센서 네트워크의 노드간 세션키 생성을 위한 개선된 프로토콜

김 종 은† · 조 경 산††

요 약

제한된 연산 및 통신 능력을 갖는 센서 노드에서는 전통적인 공개키 기반의 보안 기법들을 사용할 수 없으므로, 두 센서 노드 사이의 안전한 통신이 센서 네트워크의 중요한 연구 과제가 되었으며 두 센서 노드 사이의 안전한 직접 통신을 위한 다양한 세션키 설정 프로토콜들이 제안되었다.

본 연구에서는 기존의 대표적인 세션키 설정 프로토콜들을 세션키 설정 방법, 세션키의 유일성, 연결성, 통신 및 연산 과부하, 공격 취약성 등의 기준 측도에 의해 분석하고, 분석 결과를 토대로 안전하고 효율적인 프로토콜을 위한 기준안을 제시하였다.

또한, 제시된 기준안을 만족시키는 개선된 세션키 생성 프로토콜을 제안하고, 제안 프로토콜의 성능적 우수성을 상세한 분석을 통해 제시하였다.

키워드 : 센서 네트워크, 세션키, 보안, 연결성, 키 유일성

An Improved Protocol for Establishing A Session Key in Sensor Networks

JongEun Kim† · Kyungsan Cho††

ABSTRACT

Because the traditional public key-based cryptosystems are unsuitable for the sensor node with limited computational and communication capability, a secure communication between two neighbor sensor nodes becomes an important challenging research in sensor network security. Therefore several session key establishment protocols have been proposed for that purpose.

In this paper, we analyzed and compared the existing session key establishment protocols based on the criterions of generation strategy and uniqueness of the session key, connectivity, overhead of communication and computation, and vulnerability to attacks. Based on the analysis results, we specify the requirements for the secure and efficient protocols for establishing session keys. Then, we propose an advanced protocol to satisfy the specified requirements and verify the superiority of our protocol over the existing protocols through the detailed analysis.

Key Words : Sensor Network, Session Key, Security, Connectivity, Key Uniqueness

1. 서 론

저전력/소용량 장치의 개발과 임베디드 시스템 및 무선 기술의 발달로 많은 응용 분야에서 효율적인 해결 방안으로 제시되고 있는 센서 네트워크는 소수의 베이스 노드와 수백개 또는 수 천개 이상의 매우 많은 수의 센서 노드들로 구성된다. 센서 노드는 계산 능력이나 저장 용량 및 통신 능력이 매우 미약한 장치로 통신 범위내의 노드와만 통신이 가능하다. 센서 네트워크는 모든 센서 노드들이 배치된 후에야 네트워크 구조가 정해지는 특성을 가지며, 응용 분야에 따라 센서 노드들은 보안이 매우 취약하거나 또는 외부의 공격이 가능한 지역에 배치될 수 있다[1, 2].

센서 네트워크의 활용 분야는 매우 다양하지만, 보안 탐색 또는 군사 추적 및 재난 지역 탐사등과 같은 분야에서는 통신 과정에서 민감한 사적 정보의 비밀성과 무결성을 유지하기 위한 보안이 요구된다. 만약, 센서 네트워크 상에 적절한 보안 체계가 없다면, 통신 과정에서 침입자가 센서 노드의 중요한 탐사 정보를 가로채거나 센서들에게 잘못된 명령을 주어 센서 네트워크의 기능을 마비시킬 수 있다.

센서 네트워크의 통신은 베이스 노드와 센서 노드사이의 통신 및 두 센서 노드 사이의 통신으로 구성된다. 센서 네트워크의 베이스 노드는 충분한 연산 능력과 통신 능력을

※ 이 연구는 2005학년도 단국대학교 대학연구비의 지원으로 연구되었음.
† 종신회원 : 단국대학교 대학원 박사과정 수료
†† 종신회원 : 단국대학교 정보컴퓨터학부 교수, 교신저자
논문접수 : 2005년 3월 30일, 심사완료 : 2005년 7월 4일

가지므로 베이스 노드와 센서 노드사이의 통신은 비교적 안전하게 수행될 수 있으며 이를 위한 여러 프로토콜들이 제안되어 활용되고 있다[2]. 하지만, 베이스 노드와 달리 여러 제약점을 갖는 센서 노드에는 공개키 기반의 전통적인 보안 기법들을 적용할 수 없으므로, 센서 노드사이의 안전한 통신이 센서 네트워크의 중요한 과제가 되고 있다[3].

두 센서 노드 사이의 통신은 베이스 노드를 통한 간접 통신과 센서 노드들이 서로 직접 정보를 주고받는 직접 통신의 두 경우가 가능하다. 베이스 노드를 통한 간접 통신에서는 베이스 노드와 각 센서 노드 사이에 안전한 통신이 가능하므로, 송신 센서 노드는 베이스 노드에게 안전하게 전송하고 이를 베이스 노드가 다시 수신 노드에게 안전하게 전송하여 두 센서 노드들 사이에서 안전한 통신이 가능하다.

하지만, 베이스 노드를 통하지 않는 직접 통신에서 센서 노드들은 다른 센서 노드들을 인증하거나 민감한 데이터를 전송하기 위해 비밀키를 사용한다. 센서 노드들이 동일한 비밀키를 사용한다면 분석적 공격을 증가시키므로 두 센서 노드의 공유된 비밀키(이를 세션키라 한다)를 설정하고 이를 이용한 암호와 인증에 기반을 둔 통신을 수행해야 안전하다. 기존의 전통적인 공개키 기반의 비밀키 형성 기법을 적용할 수 없는 세션 노드들 사이에서 세션키를 구현하는 직접적인 해결책은 센서 노드들을 배치하기 이전에 세션키를 미리 분배하는 사전 세션키 분배 방식이다[5]. 사전 세션키 분배를 위해 센서 네트워크 전체에 공통인 단일의 세션키를 사용하는 것은 가장 간단한 해결책이지만, 모든 센서 노드들이 동일한 비밀키를 사용하므로 한 센서 노드만 공격을 받아도 전체 네트워크가 노출되는 보안적 위험이 있다. 이에 대비되는 가장 안전한 방법은 센서들이 배치되기 이전에 센서 노드들 쌍 사이에 서로 다른 각각의 세션키를 미리 분배하는 두 노드간 비밀키 공유 기법(pair-wise private key-sharing scheme)으로, 이 방법은 한 센서 노드가 공격을 당해도 그 노드와 공유하는 세션키들 만이 노출되는 보안적 장점이 있다. 하지만, 각 센서 노드는 배치된 이후에만 통신이 가능한 범위에 있는 이웃 센서 노드들을 인식할 수 있으므로, 모든 센서 노드 쌍 사이에 미리 세션키를 분배하는 것은 매우 비효율적이다[3].

단일 세션키 또는 개별 쌍 세션키의 사전 분배 방법이 갖는 보안 또는 효율적 문제점에 대한 개선책으로 배치 이전에 세션키 설정에 필요한 정보를 각 센서에게 분배하고 센서 노드들이 배치된 이후에 세션키를 설정하는 방법들이 제안되었는데, 이들은 세션키를 설정하는 노드들의 구성에 따라 두 가지로 분류될 수 있다.

