무선 센서 네트워크를 위한 클러스터 기반의 효율적 키 관리 프로토콜

(A Cluster-based Efficient Key Management Protocol for Wireless Sensor Networks)

정 윤 수 † 황 윤 철 † 이 건 명 †† 이 상 호 ††
(Yoon-Su Jeong) (Yoon-Cheol Hwang) (Keon-Myung Lee) (Sang-Ho Lee)

요 약 안전한 무선 센서 네트워크 환경의 구축을 위하여 노드 간에 전송되는 메시지를 암호화하고 인증하는 것이 중요하다. 그러나 자원의 제약성 때문에 일반 네트워크에서 사용하는 Diffie-Hellman이나 공개키 기반 키 협의 방법은 적합하지 않다. 최근 활발히 연구가 진행되고 있는 사전 키 분배 방법은 q-composite 랜덤 키 사전 분배 방법을 사용하여 확률적으로 키를 분배하지만 센서 노드간의 공유키가 존재하지 않을 가능성이 매우 높고, 공유키를 발견하는데 시간과 에너지가 많이 소요되어 무선 네트워크 환경에 적합하지 않다. 이 논문에서는 확률적 키에 의존하지 않는 클러스터 기반의 새로운 키 관리 프로토콜을 제안한다. 제안 프로토콜은 부트스트랩(bootstrap) 동안 사전 배치 전에 센서간 공유하고 있는 공통키 사용을 통하여 센서의 키 전송/수용과정을 제거하였기 때문에 키 관리 효율성이 높다. 또한 네트워크 상에 존재하는 타협된 노드들을 안전하게 탐지할 수 있도록 lightweight 침입탐지 메커니즘 기능을 적용함으로써 안전성 문제를 해결한다.

키워드 : 무선 센서 네트워크, 클러스터, 키 관리 프로토콜

Abstract To achieve security in wireless sensor networks(WSN), it is important to be able to encrypt and authenticate messages sent among sensor nodes. Due to resource constraints, many key agreement schemes used in general networks such as Diffie-Hellman and public-key based schemes are not suitable for wireless sensor networks. The current pre-distribution of secret keys uses q-composite random key and it randomly allocates keys. But there exists high probability not to be public-key among sensor nodes and it is not efficient to find public-key because of the problem for time and energy consumption. To remove problems in pre-distribution of secret keys, we propose a new cryptographic key management protocol, which is based on the clustering scheme but does not depend on probabilistic key. The protocol can increase efficiency to manage keys because, before distributing keys in bootstrap, using public-key shared among nodes can remove processes to send or to receive key among sensors. Also, to find outcompromised nodes safely on network, it solves safety problem by applying a function of lightweight attack-detection mechanism.

Key words : Wireless sensor network, cluster, key management protocol

1. 서 론

컴퓨터와 통신기술의 최근 발전은 무선 센서 네트워크(WSN : Wireless Sensor Network)의 확대를 용이하게 하였다[1,2]. 센서 네트워크란 대규모의 초소형 장치로 구성된 환경으로 각 장치는 센서 노드로 불린다[3]. 이들 센서 노드는 주로 배터리로 전력을 공급받고, 통합 센서 장치로 구성되며 데이타 처리 능력과 단거리 무선 통신이 가능한 특징을 갖는다. SmartDust와 WINS가 센서 네트워크를 적용한 대표적 예이다[4].

WSN의 응용분야는 군대 센싱과 추적, 환경 모니터링, 환자 감시와 스마트 환경 등으로, 센서 노드가 위험 지역에 설치된 경우 보안성은 매우 중요하다. 예를 들

· 이 논문은 2005년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음
† 학생회원 : 충북대학교 컴퓨터과학과
bukmunro@netsec.cbnu.ac.kr
dolpin98@netsec.cbnu.ac.kr
†† 종신회원 : 충북대학교 전기전자컴퓨터공학부 교수
kmlee@chungbuk.ac.kr
shlee@chungbuk.ac.kr
논문접수 : 2005년 9월 21일
심사완료 : 2005년 12월 30일

면, 공격자는 쉽게 트래픽을 엿볼 수 있고, 주변 노드에게 잘못된 정보를 제공함으로써 네트워크 센서 노드로 흉내 낼 수도 있다. WSN에 보안성을 제공하려면 통신이 암호화되고 인증되어야 한다. 이러한 문제는 센서 노드 간의 안정적인 통신을 위하여 비밀키를 설정하도록 함으로써 부분적인 해결이 가능하다[5].

