무선 센서 네트워크 상에서 신뢰기반 Randomized Path-Hash노드 인증 프로토콜†

김진환*, 박선호**, 정성민**, 엄정호**, 정태명*
*성균관대학교 정보통신공학부
**성균관대학교 컴퓨터공학과
e-mail : {jhkim, shpark, smjung, jheom}@imtl.skku.ac.kr
tmchung@ece.skku.ac.kr

A Randomized Path-Hash Node Authentication Protocol based on Trust Relationship in Wireless Sensor Networks

Jinhwan Kim*, Seonho Park**, Sungmin Jung**, Jungho Eom** and Taimyoung Chung*
*School of Information and Communication Engineering, Sungkyunkwan University
**Dept. of Computer Engineering, Sungkyunkwan University

요 약

본 논문은 무선 센서 네트워크 라우팅 프로토콜에서 일어날 수 있는 보안 위협 요소들에 대해 알아보고 상호인증에 관한 문제를 해결할 수 있는 Randomized Path-Hash 노드 인증 프로토콜(RPHAP)을 제안한다. 이 프로토콜은 노드 간 상호인증을 제공하며 센서 추적에 대한 안전성까지 제공한다. 또한 간단한 연산 능력의 Hash 를 이용하기 때문에 전력 소모에 대한 오버헤드가 적어 모든 센서 네트워크의 프로토콜에서 활용이 가능한 장점을 갖는다.

1. 서론

센서 네트워크는 실시간으로 센서가 위치한 곳에 대한 정보를 수집하며 질의의 목적을 수행할 수 있는 무선 네트워크 환경이다. 센서 네트워크는 여러 종류의 환경에 적용 시킬 수 있으며 사용자가 원하는 정보에 대해서도 센서가 스스로 파악하여 정보를 제공해 주기 때문에 편리함을 제공해줄 수 있다[1]. 센서 네트워크 환경을 구축할 때는 보안 요소를 고려해야 한다. 센서들은 여러 곳에 설치되어 중요한 정보들을 수집하기 때문에 보안의 문제가 생긴다면 네트워크 전체에 혼란과 인간에게 피해를 입히는 문제를 발생시킬 수 있다[2].

이 논문에서는 네트워크 계층에서의 기존의 센서 라우팅 프로토콜들이 제공하지 않는 인증 기능 및 라우팅 프로토콜과 호환성을 제공하는 신뢰기반 Randomized Path-Hash 노드 인증 프로토콜(RPHAP)를 제안한다. 제안하는 프로토콜은 센서가 가지는 연산능력과 에너지의 제약을 고려하여 Hash 를 이용하여 연산을 최소화 하였다.

본 논문은 2 장에서 센서 네트워크 상에서의 위협 요소와 라우팅 방법, 라우팅 공격방법 등의 기반 요소에 대해 기술하고 3 장에서는 본 논문에서 제안하는 보안 프로토콜인 RPHAP(Randomized Path-Hash node Authentication Protocol)에 대해 기술한다. 마지막으로 4 장에서는 RPHAP 에 대한 결론 및 진행되어야 할 연구 계획을 제시한다.

2. 관련 연구

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성・지원사업의 연구결과로 수행되었음.

2.1 라우팅 프로토콜

센서 라우팅은 센서들이 하는 역할에 따라 평면 라우팅 프로토콜과 계층적 라우팅 프로토콜로 나눌 수 있다[3]. 평면 라우팅 프로토콜은 전체의 네트워크들을 하나의 영역으로 간주하며 각 센서들은 동등한 역할을 하여 통신한다. 종류로는 Direct-diffusion[5], SPIN (Sensor Protocol for Information in Negotiation)[7],[8] 등이 있다. 계층적 라우팅 프로토콜은 클러스터링을 기반으로 다수의 영역을 분할하여 대표(Cluster Header)를 선정하고 역할을 부여하여 라우팅을 수행한다. 종류로는 LEACH (Low Energy Adaptive Clustering Hierarchy)[9], TEEN(Threshold sensitive Energy Efficient sensor Networks)[10][11] 등이 있다.