첫째 방법은 센서 노드에 비해 계산 능력과 저장 용량이 뛰어난 신뢰할 수 있는 베이스 노드가 세션키를 생성하여 두 센서 노드에게 분배하는 베이스 노드 기반 방법이다. 베이스 노드와 각 센서 노드 사이에는 안전한 통신이 가능하므로, 베이스 노드가 두 센서 노드를 위한 세션키를 생성하여 두 센서 노드에게 안전하게 분배할 수 있다. 대표적인 예로는 SPINS 시스템의 SNEP 프로토콜을 들 수 있다[4]. SNEP 프로토콜에서 베이스 노드는 신뢰할 수 있는 제삼자인 KDC로 동작하여 인증과 키생성 및 분배를 수행한다. 하지만, 이 방법은 베이스 노드에게 과중한 부담을 주며, 베이스 노드가 공격을 받으면 모든 세션키 정보가 누출되어 전체 센서 네트워크가 위험할 수 있다.

두 번째 방법은 통신하려는 두 센서 노드가 협의하여 공유 세션키를 형성하는 방법이다.

하지만, 연산 능력과 저장 용량 및 통신 능력에 제한적인 센서 노드가 RSA나 DH와 같은 전통적인 공개키 기반에 의한 키 교환 방식을 이용하여 공유 세션키를 형성하거나 베이스노드가 개입하지 않으면서 Kerberos와 같은 신뢰할 수 있는 제삼자에 의한 키 분배 방식은 불가능한 실정이다. 따라서, 배치 이전에 모든 센서 노드들에게 세션키를 형성하는데 사용될 키 정보를 미리 분배하고, 이를 이용하여 배치 이후에 두 센서 노드들이 공유 비밀키를 스스로 생성하는 센서 노드 협상 방법들이 제안되었다[5-12].

이 들 중에서 가장 간단한 기법으로 센서 네트워크 공통의 단일 세션키가 갖는 보안 취약점을 개선하여 센서 네트워크에 있는 모든 센서 노드들에게 공통의 비밀키(마스터키)를 부여하고, 각 센서 노드는 마스터키로 암호화된 키 협상 메시지를 방송하여 이웃 노드와 세션키를 설정하는 BROSK(BROadcast Session Key Negotiation Protocol)이 제안되었다[5]. 하지만, 마스터키를 이용한 세션키 형성 기법은 마스터키가 모든 센서들에게 공통으로 사용되므로 마스터키의 노출이 모든 세션키의 노출로 연결되는 보안적 문제점을 가지므로, 이러한 문제점을 해결한 랜덤 키 사전 분배 기법이 제안되었다[6]. 랜덤 키 사전 분배 기법은 두 노드가 공통으로 배분된 키를 통해 세션키를 형성하고, 동일한 세션키가 여러 노드의 쌍들의 세션키로 사용될 수 있으므로 한 세션키의 노출이 다른 노드들 사이의 보안에 영향을 주는 문제점과 두 노드사이에 공유되는 세션키가 없을 수 있다는 취약점이 있다.

이러한 취약점들을 개선하기 위해 여러 개의 공유키를 결합하여 세션키를 생성하는 다양한 기법들이 제안되었는데, 그 첫째가 두 노드 사이에 일정 수 이상의 공유키가 존재하는 경우에만 세션키를 형성하는 Q 복합키 기법이다[7]. 하지만, Q 복합키 기법은 공유한 키를 발견하기 위해 퍼즐 기법을 도입하여 과다한 통신을 요구하므로, 이 문제점을 해결하기 위해 노드 Id 기반의 키 생성 기법이 제안되었으나 보안적 취약점은 오히려 증대되었다[8]. 또한, Blom의 사전 키 분배 기법[9]과 랜덤 키 사전 분배 기법[6]을 결합하여 일정한 개수 이하의 세션 노드가 공격을 받아도 다른 노드의 세션키는 안전함을 보장하는 세션키 형성 기법도 제안되었다[10]. 각 센서 노드의 위치에 대한 사전 지식이 있으면 세션키의 형성은 더욱 효율적이 되는데, 센서들의 예측적 위치에 기반한 세션키 형성 기법과 배치 지역에 대한 사전 지식이 있는 경우에 이를 활용한 세션키의 연구도 제안되었다[11, 12]. 하지만 이 기법들은 센서 노드의 위치에 대한 정보를 요구하는 제한점을 가진다. 배치 이전에 각 센서 노드에

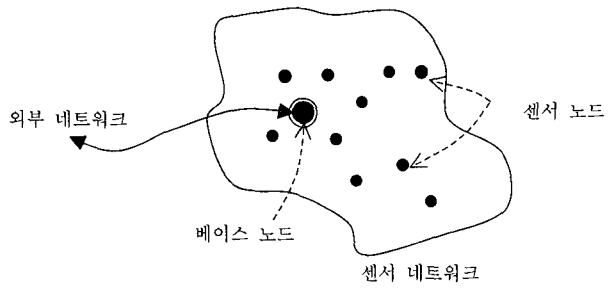
분배하는 정보를 키가 아닌 비트열을 사용한 OKS(Overlap-Key-Sharing)도 제안되었다[5].

두 센서 노드 사이의 세션키 생성을 위한 기존의 기법들은 각각 서로 다른 측면의 관리적 또는 보안적인 문제점을 가지고 있다. 본 논문에서는 기존의 키 관리 기법들을 동일한 기준(세션키 생성 방법, 세션키의 유일성, 세션키의 상호 확인, 연결성, 통신 과부하, 암호 및 연산 과부하, 공격의 취약성 등)에 의해 비교 분석하고, 분석된 결과를 기반으로 효율적인 세션키 생성 프로토콜을 위한 기준안을 제시한다. 또한, 기준안을 만족시키는 개선된 세션키 생성 프로토콜을 제안하고, 동일한 기준으로 제안 프로토콜의 우수성을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 세션키 생성 프로토콜의 분석을 위한 여러 자료들을 제시하고, 3장에서 기존의 대표적인 프로토콜들을 동일 기준에 의해 비교 분석한다, 4장에서는 분석 결과를 통해 안전한 세션키 생성 프로토콜을 위한 기준안을 제시하고, 이 기준안을 만족시키는 개선된 프로토콜을 제안하고, 또한 제안프로토콜의 성능을 상세히 분석한다. 마지막 5장의 결론으로 본 논문을 마무리한다.

2. 센서 네트워크와 키 관리 기법

전형적인 센서 네트워크는 전력, 연산 처리 및 통신 능력에 제약을 갖는 센서 노드들과 이 보다 더욱 강력한 베이스 노드들로 구성된다. 센서 노드는 무선 방송을 통해 다른 센서 노드 또는 베이스 노드와 통신하며, 베이스 노드는 외부 네트워크에 연결된다. 본 장에서는 센서 노드가 갖는 제약 특성을 설명하고, 센서 노드와 센서 노드 사이에 세션키를 형성하기 위한 여러 가지 고려 사항들을 분석한다.