안전한 통신을 위하여 일반적인 네트워크를 대상으로 하는 키 관리 방법에 대한 다양한 연구가 진행되어 왔다[6-8]. 첫째, 신뢰된 인증서버에 의하여 키를 분배받는 방법으로 이는 센서 네트워크와 같이 구조적인 기반 구조가 없는 환경에서는 적용이 어렵다[9]. 둘째, 공개키 인증서를 활용한 비대칭 암호화 방법으로 한정된 계산력과 에너지로 구성된 센서 노드에서 Diffie-Hellman이나 RSA방법을 적용하는 것은 바람직하지 않다[10]. 마지막으로 사전 키 분배 방식은 센서 노드를 배치하기 전에 키 정보를 미리 저장하는 것으로 모든 정보가 사전에 결정되어야 하나 센서 노드의 설치는 임의적으로 이루어지므로 이러한 많은 사전 지식을 보유하는 것은 어렵다[11].

이 논문에서는 WSN 환경에서 주로 사용하고 있는 센서간 사전키 분배 방식에서의 확률적 키에 의존하는 문제를 키 재사용/추가에 유연성을 갖는 ID 기반 대칭키 기법을 확장하여 해결한다. 또한 센서 네트워크 환경에 적합한 최소 에너지로 키를 사용할 수 있는 클러스터 기반의 키 관리 기법을 제안한다. 제안 기법은 부트스트랩동안 사전 배치 전 센서간 공유한 공통키를 사용하여 센서의 키 전송/수용 과정을 제거하기 때문에 키 관리 측면에서 기존 기법보다 키관리 측면에서 효율적이다. 또한 네트워크상에 존재하는 타협된 노드들을 탐지하기 위해 lightweight 침입 탐지 메커니즘 기능을 적용함으로써 안전성 문제를 해결한다. 그리고 성능평가를 통해 노드 증가에 따른 오버헤드, 전체 센서 노드의 에너지 소비 현황과 클러스터당 소비되는 평균 통신 에너지 등을 평가한다.

이 논문의 구성은 다음과 같다. 2장에서는 지금까지 연구된 무선 네트워크 환경에서의 키 분배 방식을 분석하고, 3장에서는 클러스터 기반의 키 관리 프로토콜을 제안한다. 4장에서는 시뮬레이션 환경과 제안 프로토콜에 대한 보안평가와 성능 평가 결과를 기술하고 마지막으로 5장에서 결론을 내린다.

2. 관련 연구

WSN을 위한 키 분배 방법들은 크게 기반 시스템을 활용하거나 사전 분배 방식에 기반하고 있다. 특히 센서 네트워크 구조 형성에 필요한 에너지를 최소화하기 위한 연구가 활발하게 진행되고 있으며, 그 중 클러스터링 구조가 에너지 효율면에서 뛰어난 성능을 가지는 것으로 평가되고 있다.

2.1 제한된 센서 네트워크 환경을 위한 서브시스템 활용

이 방식은 서브 시스템 간의 통신을 위하여 게이트웨이 역할을 하는 BS(Base Station)를 가정함으로써 키 분배와 키 관리가 용이한 WSN을 구현하는 것이다. BS는 워크스테이션과 유사한 성능을 갖는 신뢰된 센서 노드로서 보안에 좀 더 강한 환경을 구성할 수 있다. 또한 중앙의 BS가 시스템 전체를 통제함으로써, 서브시스템은 인증되고 기밀성 있는 통신뿐만 아니라 인증된 브로드캐스팅을 지원할 수 있다. [12,13]의 키 관리 방법은 정기적으로 대칭키를 갱신함으로써 키 관리가 가능하도록 하였으나 키 분배 전후의 비밀성이 보장되지 않는 단점이 있으며, 실제로 강력한 기능을 가진 BS가 존재하기도 어려울 뿐만 아니라 대규모의 센서 네트워크 환경을 통제하는 것도 불가능하다.

2.2 확률적인 키 분배

확률적인 키 분배 방법과 랜덤 키 사전 분배 방법은 설치 전에 각 센서 노드가 대규모 키 풀로부터 부분 키 집합을 받는 것이다. 센서 노드들이 통신을 하기 위하여 임의의 두 노드는 그들의 키 집합 내에서 공통키를 찾고, 노드간 통신을 위한 공유키로 사용한다. Eschenauer-Gigor기법을 기반으로 [14]는 이들 방법에 q-composite 랜덤 키 사전 분배 방법을 적용하여 키 셋업에 대한 보안성을 강화하였다. 그러나 이 기법은 센서 네트워크 특성을 고려하지 않고, 확률적으로 랜덤하게 키를 분배하므로 센서 노드간의 공유키가 존재하지 않을 가능성이 매우 높다. 또한 공유키가 존재하더라도 공유키를 발견하는데 소용되는 시간과 에너지가 많아 에너지 사용이 효율적이지 못하다.

