제 3의 노드를 이용한 다중 홉 환경의 센서 노드를 위한 안전한 비밀값 공유 기법

조응준*, 홍충선*
*경희대학교 컴퓨터공학과
e-mail : ejcho@networking.khu.ac.kr, cshong@khu.ac.kr

A Secret Sharing Mechanism for Multi-Hop Sensor Nodes Environment Using the Third Node

Eung Jun Cho*, Choong Seon Hong*
*Dept of Computer Engineering, Kyung Hee University

요 약

무선 통신에서는 무선 통신의 브로드캐스트한 특성으로 데이터의 기밀성 유지를 위한 암호화가 매우 중요하다. 특히 무선 센서 네트워크(WSN - Wireless Sensor Network)의 경우 일반적인 PC와는 다르게 다양한 환경에 위치할 수 있어 공격자에게 더 쉽게 노출 될 수 있는 문제점을 가지고 있다. 이런 환경에서 미리 저장된 해쉬 함수나 비밀 값에 의존한 키 분배를 할 경우 저장된 값이 노출될 경우 심각한 문제를 초래하게 된다. 그리고 D-H 키 분배 알고리즘의 경우 키 값을 안전하게 도출을 할 수 있지만 키를 도출한 대상에 대한 인증의 부재와 멀티 홉 환경에서 중간자 공격에 취약한 문제점을 드러내고 있다. 본 논문에서는 이런 문제를 해결하기위해 기존 연구를 응용하여 멀티 홉 환경에서 무선 통신의 특성을 이용한 비밀값 공유와 제 3의 노드를 이용한 간단한 인증이 가능한 기법을 제안한다.

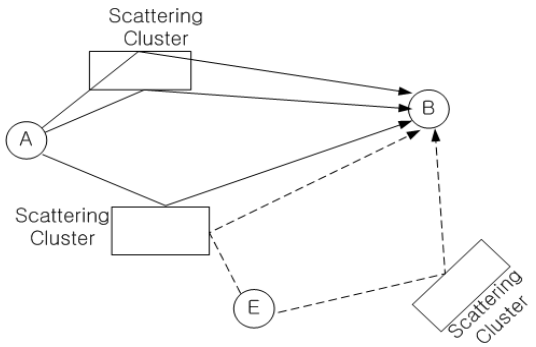
1. 서론

유선 통신에서는 데이터가 송수신되는 회선이나 컴퓨터에 직접 연결을 하거나 일반 허브를 통해 모든 포트로 데이터가 브로드 캐스팅되는 특별한 환경을 제외하면 중간에서 데이터를 가로채는 것은 매우 어렵다. 그러나 무선 통신에서는 무선 통신의 브로드캐스트한 특성으로 데이터가 타인에게 쉽게 노출 될 수 있다. 특히 멀티 홉 환경으로 구성된 무선 센서 네트워크(Wireless Sensor Network, WSN)의 경우 데이터가 중간 노드를 거쳐 전달되기 때문에 데이터의 기밀성 보장을 위해 암호화가 필수적이다. 그러나 Diffie-Hellman 키 교환 알고리즘[1]의 경우 중간 노드의 의한 공격과 인증에 취약점이 있으며 많은 수의 키 교환 메커니즘[2], [3]이 미리 공유된 해쉬 함수를 사용하거나 비밀값 풀을 이용하는 방식을 사용하지만 개방된 환경에 위치한 센서노드의 경우 물리적인 해킹에 의해 사전에 공유된 값이 유출 될 수 있기 때문에 적합하지 않다. 이를 해결하기 위해 본 논문에서는 사전에 공유된 값이 아닌 무선 통신의 특징을 이용하여 비밀값을 도출하고 도출 된 값을 이용하여 멀티 홉 환경의 무선 센서 네트워크 상의 무선 센서 노드 간 비밀값을 공유하는 방법을 제안한다.

본 연구는 지식경제부 및 한국산업평가관리원의 산업원천 기술개발사업의 일환으로 수행되었음. [과제관리번호 : 2009-S-014-01, 센싱기반 감성서비스 모바일 단말 기술개발] *Dr. CS Hong is corresponding author.

2. 관련 연구

[4]에서는 무선 통신의 지연 확산 특성을 이용하여 통신을 하는 장치의 지문(fingerprints)을 측정하는 방법을 제안하고 있다. 그림 1에서처럼 무선 신호는 물리적으로 브로드캐스팅되어 주변의 사물이나 벽에 부딪히며 많은 반사파를 만들게 된다.