(그림 1) 센서 네트워크의 구조

2.1 센서 노드의 제약

센서 노드는 다음과 같은 내부 또는 외부 환경의 제한을 가진다[1, 3].

1) 센서 노드는 연산 능력, 저장 용량 및 전원 공급 등의 내부 제약으로 Diffie-Hellman 키 동의 또는 RSA 키 전송과 같은 과중한 연산을 요구하는 전형적인 공개키 기반의 알고리즘은 사용할 수가 없다.
2) 센서 노드들은 무선으로 통신하므로 통신 범위에 제약이 있으며 또한 외부 공격에 취약하다.
3) 센서 노드의 모든 동작 중에서 전송에 의한 전력 소비가 가장 크다.
4) 센서 노드들은 공개적인 장소 또는 보안 공격이 가능한 지역에 배치될 수 있다. 따라서, 각 센서 노드는 공격에 대해 안전하다고 가정할 수 없다.
5) 센서 노드들은 배치되기 이전에 네트워크의 정확한 구조 또는 각 노드의 이웃 노드들을 알 수 없다.
6) 베이스 노드에 의존하는 프로토콜은 베이스 노드가 침입당하면 전체 네트워크의 보안이 침해된다.

2.2 센서 노드에게 가능한 공격

센서 노드는 무선 방송을 통해 다른 센서 노드와 정보를 교환하므로, 다음과 같은 수동적 또는 능동적 공격이 가능하다.

1) 도청(eavesdropping) 공격 : 센서와 센서 사이에 평문으로 전송되는 모든 정보는 제삼자에게 노출될 수 있다.
2) 링크의 트래픽 공격 : 특정 센서 노드 사이의 전송 내용을 추적하여 두 센서 노드 사이의 암호화 정보를 알아낼 수 있다.
3) 센서 노드의 공격 : 센서 노드를 공격하여 그 센서에 저장된 키의 정보와 다른 센서 노드와의 세션키 정보를 얻을 수 있다.
4) 허위 정보 전송 : 다른 센서 노드의 전송을 가로채어 허위 정보를 전송하거나, 의미 없는 정보를 전송하여 수신 노드에게 서비스 거부 공격을 할 수 있다.
5) 서비스 거부(Dos) 공격 : 센서 노드에게 과도한 연산 또는 통신을 요구하는 메시지를 전송하여 그 센서 노드가 정상적으로 동작하지 못하도록 할 수 있다.

2.3 키 관리 프로토콜의 비교 측도

앞에서 제시된 바와 같이 센서 노드가 갖는 여러 제약점을 고려하면, 전원의 소비가 많은 전송, 수신, 암호화, 복호화 등의 횟수를 줄이면서 안전성을 유지하는 키 관리 프로토콜이 요구된다. 본 연구에서는 동일한 기준에 의해 비교할 수 있는 객관적인 측도로 세션키 생성 방법, 세션키의 유일성, 세션키의 상호 확인, 연결성, 통신 과부하, 암호 및 연산 과부하, 공격의 취약성을 설정하고 이에 따라 다음 장에서 기존의 세션키 형성을 위한 프로토콜들을 비교 분석한다.

3. 센서 네트워크의 키 관리 프로토콜의 분석

본장에서는 기존에 제안되었던 센서 네트워크의 세션키 관리 프로토콜들을 상세히 분석하고, 2.3절에서 제시된 공통된 측도를 통해 비교 분석한다.

3.1. BROSK(BROadcast Session Key Negotiation Protocol)

센서 네트워크의 공통된 단일 세션키가 갖는 단점을 보완

한 BROSK에서는 모든 센서 노드에게 공통의 마스터 키(세션키가 아닌)가 할당되며, 각 센서 노드는 랜덤 번호를 생성한 후에 이 마스터키로 암호화한 키 협상 메시지를 방송하여 다음과 같이 이웃 노드와 세션키를 형성한다[5]. 각 센서 노드는 자신의 노드 Id와 자신이 생성한 랜덤번호(nonce)와 마스터키로 생성한 MAC(Message Authentication Code)을 방송하며, 이를 수신한 이웃 노드는 자신의 랜덤 번호와 이웃 노드의 랜덤 번호에 대한 MAC을 생성하여 두 노드 사이의 유일한 세션키를 형성한다.

BROSK는 통신량이 매우 적고 각 센서 노드 쌍에게 유일한 세션키를 형성할 수 있다는 장점이 있지만, 마스터키가 모든 센서 노드에게 공통이므로 마스터키가 노출된 경우에는 전체 네트워크의 세션키가 노출될 취약점이 있다.

3.2. 랜덤 키 사전 분배 프로토콜

Eschenhaur와 Gligor는 노드간 비밀키 공유 기법에서 발생한 센서 노드의 저장 부담도 줄이면서 보안 위험을 높이지 않을 수 있는 랜덤 키 사전 분배 프로토콜을 제안하였다[6]. 랜덤 키 사전 분배 기법은 네트워크에서 사용될 많은 키들의 집합을 정의하고, 이로부터 랜덤하게 선택된 소수의 키 집합(이를 키 링이라 한다)을 각 노드가 배치되기 이전에 배분하고, 두 노드가 합의하여 공통으로 배분된 키를 통해 세션키를 형성하는 기법이다. 이 프로토콜은 배치 이전의 키 사전 분배단계와 배치 이후의 공유키 발견 단계로 구성된다.

첫 번째 키 사전 분배단계에서는 센서 네트워크에서 세션키로 사용될 매우 많은 키들의 집합(P)으로부터 각 센서 노드에게 m개의 키를 랜덤하게 할당한다. 각 센서는 할당된 m개의 키(와 키 Id)를 자신의 키 링에 저장한다.

두 번째 공유키 발견 단계에서는 이웃 노드와 공통된 키를 찾아 이를 두 노드의 세션키로 형성한다. 공유키 발견은 키의 Id 전송 또는 키로 암호화한 전송의 두 가지 구현이 가능하다.

키 Id 전송에 의한 공유키 발견을 위해서는 각 센서 노드가 자신의 키 링에 저장된 키 Id의 목록을 방송하고 이웃 노드로부터의 키 Id 목록의 방송을 수신한다. 수신된 키 Id 목록과 자신의 키 Id 목록을 비교하여 동일한 Id가 발견되면, 그 Id에 해당하는 키가 해당 센서 노드와의 세션키가 된다.

암호화 전송에 의한 공유키 발견을 위해서는 각 센서 노드가 자신의 키 링에 저장된 키(k_i, i=1, 2, 3,...m)들에 대해 약속된 값 a와 $Ek_i(a)$를 방송한다. 이웃 노드로부터 수신된 $Ek_i(a)$를 자신의 키 링에 저장된 키들로 복호화하여 약속된 값 a를 얻을 수 있으면, 그 키가 해당 센서 노드와의 세션키가 된다.

랜덤 키 사전 분배 기법은 두 노드가 공유한 키가 있는 경우에만 세션키를 형성할 수 있으며. 동일한 세션키가 여러 노드들 사이의 세션키로 형성될 수 있다는 문제점이 있다. 또한, 선정된 공유키에 대한 상호 확인과정이 미비하다.