Blundo는 노드 사이의 충돌에 대해서 안전하도록 공통키를 계산하기 위해서 t 파티 그룹으로 여러 기법들을 제안했다[14-16]. 이러한 기법들은 메모리 소비가 그룹 멤버에 있지 않도록 통신 비용을 줄이는데 초점을 가진다. Perriget에 의해 제안된 SPINS는 센서 네트워크에 대해 특별하게 설계된 보안 구조이다[6]. SPINS에서 각 센서 노드는 베이스 스테이션과 함께 비밀키를 공유한다. 두 센서 노드들은 직접 비밀키를 만들지 못한다. 그러나 비밀키를 설정하기 위해서는 신뢰할만한 제3자의 베이스 스테이션을 사용해야 한다. Tatebayashi, Matsuzaki와 Newman은 이동 환경에서의 자원 소비를 위해 키 분배를 생각했으며, Park의 방식보다 더 향상된 방식이다[17,18]. 그러나 공유키를 발견하는데 시간과 에너지가 많이 소요되어 효율성면에서는 효율적이지 못하다.

2.3 클러스터 기반의 메시지 인증 방법

[8]에서는 두 통신 주체 사이에 키를 공유하기 전에 클러스터 헤드가 자신의 멤버 호스트들을 대신하여 인증을 수행하는 방법이 제안되었다. 이 방법에서는 임의의 두 클러스터 헤드가 각자 상대편 클러스터 헤드의 공개키를 이용하여 상호인증을 수행한다. 따라서 클러스터 헤드의 공개키가 먼저 모든 클러스터 헤드에 분배되어 있어야 한다. 클러스터 헤드 간 인증 후에 대칭키 기반의 세션키가 분배되고, 이는 다시 통신 주체인 멤버 호스트에게 분배된다.

이 방법은 클러스터 헤드들이 자신의 공개키를 모든 클러스터 헤드에게 분배해야 하므로 통신 오버헤드가 크다. 또한 두 멤버 호스트간 비밀키인 세션키 분배 시 헤드의 개인키로 암호화되어 해당 노드에 분배함으로써 세션키가 클러스터 내의 모든 호스트들에게 노출 될 수 있다.

2.4 ID-based threshold cryptography

Khalili[19]는 ID 기반 암호화 기법[20]의 편리성과 효율성, 임계치 암호화 기법[21]의 유연성 및 안전성의 이점을 결합하여 Ad Hoc 네트워크에서 각 노드의 공개키와 개인키를 생성하는 기법을 제안하였다[22]. 이 방식은 노드가 네트워크에 참여할 때 공통적으로 분배받는 마스터 공개키와 공개되어 있는 호스트의 ID로 해당 노드의 공개키를 유도하고 임계 개수만큼 주변 노드들로부터 ID에 해당하는 부분 개인키를 얻어내어 완전한 개인키를 획득한다. 그러나 이 방식은 비밀키를 요청하는 주체를 분명히 인증하지 못하므로 중간자 공격에 매우 취약하다.

3. 클러스터 기반의 키 관리 프로토콜 설계

이 논문에서 제안하는 클러스터 기반 키 관리 프로토콜은 대칭키 방식을 사용하며, 무선 센서 네트워크에서의 키 관리를 위해 위치 알고리즘으로 프로토콜을 표현한다. 또한 SN(Source Node)과 BS(Base Station)사이의 안전한 통신을 위해 사전에 설정된 키들을 이용하여 프로토콜을 제공한다.

3.1 가 정

키 관리 프로토콜에서 동작되는 각 객체들의 동작에 대한 주요 가정은 다음과 같다.

① 센서(Sensors)

센서가 신뢰성이 있다거나 악의적으로 사용할 수 있다는 가정을 만들지 않는다. 각 센서는 부트 스트랩동안 GPS등을 사용하여 센서의 위치를 탐지할 수 있고, 네트워크가 동작되는 동안 센서는 정지된다.

② 게이트웨이(Gateways)

네트워크상에 존재하는 모든 게이트들은 서로 직접 통신 할 수 있다. 이 때 게이트웨이간 통신은 브로드캐스트 통신을 한다고 가정한다. 또한 게이트웨이 사이에는 안전한 그룹통신을 한다고 가정한다. 통신에 사용되는 클러스터링 알고리즘[23]은 안전한 통신 설정을 할 수 있도록 쉽게 확장할 수 있다. 게이트웨이는 그룹 키 동의 프로토콜을 사용하여 그룹키를 설치할 수 있다. Carman은 [24]에서 이러한 프로토콜에 대해서 언급하고 있다.

③ 명령 노드(Command node)

명령노드는 센서 네트워크의 모든 노드들에 대해서 안전하고 신뢰적이라고 가정한다. 침입탐지 메커니즘은 명령 노드에서 완벽하게 동작되고, 약속된(타협된) 노드의 제거는 침입탐지 메커니즘에 따른다.