2.2 정보의 위협 요소

센서들은 라우팅 프로토콜에 따라 여러 가지 방법을 이용하여 정보를 교환하며, Source 센서가 Sink 에게 질의에 대한 응답을 전달하는 공통적인 특징을 가진다. 질의에 대한 응답을 전달할 때 Flooding 을 이용하는데 Flooding 은 보안 기능을 제공해주지 않아 여러 위협에 노출되기 쉽다. 이러한 취약점은 공격자의 적은 노력으로도 원하는 정보를 얻을 수 있는 원인을 제공한다[2]. 센서 네트워크에서의 정보의 위협은 크게 네 가지 정도로 나누어볼 수 있다.

1) 정보 위협 요소

· 방해(Interruption): 공격자가 많은 데이터를 보내 배터리를 소모시켜 센서를 동작하지 못하게 하거나, 많은 양의 데이터를 보내어 센서들이 다른 곳으로부터 오는 정보에 대해 반응하지 못하도록 만드는 형태의 공격이다. 대표적으로 DoS(Denial of Service) 공격이 있다.

· 도청(Interception): 공격자가 센서끼리 주고 받는 정보를 중간에서 엿듣는 행위이다. 센서들은 무선을 기반으로 통신하여 공격자들로부터 불법적인 접근을 막을 수 없으며 도청으로 얻은 정보를 프라이버시 등의 문제에 악용 할 수 있다. 대표적으로 스푸핑(Spoofing) 공격이 있다.

· 불법수정(Modification): 비인증자들이 불법적인 접근을 하여 도청을 한 후 정보들을 수정하여 보내면 불법수정이 이루어진다.

· 위조(Fabrication): 공격자는 공격자의 센서를 이용하여 특정 센서들에게 질의를 보내고 고유 정보를 획득 할 수 있다. 공격자는 이 정보를 이용하여 특정 센서로 위장이 가능하다.

센서 라우팅 프로토콜에서 일어날 수 있는 공격 방법은 다섯 가지로 나누어볼 수 있다.

2) 라우팅 공격 방법[6]

· Sinkholes: Sink 로 모이는 데이터들이 공격자가 있는 곳을 지나치게 하는 공격이다.

· Sybil: 노드에게 여러 식별자를 인식시켜 노드가 여러 개 있는 것처럼 인식하도록 만드는 공격이다.

· HELLO floods: 공격자가 HELLO 패킷을 브로드캐스팅(Broadcasting)하여 패킷을 유도하는 공격이다.

· Wormholes: 존재하지 않는 노드나 멀리 떨어져 있는 노드가 가까이 있는 것처럼 속이는 공격이다.

· Selective forwarding: 특정 메시지에 대해 전달하지 않거나 수정하는 공격이다.

위의 위협 요소들은 불법적인 센서들에 의한 접근으로 이루어지는 공격이므로 이러한 공격을 예방하기 위해서는 센서 노드에 대한 인증 및 데이터 기밀성을 제공해주는 보안 프로토콜이 필요하다.

2.3 센서 네트워크 보안 프로토콜

센서 네트워크상에서 보안을 제공하는 프로토콜에는 SPINS(Security Protocol for Sensor Network)와 LEAP(Localized Encryption and Authentication Protocol) 등이 있다. SPINS 는 데이터의 기밀성과 양단간 데이터 인증, 무결성 등을 제공하는 SNEP(Secure Network Encryption Protocol)와 대칭 키 시간 지연 메커니즘을 기반한 인증 및 노드의 브로드캐스팅을 지원하는 μTELSA 로 구성된다. 또한 키 관리 프로토콜인 LEAP 은 하나의 키를 이용한 매커니즘만으로는 센서 네트워크에서 안전성 보장이 힘들어 4 개의 암호 키와 키 설정 프로토콜을 가진다[2].

3. Randomized Path-Hash node Authentication Protocol

본 장에서는 센서 노드와 Sink 간의 통신시에 상호 인증이 가능한 두 프로토콜 Simple-Hash 노드 인증 프로토콜과 Simple-Hash 노드 인증 프로토콜을 개선한 RPHAP 에 대해 기술한다.