공유키 발견 단계에서 키 Id 전송 방법은 평문으로 방송되므로 도청 공격에 취약하고, 암호화 전송 방법은 서비스 거부 공격에 취약하다.

3.3 OKS(Overlap-Key-Sharing)

OKS 프로토콜은 매우 많은 키들의 집합(P) 대신에 매우 긴 비트열을 이용하여 두 센서 노드가 공유한 비트열로 세션키를 생성하는 프로토콜이다[5]. 따라서, 각 센서 노드들에게 네트워크의 긴 비트열의 일부분인 비트열을 랜덤으로 할당하여 저장토록 한다.

각 센서 노드는 자신이 저장한 비트열의 정보를 방송하고, 이웃 노드가 방송한 비트열의 정보를 수신하여 자신이 저장한 비트열과 비교한다. 이웃 노드와 공유되는 중복되는 구간의 비트열을 해쉬 함수를 통해 일정 크기의 세션키를 형성한다.

랜덤 키 사전 분배 방법에 비해 저장량 및 통신량은 줄일 수 있지만, 두 센서 사이에 세션키를 연결할 확률(연결성)이 줄어드는 단점이 있다.

3.4 Q 복합키 기법

두 센서 노드가 공유하는 하나의 키를 세션키로 사용하는 경우에는 동일한 키가 여러 노드들 사이의 세션키로 선택되어 한 세션키의 노출이 다른 노드들 사이의 보안에 영향을 줄 수 있다. Q 복합키 기법은 두 노드의 공유 세션키가 일정 개수(q) 이상인 경우만 세션키를 형성하며 키 사전 분배 단계와 공유키 발견 단계로 구성된다[7]. 키 사전 분배 단계는 랜덤 키 사전 분배 프로토콜과 동일하게 자신의 노드 Id를 방송하고, 자신과 이웃한(통신 범위에 있는) 노드 Id를 확인한다.

공유키 발견 단계에서 각 센서 노드는 자신의 키 링에 있는 m개의 키들에 대한 퍼즐(클라이언트 Merkle 퍼즐)을 이웃 노드에게 전송한다. 이웃 노드의 퍼즐을 수신하면, 자신의 키 링에서 퍼즐에 올바른 답을 제공하는 키(이것이 두 센서 노드의 공유키)를 찾아 그 답을 퍼즐을 송신한 센서에게 전송한다. 이웃 노드와의 공유키의 수가 일정 개수(q) 이상이면 이들 공유키로부터 해쉬를 통해 두 노드 사이의 세션키를 형성한다.

Q 복합키 기법은 서로 다른 센서 노드의 쌍이 동일한 세션키를 가질 확률을 낮추어 안전성을 높이고, 퍼즐을 사용하여 도청 공격에 대비하였다. 하지만, 재생 공격에 대비하여 각 퍼즐을 별도의 메시지로 전송하므로 센서 노드의 가장 취약한 전력에 큰 영향을 주는 전송량을 과도하게 증가시킨 문제점이 있으며, 또한 형성된 키에 대한 상호 확인 작업이 생략되어 있다.

3.5 노드 Id 기반의 키 생성 기법

모바일 통신에서는 각 노드의 주소로부터 그 노드의 고유한 공개키를 구할 수 있는 ABK 기법이 도입되었는데, 센서 네트워크에서는 연산이 과도한 공개키 기법을 사용할 수 없

지만 ABK와 유사한 개념의 노드 Id 기반의 키 생성 기법이 제안되었다[8]. 즉, 랜덤 키 사전 분배 기법과 유사하게 배치되기 전에 센서 네트워크에서 정의된 키의 집합 중에서 일정한 수의 임의의 키가 각 센서 노드에게 사전 분배된다. 각 센서 노드는 노드 Id와 랜덤 연산을 통해 키 Id들을 구하고, 네트워크에서 정의된 키 집합에서 키 Id에 해당하는 키들을 각 센서 노드에 사전 분배한다. 또한, 각 센서 노드는 다른 노드의 Id로부터 그 센서 노드에게 할당된 키들에 대한 인덱스(키 Id)의 집합을 랜덤 연산을 통해 생성하고, 그들로부터 공유키를 생성하는 방법이다.

이 때, 센서 노드의 Id로부터 그 노드에 할당된 키 Id들의 집합을 생성할 수 있는 연산을 모든 노드에게 공개하여, 각 센서 노드는 스스로 이웃 노드가 저장중인 키들의 키 Id 목록을 생성하여 공유키를 쉽게 찾을 수 있다. 따라서, 기존의 방법들에 비해 공유키를 생성에 대한 통신량과 암/복호화를 위한 연산량을 줄일 수 있다.

노드 Id 기반의 기법은 다중의 공유키를 결합하여 세션키를 형성하므로 다른 세션키의 노출에도 비교적 안전하고 이웃 노드의 Id만으로 상호 협상 과정 없이 공유키를 발견할 수 있어 전송량을 줄이는 장점이 있지만, 어떤 센서 노드라도 두 센서 노드의 세션키를 쉽게 알 수 있다는 보안적인 취약점이 있다.

3.6 독립 세션키 사전 분배 기법

배치 이전에 세션키를 형성에 필요한 키 정보를 미리 분배하고, 이를 이용하여 배치 이후에 두 센서 노드들이 공유 비밀키를 생성하는 센서 노드 협상 방법들은 미리 분배되는 정보의 공유성으로 인해 각 세션키들이 서로 독립적이지 않다는 문제점이 발생한다. 따라서, 일부 센서 노드가 공격을 받으면 다른 센서 노드의 세션키가 노출될 수 있다. 이러한 보안 문제의 해결책으로 Blom의 사전 키 분배 기법[9]과 랜덤 키 사전 분배 기법[6]을 결합하여 일정한 개수 이하의 세션 노드가 공격을 받아도 다른 노드의 세션키는 안전함을 보장하는 독립 세션키 사전 분배 기법이 제안되었다[10].

Blom의 사전 키 분배 기법은 매트릭스의 대칭성(symmetry)을 이용한다. 즉, 대칭적 매트릭스(N×N ; N은 센서 노드의 수)를 형성한다면 대칭 위치의 두 항목은 Kij=Kji이므로, Kij을 노드 i가 생성하고 Kji을 노드 j가 생성할 수 있다면 이 두 값은 일치하게 되므로 이를 두 노드 사이의 세션키로 사용할 수 있다. 이 때, N×N의 대칭적 매트리스를 다른 두 매트릭스(A와 G)의 곱으로 표현하면 Kij=Ai(매트릭스 A의 i번째 행)×Gj(매트릭스 G의 j번째 열)이 되므로, 곱셈 연산을 위해 각 노드는 자신의 Id에 해당하는 매트릭스 A의 행과 매트릭스 G의 열을 저장하도록 하여 세션키를 형성한다. 매트릭스 G에 있는 r+1개 항의 행들이 서로 독립적이라면, 세션키는 r개 이하의 노드(세션키)가 공격을 받아도 안전하다.