3.2 키 관리 프로토콜

이 논문에서 제안한 키 관리 프로토콜의 목적은 높은 에너지를 가지는 게이트 노드들간에 효율적으로 센서 네트워크를 클러스터 하는데 있다. 제안 프로토콜은 대칭키 메커니즘을 사용하면서 센서 네트워크의 생명주기 동안 키 분배/추가/폐기/갱신 등의 4개 하부 프로토콜이 수행된다. 각각의 세부적인 하부 프로토콜 접근방법은 키 관리와 관련있는 확장성 있는 계산을 수행하거나 키를 생성하는 센서를 호출하는 기능을 한다.

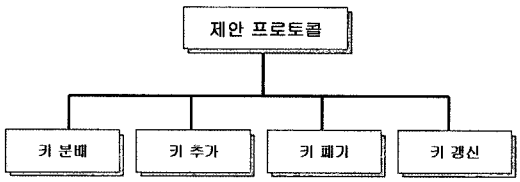

그림 1 제안 프로토콜 기본 구조도

3.2.1 키 분배

키 분배는 비밀키 메커니즘을 이용하고, 사전분배 방식을 통해 사전에 2개의 키를 센서에 저장한다. 센서에 저장된 키 중 하나는 게이트웨이와 공유하고 다른 하나는 명령(command) 노드와 공유한다. 일반적으로 센서들은 신뢰적이지 못하고 메모리 소비가 있어 적은수의 키만이 센서에 저장되지만 이런 점이 네트워크 보안에는 잇점이 된다.

게이트웨이는 메모리 자원이 풍부하고 많은 키를 저장할 수 있지만 게이트웨이를 완전히 신뢰할 수는 없다. 게이트웨이에 할당된 모든 키들은 전체 네트워크뿐만 아니라 단일 게이트에서 타협된다. 명령 노드는 안전하다고 가정하고 충분한 메모리를 가지고 있어 네트워크의 모든 비밀키들을 저장할 수 있다. 그리고, 센서키는 사전에 센서에 분배되도록 센서 메모리에 프로그램된다. 센서에 저장된 키들은 플래쉬 RAM에 저장될 수 있고 필요에 따라서는 지울 수 있다. 표 1은 프로토콜의 기술

표 1 프로토콜 주요 용어

개 념	설 명
C	명령 노드
G_i	게이트웨이 i
S_i	센서 노드 i
G	전체 게이트웨이
S	전체 센서노드
id_i	노드 인식 i
$nonce$	랜덤 난수 값
$sdata$	센서 위치 및 에너지 레벨 데이타
$E_K()$	키 K를 사용한 대칭 암호 함수
||	연계 동작자
G_h	복구에 사용될 헤드 게이트웨이

에 사용하는 주요 용어를 기술한 것이다.

명령 노드에 저장된 키들의 수는 |G|+|S|와 같다. |G|는 게이트의 수이고 |S|는 센서의 수이다. 각 게이트웨이는 키들을 저장하고 클러스터내 센서들과 명령 노드가 키를 공유한다. 또한 네트워크의 서로 다른 게이트웨이는 하나의 키를 공유하고 모든 게이트웨이는 그룹키를 공유한다. 키들이 사전 배치되기 때문에 브트스트랩 동안 센서측면에서 키 전송/수신 오버헤드가 없다.

센서 노드는 사전 분배 방식을 통해 센서에 셋팅되어 있는 2개의 대칭키를 표시하기 위해 키들에 대한 식별번호를 할당받는다. 식별정보의 무선전송이 안전하지 않을 경우 배치 전 제조 구문 동안에 새로 식별정보를 노드에 할당한다.

분배 기간에 각 게이트웨이는 임의로 |S|/|G|개의 키를 할당받는다. 각 게이트웨이는 클러스터 형성 알고리즘을 사용하여 클러스터를 형성하고 다른 게이트웨이로부터 클러스터 내에 있는 센서 키를 요구한다. 게이트 레벨에서 키가 교환 된 후 각 게이트웨이는 클러스터 내에 있는 센서의 키를 유지하고 나머지 키들은 제거한다. 이것은 게이트웨이가 수집한 클러스터의 키가 적에게 이용될 수 있기 때문에 초기구문에서는 필수적인 과정이다.

초기 구문 프로토콜의 동작과정은 다음과 같다.

① $S_i \rightarrow S$

$$id_{S_i}||id_{G_i}||E_m[sdata||nonce||k_c^i|h(k_c^i||sdata)]$$

각 센서는 공유된 키를 얻기 위해서 게이트웨이의 식별번호와 함께 사전 로드(preload)된다. 'hello' 메시지에 식별번호를 포함한 센서는 배치 후에 브로드캐스트한다.

② 클러스터링 과정

hello 메시지를 브로트캐스트 한 후 센서들은 클러스터링 메커니즘을 사용하여 센서들을 클러스터한다. 이 과정에서 사용되고 있는 클러스터링 메커니즘은 클러스터 재구성에 의해서만 적용된다.