(그림 1) 지역 확산의 예시

그러나 이 방법의 경우 장치가 이동을 할 경우 측정되는 지문 값이 변경되기 때문에 환경이나 통신을 하는 장치가 정적인 곳에서만 사용가능한 단점이 있다.

[5]에서는 두 장치간의 지역 확산 신호의 세기를 이용하여 비밀키를 도출하는 법을 제안하고 있다. 이 경우 [4]와는 다르게 장치가 이동을 하여도 한번 만들어진 비밀키는

계속 사용할 수 있는 장점이 있다. 그러나 이 방법의 경우 지연 확산 신호를 측정할 수 있는 단일 홉 환경의 장치에 한하여 적용이 가능하며 다중 홉 환경에는 적용이 불가능한 단점이 있다.

3. 제안 사항

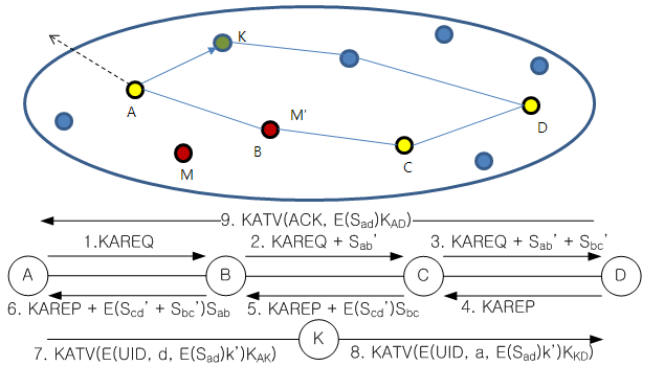
본 논문에서는 [5]의 내용을 바탕으로 하여 다중 홉 환경에서 사용가능한 비밀값 공유 기법을 제안한다. 이를 위해 다음과 같은 사항들을 가정한다.

- 모든 노드는 자신 이웃노드와 [5]의 내용에서 나온 비밀값을 측정 할 수 있다.
- 모든 노드는 비밀값을 해쉬하기 위한 해쉬 함수를 공유하고 있다.
- 노드들은 설치 시 적어도 두 개 이상의 대칭키를 다른 노드들과 공유하고 있다.

<표 1> 정의한 기호 및 그 설명

Symbols	Decryption
S_{ab}	Secret value between A and B
S_{ab}'	Hashed secret value between A and B
$E(m)S_{ab}$	Encrypted message m by key S_{ab}
K_{AB}	Symmetric key between A and B
K'	$S_{ab}'+S_{bc}'+S_{cd}'$
KAREQ	Key Agreement Request
KAREP	Key Agreement Reply
KATV	Key Activation

표 1에는 제안 사항에 필요한 기호들과 그 설명들이 나타나 있다. 그리고 그림 2에는 본 논문에서 제안한 메커니즘과 시나리오가 나타나 있다.



(그림 2) 제안하는 시나리오 및 메커니즘

그림 2는 노드 A가 노드 D로 안전하게 데이터를 전송하기 위해 비밀값을 공유하는 절차이다. 해당 절차는 3단계의 과정을 거치게 된다.

(1) 키교환 요청

키 교환을 위해 노드 A가 노드 D로 KAREQ(Key Agreement Request)를 보낸다. 이때 노드 A의 신호는 노드 D에 직접 전달되지 않기 때문에 그림 2에서처럼 노드 B와 노드 C를 거쳐 전달되게 된다. KAREQ 메시지를 수신한 노드 B는 자신과 이전 노드인 노드 A 사이의 비밀값 S_{ab}를 KAREQ 메시지에 추가한다. 이때 KAREQ 메시지에 S_{ab}값을 바로 추가할 경우 다른 주변 노드에게 노드 A와 노드 B의 비밀값이 유출될 수 있으므로 S_{ab}값을 해쉬하여 S_{ab}'로 변형하여 추가한다. 이와 같이 노드 C도 수신한 KAREQ 메시지에 자신과 노드 B 사이의 비밀값을 해쉬한 S_{bc}'를 추가하여 노드 D로 전달한다. 최종적으로 노드 D는 $S_{ab}'+S_{bc}'+S_{cd}'$ 값을 수신하게 된다.