제안된 기법에서는 Blom의 사전 키 분배를 위한 매트릭스 공간(매트릭스 A와 G로 구성된)을 여러 개 정의하고, 랜덤 키 분배 기법에 따라 매트릭스 공간들 중에서 랜덤으로 선정된 일부 공간들을 각 센서 노드에게 할당한다.

따라서, 이 기법에서는 각 센서 노드의 저장량을 줄이면서, 세션키를 형성하기 위해 이웃 노드에게 자신의 Id와 사용할 매트릭스 공간의 Id 및 매트릭스 열의 생성을 위한 기본값(seed)만을 전송함으로 전송량도 최적화하며 세션키 형성 과정이 완료된다. 이때 평문으로 전송되는 기본값은 공개되어도 무방하다.

하지만, 이 제안도 일부 노드에 대한 공격으로부터 다른 세션키의 보호를 위해 Blom의 기법을 수정하여 모든 이웃 노드들 사이의 연결성을 보장하지 못하므로 경로 키(path key)를 도입하였다.

3.7 프로토콜들의 비교

<표 1>은 앞에서 제시된 프로토콜들을 동일한 기준에서 분석한 비교표이다. 두 이웃 센서 사이에는 직접 연결이 존재한다고 가정하였고, 제시된 통신 항목은 두 센서 노드 사

〈표 1〉 세션키 형성 프로토콜들의 비교

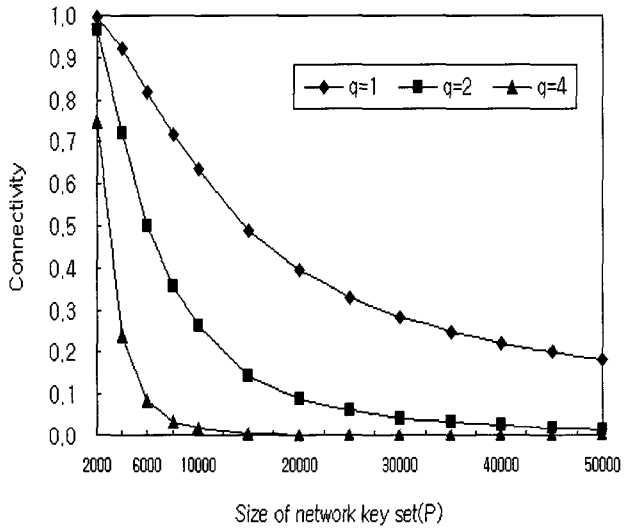
		BROSK	랜덤 키 분배 (암호화)	OKS	Q 복합키	노드 Id 기반	독립 세션키
사전 분배 정보		마스터키	m×(키, 키Id)	비트열	m×(키, 키Id)	키 Id 생성 함수	매트릭스
	생성 기법	랜덤 생성	단일 공유키	공유 비트열	다중 공유키	다중 공유키	매트릭스 곱셈
	연결성	O	△	△	△	△	△
	유일성	O	X	△	△	△	O
	상호확인	X	X	X	X	O	X
	키 정보 교환	2	2m	2	2m	2	2
	키 교환/검증	(2)	(2)	(2)	(2)	(2)	(2)
연산 (두 노드에서의)		MAC : 6	암호화 : 2m 복호화 : $2m^2$	비교 : 2 해성 : 2	퍼즐 생성 : 2m 퍼즐 풀이 : 2m 해성 : 2	키 생성 : 2 키 비교 : $2m^2$	컬럼생성[1] 키생성[2]
	서비스 거부	X	X	△	X	△	O
	도청	O	O	X	O	△	△
	노드 공격	X/O	△	△	△	△	O

O : 우수, △ : 보통 X : 취약
( )는 세션키 상호 확인을 위한 전송으로 모든 프로토콜에 적용, 키 링의 크기=m;
1) 공개할 매트릭스의 컬럼 생성, 2) 곱셈 연산

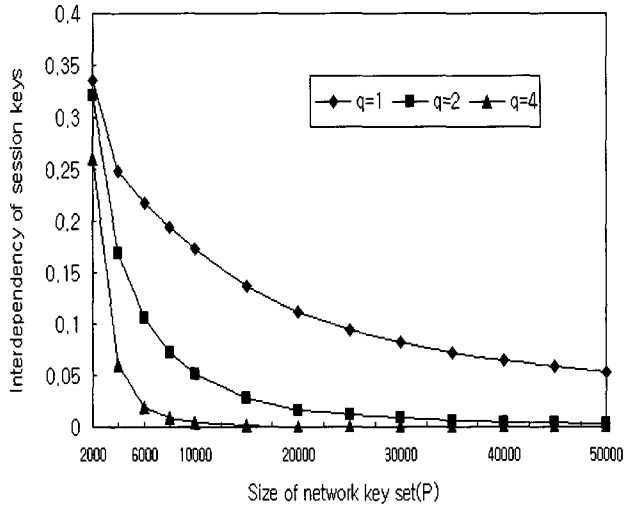
이에서 세션키 생성에 필요한 전송의 수이며, 연산 항목은 세션키를 생성하기 위해 두 센서 노드가 수행하는 연산의 수이다.

<표 1>에서 보듯이 기존의 모든 프로토콜은 한 가지 이상의 기준에서 제한점을 보이고 있다.

사전 키 정보 분배를 이용하는 랜덤 키 분배, OKS, Q 복합키 기법, 노드 Id 기반 기법은 연결성, 세션키의 유일성 및 보안성에서 취약하다. 이들 프로토콜에서는 연결성이 확률적으로 정해지므로, 이웃 노드들 사이에 완전한 연결성을 제공하지 못한다. 연결성을 증가시키기 위해서는 네트워크의 키 집합(P)의 크기를 줄이거나 또는 각 센서 노드의 키 링의 크기(m)를 늘려야한다. 하지만, 이는 세션키의 유일성을 감소시키게 된다. 이러한 관계는 [6]과 [7]에서 제시된 수식을 근거로 작성한 (그림 2) 및 (그림 3)에서 확인 할 수 있다.



(그림 2) 센서 네트워크의 연결성



(그림 3) 센서 네트워크의 의존성

(그림 2)는 센서 네트워크의 연결성(m=100인 경우에 두 이웃 노드가 q개 이상의 키를 공유하여 세션키를 형성할 확률로 표현)을 보이며, (그림 3)은 세션키의 상호 의존성(m=100인 경우에 30개의 센서 노드가 공격을 받아 정보가 노출된 상황에서 다른 노드들의 세션키가 노출될 확률로 표현)을 보인다. P가 감소함에 따라 연결성은 증가하여 개선되지만 동시에 세션키의 상호 의존성도 같이 증가하여, 기존 사전 키 정보 분배를 이용하는 프로토콜들은 연결성과 세션키의 유일성을 동시에 만족시키지 못한다. 이는 m에서도 동일한 특성을 보인다. 또한, m은 통신량, 연산량 및 저장 용량에 영향을 주므로, m값의 선택시에는 연결성 및 세션키의 유일성과 함께 이점도 고려해야한다.

4. 제안 기법

본 장에서는 앞장에서 설명된 기존 프로토콜들의 분석 결과로부터 안전한 세션키를 생성하기 위한 프로토콜의 요건들을 제시하고 요건을 충족하는 세션키 프로토콜을 제안한다.