③ $G_i \rightarrow G$

$$id_{G_i}||E_{K_m}[nonce||\{k_c^i,id_i\}||h(k_c^i||id_i)]$$

클러스터 형성 후에 각 G_i는 클러스터에 위치한 센서 설정 $\{k_c^i,id_i\}$를 표시하고 다른 게이트웨이에게 브로트캐스트한다. 브로드캐스트는 게이트웨이간 트래픽의 볼륨을 줄이는데 도움을 준다.

④ $G_i \leftarrow G_j$

$$E_{K_m}[nonce||(k_c^i, \{id_{S_K}\})]||ticket$$

각 G_j는 키 설정 $k_c^i, \{id_{S_K}\}$와 함께 G_i와 교체된다. 그리고 게이트웨이를 인식하기 위해 티켓(ticket)을 부여하여 전송한다. 이때, 티켓을 이용하는 것은 네트워크에 존재하는 타협된 노드들을 안전하게 탐지할 수 있는 역할을 하면서 lighweight 침입탐지 기능도 포함하고 있기 때문에 무선 네트워크의 안전성 문제를 해결하고 있다. 키 설정 중 $\{id_i\}$는 $\{id_j\}$의 하위 설정값이다.

⑤ $S_i \leftarrow G_i$

$$id_{G_i}||E_m[nonce||id_{G_i}||k_c^i||msg||h(k_c^i||msg)]||ticket$$

게이트웨이 G_i의 클러스터에 있는 각 센서 S_i은 게이트웨이 G_i에 할당하여 G_i로부터 메시지를 수신한다.

3.2.2 키 추가

네트워크에 추가되는 새로운 센서는 인위적으로 배치된다. 이 센서들은 클러스터에 미리 할당되지는 않지만 다른 센서와 동일하게 두개의 키를 미리 저장한다. 명령 노드는 새로 추가되는 센서의 키를 게이트웨이가 공유할 수 있도록 임의의 게이트웨이 G_H에 (identifier, key) 쌍의 리스트를 전송한다. G_H는 전체 게이트웨이 그룹이 아니며 타협의 위험을 줄이기 위해 사용된다.

① $C \rightarrow G_i$

$$E_{K_m}[nonce||(k_c^i, \{id_{S_K}\})]$$

더욱이, 추가된 각 센서 노드는 3.2.2절 초기단계 ①에서 'hello' 메시지를 브로드캐스트한다.

② $S_i \rightarrow S$

$$id_{S_i}||id_{G_i}||E_M[sdata||k_c^i||\text{nonce}||h(sdata||k_c^i)]$$

센서 노드 i는 주위 센서노드에게 G_i로부터 받은 정보를 전달한다.

③ 클러스터링 과정

정보를 전달받은 센서들은 클러스터링 메커니즘을 사용하여 센서들을 클러스터한다. 이 과정에서 사용되고 있는 클러스터링 메커니즘은 클러스터 재구성에 의해서만 적용된다.

④ $G_i \rightarrow G$

$$id_{G_i}||E_{K_m}[nonce||\{k_c^i, id_i\}||h(k_c^i||id_i)]$$

각각의 게이트웨이는 G의 게이트웨이 범위 안에 있는 센서들에게만 브로드캐스트 한다.

⑤ $G_i \leftarrow G_h$

$$E_{K_m}[nonce||(k_c^i, \{id_{S_K}\})]||ticket$$

G_h는 이러한 요청에 응답한다. 응답한 후에 각각의 새로운 센서 S_l은 게이트웨이 G_i에 할당한다.

⑥ $S_l \leftarrow G_i$

$$id_{G_i}||E_m[nonce||id_{G_i}||msg||k_c^i||h(k_c^i||msg)]||ticket$$

3.2.3 키 폐기(철회)

키 철회(노드 폐기)는 타협노드를 탐지한 후에 수행되며 침입탐지 메커니즘은 타협노드의 명령 노드에게 통보한다. 센서 그룹이 타협(compromised)된다면 게이트웨이에서 클러스터까지 명령 노드의 센서 리스트를 제거한다. 게이트웨이 (G_j) 키의 철회의 경우 명령 노드는 G로부터 G_j를 제거하고 타협하지 않은 헤드 게이트웨이 G_h를 선택한다. 선택된 G_h에는 센서간 새로운 게이트웨이 (G_i)의 식별번호와 G_i와 공유된 새로운 키를 보낸다. 또한, 새로운 게이트웨이-센서 비밀 키는 그룹 브로드캐스트를 통해 G_i에게 보낸다. 이런 과정 후에 재 클러스터링 단계를 수행한다.

① $C \rightarrow G_h$

$$nonce||\{id_{S_h}||id_{G_i}||\ E_m[nonce'||id_{S_h}||k_c^i||h(id_{S_h}||k_c^i)||$$
$$E_{K_m}[nonce''||id_{G_i}||h(id_{G_i}||k_c^i)]]\}_j$$

② 클러스터링 과정

메시지의 복호화가 성공적으로 이루어지면 센서는 G_i와 공유된 새로운 키를 수신받는다. 그러면, 새로운 게이트웨이 G_i는 받아들여지고, G_j로부터 오는 메시지는 다음부터 무시된다.