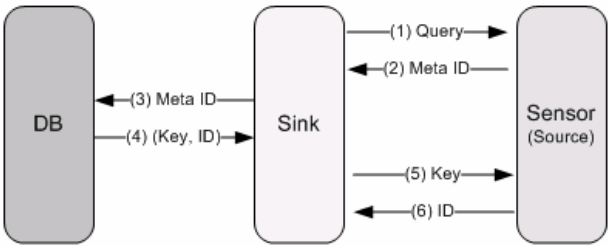
센서 네트워크상에서는 무선을 기반으로 통신하여 공격자가 불법수정이나 위조하기 쉬워 상호 인증이 가능한 방법을 사용한다. RPHAP 의 기본 아이디어는 라디오 주파수를 이용하여 인식하는 RFID (Radio-Frequency Identity) Randomized Hash-Lock 알고리즘[4]을 기반으로 한다. RFID 는 센서와 마찬가지로 작은 크기와 적은 배터리를 사용하여 임무를 수행하기 때문에 연산 능력이나 자원 면에서 기존의 접근 제어 메커니즘을 그대로 적용하기 힘들며 RFID 와 센서는 차별된 특징과 기술을 가지고 있기 때문에 이 알고리즘을 센서에 그대로 적용시킬 수가 없다. 그래서 이를 개량하여 기존 RFID 에서 Lock 을 이용하여 인증을 제공하던 방법을 단 방향(One-way) Hash 함수를 기반으로 경로(Path)에 적용시켜 데이터가 이동하는 경로에 대한 인증이 가능하도록 설계한다.

3. 1 Simple-Hash 노드 인증 프로토콜

이 장에서는 Source 센서와 Destination 센서간의 인증만을 제공하는 프로토콜인 Simple-Hash 노드 인증 프로토콜을 소개한다. Source 센서와 Destination 센서는 주소 기반 방식의 통신이 아닌 데이터 기반의 통

신이므로 RFID 와 같은 1:1 통신을 사용하지 않는다. 그러므로 Multi-hop 라우팅의 통신이 이루어진다는 특징을 갖고 있어 라우팅 되는 중간 지점에 대한 인증을 제공하지 않는다.

센서 네트워크상에서 Hash 를 이용한 인증을 제공하기 위해서는 다음과 같은 전제가 필요하다. 첫 번째 이 인증 프로토콜은 Hash 를 이용하기 때문에 센서들은 Hash 연산을 수행할 수 있어야 하며, 두 번째 미리 임의의 키를 가지고 Hash 된 값 metaID=H(key)을 데이터베이스는 미리 저장해야 한다. 세 번째는 센서들은 Global ID 를 가질 수 없기 때문에 지상에 설치되기 전에 미리 고유한 ID 을 저장시켜야 한다. 네 번째는 데이터베이스와 Sink 사이에는 안전성을 보장하지 않기 때문에 보안채널이라 가정한다. 마지막으로 다섯 번째는 경로 설정이 완료된 후 상호간 데이터를 원활하게 주고받을 수 있는 환경이 되었을 때 사용할 수 있다. 이유는 센서들은 대부분 Flooding 방식으로 데이터를 교환하기 때문에 Sink 가 Meta ID 를 받았다 할지라도 경로가 고정되지 않으면 Meta ID 를 보낸 센서를 찾을 수 없기 때문이다.



(그림 1) Simple-Hash 노드 인증 프로토콜

이 프로토콜은 DB 와 Sink 그리고 센서들에 대한 별도의 라우팅 프로토콜을 가지고 통신을 하며 인증 프로토콜을 추가시켜 동작하면 동작 과정은 다음과 같다.

(1) Sink 가 센서에게 쿼리를 보내면 센서들의 고유한 Meta ID 를 Sink 에게 보낸다.
(2) Meta ID 를 받은 Sink 는 별도의 연산 없이 데이터베이스에게 전달한다.
(3) 데이터베이스는 Meta ID 를 이용하여 검색해 해당 ID 와 Key 값을 찾아낸다.
(4) Key 값과 해당 ID 를 다시 Sink 에게 보내면 Sink 는 ID 는 비교대상으로 가지고 있는다.
(5) Destination 센서에게는 Key 를 보낸다.
(6) Key 를 가지고 센서에서는 H(key) 연산을 하여 허가된 센서임을 Sink 에 전달한다.
(7) Sink 는 센서가 불법적인 접근인지 판별한다.