4.1 안전한 세션키의 생성 프로토콜

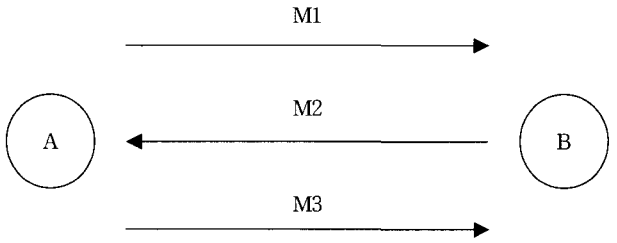
앞 장에서 제시된 기존 프로토콜들의 분석 결과로부터 안전한 세션키 생성 프로토콜의 요건을 다음과 같이 제시한다.

1) 사전 키 정보 분배를 이용하는 세션키 생성 프로토콜(랜덤 키 분배, OKS, Q 복합키 기법, 노드 Id 기반 기법)에서는 세션키의 유일성에 한계가 있다. 이들 프로토콜에서는 연결성과 세션키의 상호 의존성이 동일한 인수에 의해 작용하므로 이들은 서로 상대적인 특성이 있다. 따라서, 네트워크의 연결성은 높이면서 세션키의 노출에는 영향이 없도록 설계해야 된다.
2) 세션키 생성 프로토콜에서는 최소한 4회의 전송(2회의 센서 ID 방송, 2회의 세션키 교환/확인)을 필요로 한다. 이외에 다른 기능을 추가하면 전송량은 증가한다. 예를 들어, 세션키 생성을 위해 교환되는 정보에 대한 도청 공격에 대응하기 위해 전송되는 정보를 암호화하거나 퍼즐을 사용하여 보안성을 강화시키면, 전송량이 증가한다. 센서 노드의 가장 큰 제약은 전력(건전지의 수명)이며, 센서 노드의 동작 중에서 전송이 가장 큰 전력을 소모하므로 세션키 형성 프로토콜은 보안을 유지하면서 통신 횟수를 줄이도록 설계해야 한다.
3) 공격자가 센서 노드에게 복호화 또는 퍼즐과 같은 고비용의 연산을 수행하도록 메시지를 대량으로 전송하여 서비스 거부 공격을 시도하면, 센서 노드는 고비용의 연산 수행으로 정상적인 동작이 어렵게 된다. 따라서, 고비용 연산의 요청에 대한 간단한 검증을 통해 이러한 서비스 거부 공격을 피하도록 설계해야 한다.
4) BROSK의 네트워크 공통의 마스터키나 노드 Id 기반 기법의 공개된 키 생성 연산은 제삼자에 의한 세션키 공격에 매우 취약하다. 따라서, 공개되는 정보의 수나 유효 시간을 공격에 대응할 수 있는 만큼 감소시키거

나 또는 공개되는 정보로부터 세션키를 유추할 수 없도록 대응한다.

4.2 제안 프로토콜

본 절에서는 앞에서 제시된 기준안을 만족시키기 위해 노드 Id 기반 프로토콜로부터 생성된 키를 세션키 협상을 위한 1회용 비밀키로 사용하는 프로토콜을 제안한다. 제안 프로토콜은 각 센서에게 키 배치 이전의 키 사전 분배 단계, 배치 이후의 1회용 비밀키 생성 단계와 두 세션키 교환 단계로 구성된다. 임의 센서 노드 A와 B가 세션키 협상을 위한 메시지 교환의 예는 (그림 4)와 같다.



$M1 : request|ID_A$

$M2 : (ID_B|ID_A|EK_T[K_{AB}])|MACK_T[ID_B|ID_A|EK_T[K_{AB}]]$

$M3 : (ID_A|ID_B|EK_{AB}[K_T])|MACK_{AB}[ID_A|ID_B|EK_{AB}[K_T]]$

ID_A : 세션 노드 A의 식별자
K_{AB} : 세션키, K_T : 1 회용 비밀키
$E_K[M]$: 키 K로 메시지 M의 암호화
$MAC_K[M]$: 키 K로 생성한 메시지 M의 MAC

(그림 4) 세션키 협상 메시지

4.2.1 키 사전 분배 단계

제안 프로토콜의 키 사전 분배 단계는 노드 Id 기반의 키 생성 기법[8]에서의 랜덤 연산을 이용한 키 사전 배포 정책과 동일하다. 키 사전 분배 단계는 센서 네트워크에서 사용될 많은 키들($k_1,k_2,...,k_p$)의 집합(P)을 생성한다. 각 센서 노드는 센서 네트워크에서 유일한 노드 Id을 가지고 노드 Id를 기반으로 랜덤 연산을 통해 1과 p사이에서 m개의 키 Id들(키 Id 목록)을 구한다. 각 센서 노드는 네트워크의 키 집합(P)으로부터 키 Id에 해당하는 키를 센서 노드의 키 링에 저장하고 노드 Id를 이용해 인덱스를 구할 수 있는 랜덤 연산 방법을 공유한다.

4.2.2 1회용 비밀키 생성 단계

임의 두 센서 노드 간 통신 채널은 각 센서 노드의 키 링에서 동일한 키의 존재 여부에 따라 결정된다. 동일한 키가 존재하면 공유키라 하고 이를 이용하여 1회용 비밀키를 생성한다. 1회용 비밀키 생성 단계는 다음과 같다.

① 각 센서 노드는 자신의 노드 Id를 방송한다. (그림 4)의 예에서 노드 A는 노드 B에게 M1를 전송한다.

② 각 센서 노드는 방송을 수신하여 송신 노드의 Id를 확인하고, 수신된 Id와 랜덤 연산을 통해 송신 노드의 키 링에 저장된 키들에 대한 키 Id 목록을 생성한다. 송신 노드의 키 Id 목록과 자신이 저장한 키 Id 목록을 비교하여 동일한 키 Id 목록을 찾는다. 센서 노드는 동일한 Id 목록에 해당하는 공유키를 결합하여 1회용 비밀키(1회용 임시 세션키=⊕공유키)를 형성한다.

4.2.3 세션키 교환 단계

임의 두 센서 노드 간 통신 채널이 존재한다면 랜덤 번호를 생성하고 이를 안전한 통신 채널을 위한 세션키로 사용한다. 세션키를 생성한 노드는 상대 노드에게 세션키를 전송하고 상호 확인한다. 이를 위한 세션키 교환 단계는 다음과 같다.

① 1회용 비밀키를 생성한 센서 노드는 상대 노드와 공유할 세션키(K_{AB})를 랜덤하게(랜덤 번호 생성을 통해) 형성한다. 세션키를 생성하는 노드는 노드 Id에 의해 정해진다.(두 노드의 Id의 합이 홀(짝)수이면 작은(큰) Id의 노드가 생성한다.)

② 세션키를 생성한 노드는 상대 노드에게 1회용 비밀키로 세션키를 암호화하고 MAC을 생성하여 메시지(M2)를 전송한다.