③ $G_i \rightarrow S_K$

$$E_m[nonce||id_{G_i}||k_c^i||h(id_{G_i}||k_c^i)]||ticket$$

3.2.4 키 갱신

확장기간 동안 동일한 암호키를 사용하는 것은 암호학적 위험을 초래할 수 있다. 센서 전지가 빨리 소모되는 네트워크에서는 센서 전지의 복구가 위협으로부터 적당히 무시될 수 있다[19]. 경우에 따라서는 다른 네트워크를 위해 암호 키를 새로 만들 필요가 있다[8]. 센서 키의 갱신을 수행하기 위해 명령 노드는 새로운 키를 생성하고 철회와 같은 경우가 발생할 경우 게이트웨이에게 키를 넘긴다. 연속적인 갱신이 이루어지는 동안에 시간 간격은 데이타 트래픽 볼륨, 암호학적 이론의 길이 그리고 게이트웨이에서 발생하는 여분의 처리 로드에 의존한다.

4. 시뮬레이션

이 절에서는 NS-2를 이용하여 제안 프로토콜의 성능 평가를 수행한다. 시뮬레이션을 위해 CMU(Carnegic Mellon University)의 Monarch Research Group에서 NS-2 시뮬레이터를 위해서 개발한 모델을 이용하였다[25].

4.1 환경설정

제안 프로토콜의 실험을 위하여 표 2의 실험 시나리오를 통해 임의적으로 생성되는 모델을 사용한다[2,14,18].

표 2 NS-2 실험 시나리오(Scenario of the ns-2 experiments)

노드의 수(Nodes number)	1000
크기(Scene)	1000m × 1000m
초기 에너지값(Initial energy)	0.5 joules
무선 범위(Wireless range)	200 m
버퍼(buffer)	50 packet
소스 수(Number of sources)	10
트래픽(Traffic)	4 pkts/s

실험에서 설정된 센서 필드의 크기는 $1{,}000m^2$ 이며 센서 노드의 개수는 1000개이다. 소스 노드는 초당 1개의 데이타 패킷을 싱크 노드에게 전송한다. 셀 사이즈는 $200m^2$으로 설정하고 600초 동안 실험을 수행한다. 그리고 각 센서의 초기에너지는 0.5 줄(Joule)의 에너지를 가지는 것으로 가정하고 버퍼의 크기는 50패킷의 크기를 가진다. 만약 노드의 에너지 레벨이 0줄이 되면 노드는 동작되지 않는다.

각 패킷은 패킷 전송동안 매 패킷 에너지를 계산하기 위해 갱신되는 에너지 필드를 가지며, 이때 패킷 드롭 확률은 0.01과 같다. 이것은 실제상황에 맞는 시뮬레이션을 만들기 위해서 사용되고 활동적인 에너지로부터 게이트 에너지 모델의 유추를 시뮬레이트하기 위해 사용된다.

4.2 실험 결과

이 절에서는 센서 노드 수의 변화에 따른 평균통신 에너지, 오버헤드, 센서 노드의 에너지 소비 비율 등을 시뮬레이션을 통해 분석하였다.

4.2.1 안전성 분석

{IP address, key} 묶음 보안은 비밀키 암호 알고리즘 보안과 해쉬함수의 두 번째 사전 이미지 저항 속성에 의존한다. 이러한 두 가지 가정은 센서 네트워크 환경에서 매우 실용적이다. 예를 들어 비밀 키 암호시스템은 제안 시스템의 보안 요구사항에 효과적이다. 더욱이 MD5나 SHA-1이 판독되는 두 번째 사전 이미지 저항

과 64비트의 출력을 가지는 해쉬함수는 (만일 우리가 64비트중 하나를 보관하고 있다면) 공격자가 주어진 IP 지역의 두 번째 비밀키를 찾기 위해 평균 2^{62}번 시도한다.

이러한 작업은 공격자가 빠른 작업처리를 하지 못하게 할 뿐만 아니라 공격자가 시도한 비밀키에 대해 인위적인 추측이 불가능하다. 만약 공격자가 해쉬함수 입력에 대한 추측을 한다면 두 번째 pre-image resistant 해쉬함수를 빠르게 처리하여 실제 공격자가 사용하지 못하도록 한다.

해쉬함수에 대한 생일공격이 제안 프로토콜의 함수 사이에서 발생하더라도 제안 프로토콜은 입력이 2^{32}시도만큼 유일 분포로 나타나고, 임의 두 노드 사이에서 충돌할 노드의 수는 10^9노드 순서에 의해서만 존재하기 때문에 제안 프로토콜은 해쉬함수에 대한 생일공격에 안전하다.

