 네트워크의 경우 거의 모든 노드가 라우팅에 참가하므로 하나의 노드가 마비되면 전체 네트워크의 통신장애가 발생하게 된다. 그림 5의 (a)는 flooding 공격 모델, (b)는 대응 모델을 나타낸다. 공격 노드인 탐지한 후 이 노드로부터 계속해서 전송되는 패킷에 대해 수신 하지 않음과 동시에 응답 또한 하지 않음으로써 노드를 보호한다.

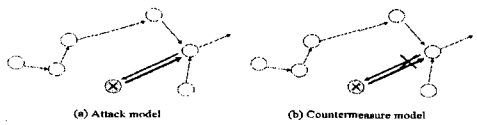

그림 5 Flooding 공격 모델과 대응 모델

V. 관련연구

TinyOS의 TinySec은 deploy 시점에서 지정된 group key를 이용해서 접근제어 제공한다. 또한 IV와 counter를 이용하여 기밀성과 무결성을 제공한다[10]. 그러나 도청을 통해 group key를 획득한 침입 노드 또는 침해 노드가 메시지 가로채기-라우팅, 잘못된 메시지 전송, DoS 공격 등으로 그룹 통신에 방해를 하게 되면 네트워크의 가용성이 떨어진다. 이러한 문제를 해결하기 위해 노드 자체의 보안도 중요하다. 오동작을 일으키고 있는 노드에 대해서 멤버 노드들이 인지를 하고 이 노드로부터의 접근을 제어함으로써 침해의 확산을 막아 노드 및 네트워크 전체의 가용성을 높일 수 있다.

표 5 TinySec과 제안 방법론 비교

요소 / 대상	TinySec	제안된 방법론
방식	인증, 암호화	인증, 암호화 그리고 RBAC을 통한 접근 제어
유연성	-	노드에 대한 역할 또는 역할의 자원 접근제어만 수정
확장성	키 재분배	멤버십리스트에 1개의 엔트리 추가 (동적 대응 가능)
공격 방어	기밀성, 무결성 보장	key 노출, DoS공격(Network/Transport layer) 방어 추가

표 6은 TinySec과 제안된 방법론의 보안 방식과 유연성, 확장성, 공격 방어 능력에 대해 비교해놓은 표이다.

VI. 결론

기존의 센서 네트워크 보안은 주로 기밀성과 무결성을 보장하고 그룹키 또는 키 사전분배 등을 통한 인증 방법에 대해 초점이 맞춰져 왔다. 그러나 센서 네트워크의 특성상 하나의 노드가 침해되면 브로드캐스트를 통해 침해가 확산된다. 이를 막기 위해서는 센서 노드의 자체적인 보안 방안이 필요하며 본 논문에서는 T-RBAC 메커니즘을 활용한 노드 접근 제어 방법을 제안했다. 제안 방법론은 노드 보안을 통해 침해 전파를 줄여, 침해 시에도 사용가능한 노드의 수를 증가시킴으로써 네트워크 전체의 가용성 증대시킬 수 있다.

Acknowledgement

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성지원사업의 연구결과로 수행되었음

[참고문헌]

[1] 나재훈, 채기준, 정교일."센서 네트워크 보안 연구 동향", 한국전자통신연구원 전자통신동향분석, 2005.02.

[2] L. Eschenauer and V. D. Gligor. "A key-management scheme for distributed sensor networks". In Proc. of the 9th ACM Conf. on Computer and Communications Security, pp. 41 - 47, November 2002.

[3] H. Chan 외. "Random key predistribution schemes for sensor networks". In IEEE Symposium on Research in Security and Privacy, 2003.

[4] Donggang Liu, Peng Ning. "Establishing Pairwise Keys in Distributed Sensor Networks". In Proc. of the 10th ACM Conf. on Computer and Communications Security, pp. 52 - 61, 2003.

[5] Jong Sou Park, Mohammed Golam Sadi,

Dong Seong Kim, "Randomized Grid Based Scheme for Wireless Sensor Network", 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks

[6] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. "SPINS: Security Protocols for Sensor Networks", Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001, July 2001

[7] Sye Loong Keoh, Emil Lupu, An Efficient Access Control Model for Mobile Ad-Hoc Com-munities, SPC 2005, 210-224

[8] Ian F. Akyildiz and Ismail H. Kasimoglu, "Wireless sensor and actor networks: research challenges", Ad Hoc Networks, Volume 2, Issue 4, October 2004, Pages 351-367

[9] Sejong Oh, Seog Park , "Task-role-based access control model", Information Systems Volume 28 , Issue 6, September 2003, Pages: 533 - 562

[10] Chris Karlof, Naveen Sastry, David Wagner, "TinySec : User Manual", (www.tinyos.net)