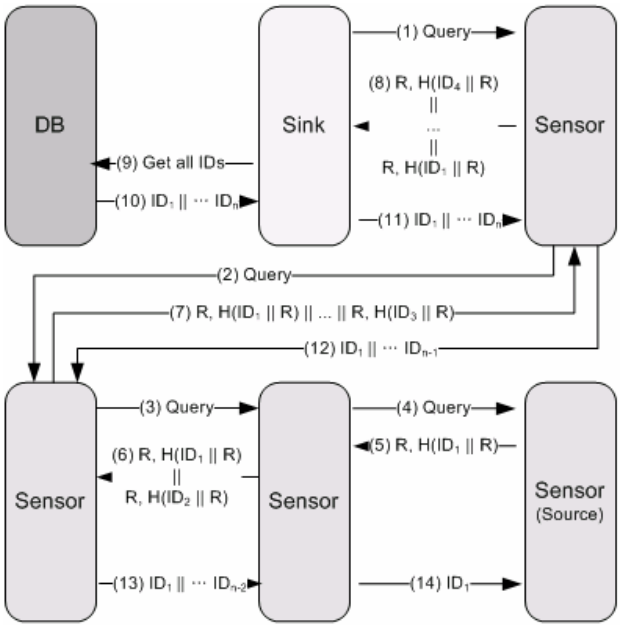
이 Simple-Hash 노드 인증 프로토콜의 장점은 Hash 특성상 역 변환이 어렵기 때문에 불법적인 접근자가 Meta ID 만 가지고 Key 값을 유추해 낼 수 없고 데이터베이스에서 키 관리만 하면 되므로 간단하게 구현, 사용이 가능하다. 하지만 단점으로는 Source 센서와 Destination 센서 간 인증만을 제공하기 때문에 전체 경로에 대한 인증을 제공하지 않는다. 또한 스푸핑 공격자는 Destination 센서에게 Source 센서로 가장하여 Meta ID 쿼리를 보내어 센서 자체를 추적할 수 있다.

위의 문제점을 개선하여 전체 경로에 대한 인증을 제공하고, 난수를 이용한 Hash 를 이용해 보안을 강화시킬 수 있는 Randomized Path-Hash 노드 인증 프로토콜을 제안한다.

3. 2 Randomized Path-Hash 노드 인증 프로토콜

이 장에서는 Simple-Hash 프로토콜의 단점을 개선해 확장한 새로운 프로토콜인 Randomized Path-Hash 노드 인증 프로토콜(RPHAP)을 소개한다. Source 센서와 Destination 센서간의 인증만 제공하는 Simple-Hash 에서 발견되었던 취약한 공격들은 노드 경로에 대해 상호간 신뢰를 제공하여 취약점에 대응할 수 있다.

RPHAP 를 사용하려면 몇 가지 전제 사항이 필요하다. 기존의 Simple-Hash 알고리즘이 가지는 전제조건을 포함한 이외의 전제는 다음과 같다. 첫 번째는 각 센서들은 PRF(Pseudo Random Function)의 기능을 가지고 있어야 한다. 두 번째는 지나온 노드 모두를 기록하여 인증하기 때문에 센서들 간의 Multi-hop 라우팅이 이루어지고 있는 상태에서 사용하여야 효과적인 이용이 가능하다.



(그림 2) Randomized Path-Hash 노드 인증 프토토콜

Randomized Path-Hash 노드 인증 프로토콜의 동작 과정은 다음과 같다.

(1)~(4) Sink 는 센서에게 쿼리를 전송하고 경로가 설정되어 있으므로 소스 노드까지 문제없이 찾아 갈 수 있다.
(5) 쿼리를 받은 Source 센서는 의사 난수 생성기를 이용하여 랜덤 값 R 을 생성하고 R 과 센서에 대한 ID 를 연접한 Hash 값을 H(ID||R) 값과 함께 이전 센서에게 전달한다.

(6)~(8) 이와 같은 방법으로 경로에서 생성된 R, $H(ID_1||R) \| \ldots \| R$, $H(ID_{n+1} \| R)$의 값을 Sink가 전달 받는다.
(9) 이 전달받은 값들을 다시 데이터베이스에 전송시켜 데이터베이스는 보낸 값과 일치하는 ID_n 을 찾는다.
(10) 연접되어있는 $ID_1||\ldots \| ID_n$ 값을 보낸다.
(11)~(14) 각 센서들은 이에 해당하는 값과 자신의 ID 값이 서로 일치하면 다음 단계의 센서에게 전달하며, 전달 시에는 자신이 찾은 ID 값을 제거하여 전달한다. 마지막 Source 센서에게 전달되어 ID 값이 일치하면 안전한 센서라고 생각할 수 있다.