③ 이를 수신한 상대 노드는 전송 노드와 공유한 1회용 비밀키로 수신한 MAC 정보를 통해 상대 노드를 인증한 후 복호화하여 세션키를 얻는다. 키 형성을 확인하기 위하여 1회용 비밀키를 세션키로 암호화하여 상대 노드에게 메시지(M3)를 전송한다.

• 제안 프로토콜의 개선 특성

제안 프로토콜은 다음과 같이 제시된 요구 사항들을 만족시킨다.

1) 제안 프로토콜에서는 다중 공유키가 일회용 비밀키에만 사용되므로, 네트워크의 키 집합 또는 각 센서 노드의 키 링의 크기에 무관하게 세션키가 노출될 확률에는 변화가 없다. 따라서, 제안 프로토콜은 키 링의 크기를 증가시켜 두 센서 노드가 공유키를 가질 확률을 높일 수 있다.
2) 각 센서 노드는 자신의 Id와 생성된 세션키만을 전송하므로 통신의 횟수를 최소화한다.
3) 센서 노드는 자신에게 전송된 모든 세션키를 복호화할 필요는 없고, 자신과 1회용 비밀키를 공유한 센서 노드로부터의 전송인가를 MAC를 통해 확인하여 복호화한다. 따라서, 센서 노드는 무차별 전송에 의한 메시지의 복호화를 줄일 수 있다.
4) 세션키는 공유키로부터가 아닌 별도의 생성 연산을 통해 만들어지므로, 세션키의 유일성을 높일 수 있다. 즉, 한 노드에게 할당된 키의 노출이 다른 노드의 세션키에는 영향이 없으므로 전체 네트워크 보안에는

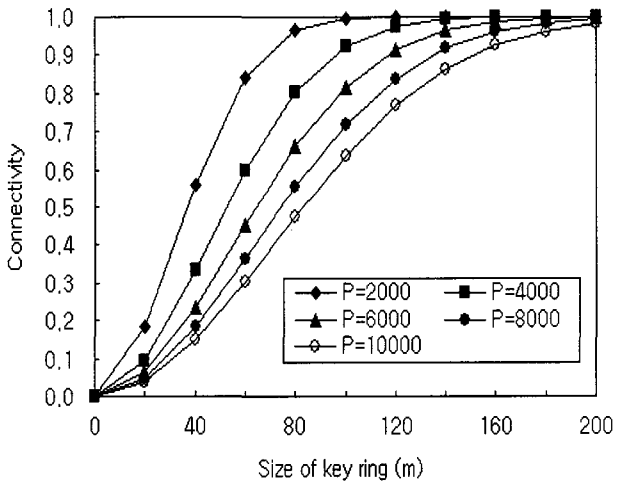
영향이 없다. 또한, 두 센서 노드가 서로 형성된 세션키를 확인하는 과정을 추가하였고, 각 센서 노드의 쌍에는 서로 다른 세션키가 부여되므로 세션키로 상대 노드를 인증할 수 있다.

5) 공유키의 노출 위험성은 이를 일회용 비밀키로 사용하여 취약점을 보완하였다. 두 센서 노드가 공유키를 이용하여 세션키를 교환한 후, 공격자가 각 센서 노드의 Id로부터 키의 Id를 생성하고, 이로부터 공유키를 구할 수 있어도 이는 초기에 세션키를 전송하기 위한 1회용 암호화키로만 사용되므로 세션키는 노출되지 않는다.

4.3 제안 프로토콜의 성능 분석

4.3.1 연결성과 세션키의 유일성

사전 키 정보 분배를 이용하는 기존의 프로토콜(랜덤 키 사전 분배 프로토콜, Q 복합키 기법, 노드 Id 기반의 키 생성 기법)에서는 연결성을 높이면 세션키의 보안성은 약화되는 문제가 있었다. 하지만, 제안 프로토콜에서는 공유키가 일회용으로 사용되므로 세션키의 보안에 영향없이 연결성을 높일 수 있다. 즉, 세션키가 공유키와 무관하게 랜덤하게 생성되므로 유일성을 제공한다



(그림 5) 제안 프로토콜의 연결성

제안 프로토콜이 세션키의 유일성을 보장하지만, 연결성을 높이기 위해 각 센서 노드에 할당하는 키 링의 크기(m)를 무조건 늘리면 각 센서 노드의 연산량과 메모리 요구를 증가시킨다. 따라서, m은 연결성과 센서 노드의 부하를 고려해서 선택되어야한다. 제안 프로토콜에서 연결성은 1회용 비밀키 생성에 의해 결정되고, 1회용 비밀키 생성은 노드 ID 기반 프로토콜의 세션키 생성 과정과 동일하다. 그러므로, 제안 프로토콜의 연결성은 노드 기반 프로토콜[8]에서 적어도 하나의 세션키가 존재할 확률($Pr[E]$)과 같다.

$$Pr[E] = 1 - \frac{\binom{P-m}{m}}{\binom{P}{m}}$$

P는 네트워크 키의 집합이고 m은 각 센서 노드에 할당되는 키 링의 크기이다. (그림 5)에서 보이듯이, 일회용 비밀키의 보안을 유지할 수 있는 수준의 네트워크 키의 집합(P)에 대해 제안 프로토콜의 연결성을 높일 수 있도록 각 센서 노드에 할당하는 키 링의 크기(m)를 적절하게 선택할 수 있다. P가 2000에서 10000사이이고, m이 200 이하인 경우에 제안 프로토콜의 연결성을 보이는 (그림 5)에서 P=2000, m=100이면 연결성을 99% 이상으로 얻을 수 있다. 즉, 사전 키 정보 분배를 이용하는 기존의 프로토콜에 비해 작은 m 값을 선택하여 각 센서 노드의 부하를 줄이면서 연결성을 높일 수 있다.

4.3.2 통신량

비밀키 생성 단계에서는 각 센서 노드가 자신의 노드 Id만 방송으로 전송하고, 세션키 교환 단계에서는 두 이웃 노드 사이에서 세션키와 세션키의 검증(verification) 정보만 전송된다.

따라서, 두 노드 사이의 전송 횟수는 세션키의 형성과 확인에 필수적인 4회로 전송 횟수를 최소화하였다. 각 전송의 유효 자료 크기는 노드 Id:16비트, 노드 Id:16비트, 암호화된 세션키:64비트, 1회용 비밀키로 생성된 메시지 인증 코드:64비트(노드 Id/키 Id 및 키 정보의 크기는 각각 16비트 및 64비트라 가정한다.)으로 최소화 되었으므로, 제안 프로토콜은 통신에 의한 에너지 소모를 극소화하면서 연결성과 세션키의 유일성을 제공하는 장점이 있다.

4.3.3 연산량

비밀키 생성단계에서는 수신된 노드 Id로부터 이웃 노드에 저장된 키의 Id 목록을 생성하고 일회용 키를 생성한다. 세션키 교환 단계에서는 세션키 생성, 세션키를 일회용 키로 암호/복호, 일회용 키를 세션키로 암호/복호한다.

따라서, 두 세션 노드가 수행하는 전체 연산은 키 Id 목록의 생성(m번×2회), 키 Id의 비교(m×m×2회), 일회용 키의 생성(해쉬×2회), 세션키의 생성(랜덤 번호 생성), 세션키의 암호 및 복호, 검증 정보의 암호 및 복호 이다. m 값을 적절히 선정하면 연산량은 증가되지 않는다.