4.2.2 효율성 분석

그림 2는 노드 증가에 따른 트래픽 오버헤드를 평가한 결과이다. 노드 수가 25보다 적을 경우 제안기법은 기존의 사전분배 방식보다 오버헤드가 4% 높지만 노드 수가 25보다 클 경우 사전분배 방식이 제안기법보다 오버헤드가 평균 1.5%씩 높게 나타났다. 따라서 전체 트래픽 오버헤드 측면에서 볼 때 사전분배 방식이 제안기법보다 평균 0.33% 높은 트래픽 오버헤드를 가짐을 알 수 있다.

이 노드 수에 따른 실험을 통해 얻은 결과는 다음의 3가지이다. 첫째, 트래픽 오버헤드는 노드 수에 따라 증가하고 많은 제어 패킷이 필요하다. 두 번째, 트래픽 오버헤드는 노드 증가 비율과는 다르게 일정한 크기로 증가하지 않는다. 그 이유는 네트워크의 제한된 크기로 인해 노드 수가 선형적으로 증가하지 않기 때문이다. 셋째, 기존 기법의 경우처럼 트래픽 오버헤드는 시뮬레이션에 사용된 서로 다른 트래픽 패턴에 의해서 이루어진다. 노드는 노드를 보내는 모든 트래픽 패킷에 의해서 트래픽 키를 추가한다. 그리고, 전체 오버헤드는 주로

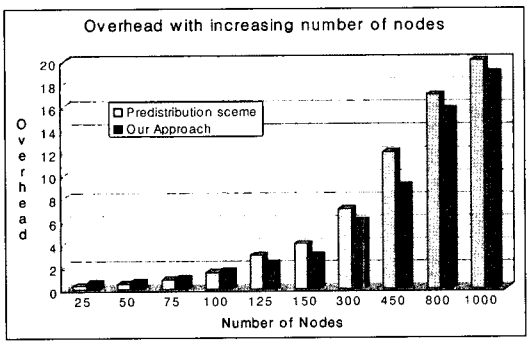

그림 2 노드 증가에 따른 오버헤드

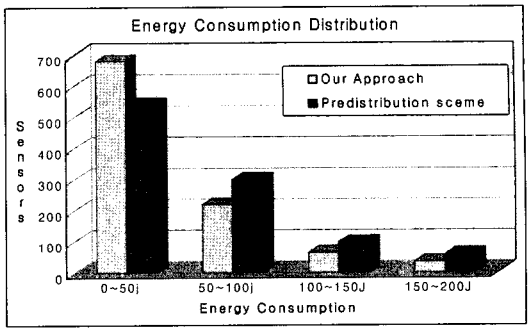

그림 3 에너지 소비 분배

데이타 소스의 수와 노드의 트래픽 모델에 의해 주로 결정된다.

그림 3은 실험에 사용된 1000개 센서들의 에너지 소비 비율을 나타내고 있다. 그림 3의 결과처럼 제안 방식에서는 전체 센서노드의 60%이상이 50J보다 적은 에너지를 사용하고 있으며, 50~100J, 100~150J, 150~200J의 에너지를 소비하는 센서들도 각각 22%, 6.5%, 3.5%로 나타났다. 반면 사전분배 방법은 0~50J, 50~100J, 100~150J, 150~200J의 에너지를 소비하는 센서들이 각각 54%, 30%, 10%, 6%로 나타났다. 이 결과는 게이트웨이의 밀집상태와 수행상태에 따라 평균 에너지 소비가 다름을 보여준다. 특히 사전분배 방식은 시간이 지남에 따라 처리해야 할 데이타가 늘어나기 때문에 제안기법보다 많은 에너지를 소비하는 노드들이 필요하다.

그림 4는 클러스터 내의 게이트웨이와 모든 센서 사이의 통신으로부터 요구된 평균 통신 에너지를 측정한 결과이다. 통신 에너지는 직접적으로 두 노드 사이의 거리에 비례적이다. 그러나 클러스터 수의 증가에 따른 평균 통신 에너지 비율은 반비례적이다.

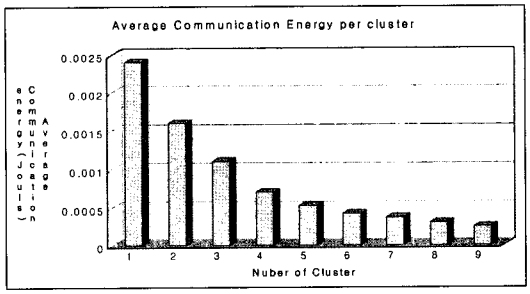

그림 4 클러스터당 평균 통신 에너지

이 논문에서는 그림 4의 결과를 통해 크게 2가지 특성을 도출할 수 있다. 첫째, 클러스터가 짧은 거리(short-distance) 기반으로 형성된다면 소비된 평균 에너지는 최소화되겠지만 로드는 균형잡히지 않는다. 둘

째, 짧은 거리로 클러스터된 센서들은 통신을 시작하면서 최소의 통신 에너지를 소비하려고 하지만 재 클러스터링 과정을 통해 오버헤드 에너지는 더 소비된다.