이 Randomized Path-Hash 노드 인증 프로토콜은 Simple-Hash 와 공통적인 장점을 가지며 데이터 전달 경로에 대해서 모두 인증을 제공하기 때문에 높은 안전성을 제공한다. 하지만 DoS 공격을 이용해 센서에 대한 반응을 유도시켜 에너지를 소비시키는 공격과 경로 설정 중 일어날 수 있는 공격 등에 대해 보안을 제공하지 못한다는 단점이 있다.

3. 3 Simple-Hash 와 Randomized Path-Hash 의 비교

이 논문에서 제안한 두 프로토콜을 비교해보면 아래의 <표 1>와 같다.

<표 1> Simple-Hash 와 Randomized Path-Hash 의 비교

프로토콜	Simple-Hash	Randomized Path-Hash
키 관리	O	X
노드 인증	O	O
메시지 인증	X	X
패스 인증	X	O
에너지 효율	높음	Simple-Hash 에 비해 낮지만 타 프로토콜에 비해 높은편
위협 공격	DoS, Replay, Spoofing Attack	DoS

RPHAP 는 Simple-Hash 에서 발생할 수 있는 Meta ID 의 추적 공격에 따른 취약점을 보완할 수 있으며 지나가는 모든 센서들에 대해서 상호 인증을 제공하기 때문에 높은 안전성을 보장한다. 또한 Hash 의 간단함을 이용하기 때문에 인증 기능을 제공하여도 네트워크 에너지 사용에 대한 오버헤드가 적다.

4. 결론 및 향후 계획

본 논문에서 제안한 Randomized Path-Hash 노드 인증 프로토콜은 센서들에 대한 추적이 불가능하며 상호인증이 가능한 프로토콜이다. 인증 등은 이미 센서 네트워크에서 유용하게 쓰고 있는 SPINS, LEAP 등에서 MAC 등을 이용해 제공하고 있지만 이 인증 프로토콜은 Hash 를 이용해 간단하게 구현할 수 있으며 에너지 보존 효과와 다른 프로토콜과의 사용에 있어서 호환성도 유지할 수 있어 여러 네트워크에서 활용이 가능하다.

센서 네트워크 상에서 인증만으로는 모든 공격에 대응할 수 없다. 특히 DoS 공격 방법 등에 Hash 만을 이용하여 안전성을 보장 받기는 어렵다. 또한 이 프로토콜에서 단점으로 가지고 있는 경로 설정 전에 일어날 수 있는 공격에 대한 오버헤드는 해결해야 하는 과제로 남으므로 이 논문에서 제시된 노드 인증 프로토콜을 이용하여 혼합(Hybrid) 한 방식으로 프로토콜을 설계하여 보안성을 높이는 방법을 연구해야 한다.

참고문헌

[1] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam,and E. Cayirci, “A Survey on Sensor Networks”, Comm. IEEE. Vol. 40, 2002.
[2] C. Karlof, D. Wanger, “Secure Routing in Wireless Sensor Networks: Attackers and Countermeasures”, First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
[3] Al-Karaki, J.N. and Kamal, A.E., “Routing Techniques In Wireless Sensor Networks: A Survey”, IEEE Wireless Communications, December2004
[4] S. Weis, S. Sarma, R. Rivest, and D. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identication Systems”, Proc. of the 1st Security in Pervasive Computing, LNCS, 2004.
[5] C. Intanagonwiwat, R. Govindan, and D. Estrin, Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks”, MobiCOM 2000, 2000.
[6] 김영한, 한영주, 정태명, “센서 네트워크에서의 공격에 대한 라우팅 프로토콜의 안전성 평가에 관한 연구”, 정보처리학회, May,2005.
[7] W. R. Heinzelman, “Adaptive Protocols for Information Dissemination in Wireless Sensor Networks”, ACM/IEEE, 1999.
[8] J. Kulik, W. R. Heinzelman, H. Balakrishnan, “Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks”, Wireless Networks, 2002.
[9] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”, 33rd Hawaii Int'l. Conf. Sys, Sci., Jan. 2000.
[10] A. Manjeshwar and D. P. Agrawal, “TEEN: a routing protocol for enhanced efficiency in wireless sensor networks”, ICPDPS, 2001.
[11] A. Manjeshwar and D. Agrawal, “APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive information Retrieval in Wireless Sensor Networks”, IPDPS 2002 Workshops, 2002.