(2) 키교환 응답 단계

노드 A로부터 KAREQ메시지와 $S_{ab}'+S_{bc}'+S_{cd}'$값을 수신한 노드 D는 노드 A에게 KAREP(Key Agreement Reply) 메시지를 사용하여 메시지 수신에 대한 확인을 보내준다. KAREP메시지는 KAREQ와 전달되는 과정이 유사하지만 그림 3에서와 같이 전달 경로의 이웃 노드에게 비밀값을 노출 시키지 않기 위해 구간별로 암호화 과정을 거친다. 즉 노드 C가 KAREQ 메시지를 받아 자신과 노드 D의 비밀값을 해쉬한 Scd'를 첨부할 때 자신이 KAREQ 메시지를 전달한 노드 B와 이미 공유하고 있는 비밀값은 Sbc로 암호화를 한다. 즉 KAREQ 메시지에는 $E(S_{cd}')S_{bc}$가 추가된다. 노드 B는 노드 C에서 받은 메시지에서 $E(S_{cd}')S_{bc}$를 복호화 하여 S_{cd}'와 S_{bc}'를 추가한 후 S_{ab}로 암호화 하여 노드 A에게 전달한다. 최종적으로 노드 A는 $S_{ab}'+S_{bc}'+S_{cd}'$ 값을 수신하게 된다.

(3) 목적지 노드 인증 및 키 활성화 단계

앞서 두 단계에 걸쳐 노드 A와 노드 D사이에 공유된 비밀값은 비밀값 공유를 위해 데이터를 전달하는 중간 노드들에게 노출이 된다. 즉, 그림 2에서처럼 노드 B가 공격자 노드일 경우 노드 B는 KAREQ 메시지를 노드 C로 전송 할 때 S_{ab}'를 알 수 있고 KAREP 메시지를 노드 A로 전송 할 때 S_{bc}' + S_{cd}'를 알 수 있기 때문에 두 메시지를 조합하여 $S_{ab}'+S_{bc}'+S_{cd}'$를 알아내는 것이 가능하다. 즉 앞선 두 과정을 통해 공유되는 비밀값은 경로 이웃 노드들로부터는 안전하지만 경로상에 공격자가 있을 경우 비밀값이 노출 될 수 있다. 이를 방지하고 KAREP 메시지가 노드 D로부터 온 것을 인증하기 위해 KATV(Key Activation) 메시지를 사용한다. KATV 메시지는 라우팅 경로를 따라 전달되지 않고 노드 A가 대칭키를 공유하고 있는 노드 (그림 2에서 노드 K)를 통해 전달이 된다. 이때 메시지에는 노드 A와 노드 D 사이에 이미 공유된 비밀값으로 암호화된 새로운 시드값인 S_{ad}와 목적지 노드의 주소, KAREQ 메시지의 UID 값이 포함되며 전체 메시지는 노드 A와 K사이의 대칭키로 암호화 된다. 이를 전달받은 노드 K는 자신과 노드 D 사이에 이미 비밀값이 공유되어 안전한 채널이 형성된 경우 해당 채널을 통해 노드 D로 KATV 메시지를 전달해준다. KATV 메시지를 수신한 노드 D는 기존 노드 A와 공유된 비밀값 $S_{ab}'+S_{bc}'+S_{cd}'$와 새롭게 받은 시드값인 S_{ad}를 조합하여 A와의 통신에 사용할 비밀키를 생성한다. 그리하여 노드 A에서 KATV 메시지를 보내며 방금 수신한 S_{ad} 값을 암호화 하여 노드 A로 전달해주며 KATV 메시지 수신을 확

인시켜 준다.

그러나 만약 노드 K가 D와 아직 안전한 채널을 확보하지 못한 경우 노드 K는 노드 A가 노드 D와 비밀값을 공유하는 방식으로 비밀값 공유를 위한 메커니즘을 수행한다. 이와 같이 재귀적으로 해당 과정을 거쳐 최종적으로 노드 D와 초기 대칭키를 공유한 노드를 발견하게 되면 노드 K를 거쳐 노드 A도 비밀값 공유를 하게 된다.

4. 평가

본 논문의 메커니즘을 이용할 경우 다중 홉 환경에서 두 단말사이의 비밀 값을 안전하게 공유할 수 있다. 특히 키 공유를 위한 메시지가 전달되는 경로상에 공격자가 존재하거나 미리 공유된 해쉬 함수가 유출되어도 비밀값이 노출되지 않는 큰 강점이 있다. 그러나 키 활성화를 위한 KATV 메시지 전송 시 가장 좋은 경우와 가장 나쁜 경우의 차이가 큰 점이 있다. 예를 들어 전체 노드의 수가 100개이고 모든 노드가 2개의 초기 대칭키를 공유한 경우에 그림 2에서처럼 노드 A가 노드 D와 초기 대칭키를 공유한 노드와 초기 대칭키를 공유할 확률은 100개중 노드 A와 노드 D를 제외한 98개의 노드 중에서 노드 D와 초기 대칭키를 공유한 노드 2개 중 하나를 선택할 확률이므로 2/98이 된다. 만약 두 홉에 걸쳐 노드 D와 초기 대칭키를 공유한 노드를 선택하게 될 확률은 처음 98개의 노드 중에서 노드 D와 초기 대칭키를 공유하지 않은 노드를 선택할 확률과 두 번째 선택에서 노드 D와 초기 대칭키를 공유한 노드를 선택할 확률의 곱인 96/98 x 2/97 로 나타낼 수 있다. 이를 일반화 하면 다음과 같다.