4.3.4 배치 이전의 저장 정보

각 센서 노드는 배치되기 이전에 자신의 노드 Id(16비트), 자신에게 할당된 키 값(64비트×m)과 해당키의 Id(16비트×m)를 저장한다. 앞에서 분석한 바와 같이 높은 연결성을 유지하도록 키 링의 크기(m)를 적절히 선택하여 배치 이전의 저장 정보를 크게 줄일 수 있다.

제안 프로토콜의 특성을 요약하면 <표 2>와 같다.

〈표 2〉 제안 프로토콜의 특성

사전 분배 정보	세션키				통신		연산		서비스 거부	도청	노드 공격
	생성 기법	유일성	연결성	확인	키 생성	키 교환	키 생성	키 교환			
키 Id 생성 함수	랜덤 생성	O	O	O	· 노드 Id ×2	· 세션키 · 검증 정보	*	· 암호 ×2 · 복호 ×2	△	O	O

O : 우수, △ : 보통 X : 취약
* : 키 Id 생성:m×2회, 키 Id 비교:(m×m)×2회, 일회용 키 생성:2회, 세션키 생성
저장 정보량 : 노드 Id, 할당된 키 Id, 할당된 키

5. 결론 및 향후 연구

센서 네트워크는 수 백개에서 수 천개 이상의 센서 노드들로 구성되는 네트워크이다. 각 센서들은 자신의 통신 범위에 있는 이웃 센서들과 라디오파를 이용한 무선 통신을 하므로 공격에 매우 취약하다. 따라서, 보안을 요구하는 응용 분야에서는 상대 센서 노드를 인증하고 안전한 통신을 위해서 각 센서 노드 사이에 세션키(공유 비밀키)를 필요로 한다. 하지만, 센서 노드가 갖는 통신, 연산 능력 및 저장 용량의 제약으로 인해 전통적인 공개키 기법을 사용할 수 없고 또한 센서들의 배치가 완료되어야만 이웃 노드가 정해지므로, 이러한 특성에 따라 세션키를 형성하는 여러 기법들이 제안되었다.

본 연구에서는 센서 노드 사이의 세션키를 형성하는 기존 여러 기법들의 특성을 동일한 기준에서 비교하여 분석하였고, 이로부터 세션키 형성을 위한 개선된 프로토콜의 요구사항을 제시하였다. 이러한 연구는 최초로 시도되었다. 또한, 요구 사항을 만족시키며 기존의 세션키 형성 프로토콜들이 갖는 연결성, 세션키의 유일성, 공격 취약점 및 통신 과부하의 단점을 개선할 수 있는 세션키 형성 프로토콜들을 제안하였다. 제안 프로토콜은 첫 단계에서는 배치 이전에 분배된 정보를 이용하여 일회용 비밀키를 형성하므로 각 센서 노드의 키 링의 크기를 적절하게 선택하여 메모리 요구도 줄이면서 연결성을 99%이상으로 제공할 수 있다. 두 번째 단계에서는 세션키를 형성하고 일회용 키로 서로 합의토록 하여 세션키의 유일성을 보장한다. 제안 프로토콜은 센서 노드의 연산량은 줄이지 못하였지만, 세션키를 형성하고 확인하는데 필수적인 4번의 전송만을 필요로 하며 또한 전송 정보의 양도 최소화하여 에너지의 소비를 극소화 하였다, 하지만, 제안 프로토콜이 완전한 연결성(모든 이웃 노드가 직접 세션키를 형성할 수 있는)을 제공하지는 못하므로 이를 보안하기 위해 경로키(path key) 또는 마스터키를 함께 사용하도록 할 수 있다. 완전한 연결성과 세션키의 유일성을 모두 제공하기 위해 Blom의 제안 기법과 BROSK를 혼합한 두 단계 세션키 형성 프로토콜을 연구중이다.

참 고 문 헌

[1] A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM*, Vol.47, No.6, pp.53~57, 2004.

[2] N. H, R. Smith, and P. Bradford, "Security for Fixed Sensor Networks," *Proc. of ACMSE'04*, pp.212~213, 2004.

[3] Y. Wang, "Robust Key Establishment in Sensor Networks," *SIGMOD Record*, Vol.33, No.1, pp.14~19, 2004.

[4] A. Perrig, R. Szewczyk and D. Cuiller, "SPINS : Security Protocols for Sensor Networks," *Journal of Wireless Nets.*, Vol.8, No.5, pp.521~534, 2002.

[5] B. Lai, D. Hwang, S. Kim and I. Verbauwhede, "Reducing Radio Energy Consumption of Key Management Protocols for Wireless Sensor networks," *Poc. of ISLPED'04*, pp.351~356, 2004.

[6] Eschenhaur and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. of CCS'02*, pp.41~47, 2002.

[7] H. Chan, A. Perrig and D. Song, "Random Key Predi- stribution Schemes for Sensor Networks, *Proc. of 2003 IEEE Symposium on Security and Privacy(SP'03)*, pp.197~213, 2003.

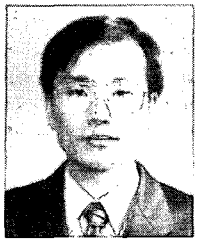
[8] R. Pietro, L. Mancini and A. Mei, "Random Key-Assignment for Secure Wireless Sensor Networks," *Proc. of 1st Workshop Security of Ad Hoc and Sensor Networks*, pp.62~71, 2003.

[9] R. Blom, "An Optimal class of symmetric key generation systems," *Proc. of EUROCRYPT84, Lecture Notes in Computer Science*, Springer-Verlag 209, pp.335~338, 1984.

[10] W. Du, J. Deng and J Katz, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks, *Proc. of CCS'03*, pp.27~31, 2003.

[11] D. Liu and P. Ning, "Location-based Pairwise Key Establishments for Static Sensor Networks," *Proc. of 1st Workshop Security of Ad Hoc and Sensor Networks*, pp.72~82, 2003.

[12] W. Du, J. Deng, and S. Chen, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," *Proc. of the IEEE INFOCOM'04*, pp.586~597, 2004.



김 종 은

e-mail : semico@dankook.ac.kr

1995년 단국대학교 전자계산학과(이학사)

1997년 단국대학교 대학원 전산통계학과 (이학석사)

2000년 단국대학교 대학원 박사과정 수료

2001년~2005년 단국대학교 정보컴퓨터학부 강의전임 교수

관심분야 : 컴퓨터 네트워크, 분산 시뮬레이션

조 경 산

e-mail : kscho@dankook.ac.kr

1979년 서울대학교 전자공학과(학사)

1981년 한국과학원 전기 및 전자공학과 (공학석사)

1988년 텍사스 대학원(오스틴) 전기 전산공학과(Ph.D.)

1988년~1990년 삼성전자 컴퓨터부분 책임연구원

1990년~현재 단국대학교 정보컴퓨터학부 교수

관심분야 : 컴퓨터 시스템, 컴퓨터 네트워크, 성능분석