n: 전체 노드 수
h: 초기 대칭키를 공유하는 노드를 발견하는 횟수
k: 한 노드가 가지는 초기 대칭키 수

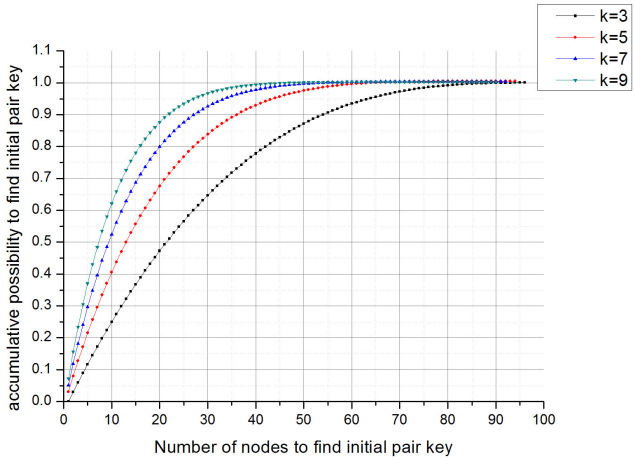
$$\sum_{h=1}^{n-2}(1-\frac{k}{n-2})(1-\frac{k}{n-3})\ldots(1-\frac{k}{n-h})(\frac{k}{n-(h+1)})=1$$

위의 식을 바탕으로 n = 100, k = 3~10일 때, 초기 대칭키를 공유하는 노드를 발견하는 횟수(h)의 증가에 따른 초기 대칭키를 공유한 노드를 발견할 확률은 그림 3과 같다. 그림3에서 확인 할 수 있듯이 한 노드가 가지는 초기 대칭키의 수가 증가할수록 확률적으로 비밀 값 공유가 더 일찍 되는 것을 확인할 수 있다.

그러나 이 과정을 통해 다른 노드들이 비밀값 공유를 통해 비밀키를 가질 수 있기 때문에 단순한 오버헤드와는 다르다고 할 수 있다. 즉 그림 2에서의 노드 A와 노드 D만이 아니라 해당 메커니즘에 재귀적으로 참여하는 노드들도 다른 노드와 비밀값을 공유하기 때문에 단순한 오버헤드가 아닌 비밀값 공유 메커니즘의 일부인 것이다.

5. 결론 및 향후 연구

본 논문에서 제안한 메커니즘을 이용하여 다중 홉 통신 환경에서 비밀값을 안전하게 공유할 수 있는 것을 확인하였다. 그리고 Diffie-Hellman 알고리즘의 취약점인 중간노드 공격을 방지하기위해 제3 노드를 통한 비밀값 보완 및 약신 인증 기법도 추가하였다. 그러나 비밀값 분배에 있어 초기 대칭키를 공유하는 노드들의 구성에 따라 비밀값 분배에 걸리는 시간의 차이가 많이 나는 문제점이 있으며 이를 해결하기 위해 노드 배치 시 효율적인 초기 대칭키 분배 알고리즘과 같은 추가적인 기술의 연구가 진행되어야 한다. 그리고 평가에 있어 네트워크 토폴로지나 라우팅 경로와 같은 실제적인 수치들이 반영되어 있지 않기 때문에 이를 반영하기위한 시뮬레이션이 필요하다.



(그림 3) n과 h가 고정일 때 k에 따른 노드 발견 확률

참고문헌

[1] E. Rescorla, RFC 2631 : Diffie-Hellman Key Agreement Method June 1999.

[2] S.A. Camtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. In Proceedings of 9th European Symposium On Research in Computer Security (ESORICS '04), 2004.

[3] CW Chiang, CC Lin, RI Chang , "A new scheme of key distribution using implicit security in Wireless Sensor Networks", Advanced Communication Technology (ICACT), 2010 The 12th International Conference on, Feb, 2010

[4] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication", Proceedings of the IEEE Int. Conf. on Comm., pp.4646-465, June, 2007

[5] Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt. "On Key Agreement in Wireless Sensor Networks based on Radio Transmission Properties", Proceedings of the 5th Annual Workshop on Secure Network Protocols (NPSec), IEEE Computer Society, pp37-42, October 2009.