5. 결 론

무선 센서 네트워크 환경에서 보안성을 확보하기 위하여, 센서 노드간에 전송된 메시지를 암호화하고 인증하는 것이 중요시 되고 있다. 이 논문에서는 WSN 환경에서 센서간 사전키 분배 문제를 해결하기 위하여 확률적 키에 의존하지 않는 새로운 키 관리 프로토콜을 제안하였다. 제안 프로토콜은 부트스트랩동안 노드간 공유된 공통키를 이용하여 센서의 키 전송/수용 과정을 제거하였기 때문에 키 관리 측면에서 효율적이다. 또한 네트워크상에 존재하는 타협된 노드들을 탐지하기 위해 lightweight 침입탐지 메커니즘 기능을 프로토콜에 적용하여 노드의 안전성 문제를 해결하였다.

노드 증가에 따른 트래픽 오버헤드 평가 결과 사전분배 방식이 제안기법보다 전체 평균 오버헤드가 0.33% 높게 나타났다. 이 결과는 네트워크 크기로 인해 노드 수가 선형적으로 증가하지 않으며 시뮬레이션에 사용된 표 2의 트래픽 값이 서로 다르기 때문에 발생한다. 그리고 전체 센서들의 에너지 소비 비율에서도 50줄 미만의 센서들을 60%이상 요구하는 제안기법이 50줄 이상의 에너지 소비를 요구하는 사전 분배방식보다 전체 에너지 소비 측면에서 효율적이다.

앞으로 제안 기법에 센서노드의 중복 비용 부분을 함께 접목시키는 방안과 재클러스터링을 통하여 헤드노드 결함문제를 해결하는 대표적 알고리즘인 LEACH(Low Energy Adaptive Clustering Hierarchy)를 개선하는 방식 등에 대한 연구가 필요하다.

참 고 문 헌

[1] M. Horton, et al., "Mica: The commerciatlization of microsensor motes," Sensors Online Magazine, April 2002. http://www.sensorsmag.com/articles/0402/40/main/shtml

[2] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy Efficient Communication protocol for Wireless Microsensor Networks," Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, pp. 3005-3014, Jan. 2000.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, August 2002.

[4] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for smart dust," in Proceedings of the 5th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom), 1999, pp. 483-492.

[5] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, pp. 644-654, November 1976.

[6] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security protocols for sensor networks," in Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, July 2001, pp. 189-199.

[7] W. Fumy and P. Landrock, "Principles of key management," IEEE Journal of Selected Areas in Communications, vol. 11, pp. 785-793, June 1993.

[8] T. Dimitriou, I. Krontiris, and F. Nikakis, "Key establishment in sensor networks with resiliency against node capture and replication," December 2003. Submitted to 5th ACM Symposium on Mobile Ad Hoc Networking and Computing, (MobiHoc) 2004.

[9] B. C. Neuman and T. Tso, "Kerberos: An authentication service for computer networks," IEEE Communications, vol. 32, no. 9, pp. 33-38, September 1994.

[10] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[11] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, November 18-22, 2002, pp. 41-47.

[12] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti. "Secure pebblenets," In Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing, ACM Press, 2001, pp. 156-163.

[13] 김복순, 조기환, 이행곤, 박병연, "센서 네트워크에서 랜덤 키 체인을 활용한 단대단 키 협의 방안", 한국통신학회 추계종합 학술발표논문집, 28, 2003. pp. 1-12.

[14] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for Sensor networks," In IEEE Symposium on Research in Security and Privacy, May, 2003, pp. 197-213.

[15] L. Echenauer and V. D. Gligor, "A Key-Management scheme for Distributed sensor networks," In Proceedings of the 9th Computer Communication Security, Nov. 2002, pp. 41-47.

[16] S. Zhu, S. Setia, and S. Jajodia, "A distributed group key managemet protocol for ad hoc networks," Unpublished manuscript, George Mason University, Dec. 2002.

[17] Gupta G, Younis M, "Performance Evaluation of Load-Balanced Clustering in Wireless Sensor

Networks" In the proc. of 10th International Conference on Telecommunications (ICT 2003), Tahiti, French Polynesia, Feb. 2003.
[18] M. Tatebayashi, N. Matsuzaki, and D. B. Newman, "Key distribution protocol for digital mobile communication systems," Advances in Cryptology-CRYPTO'89, pp. 324-334, 1989, INCS Volume 435, Springer-verlag.
[19] A. Khalili, et al., "Toward Secure key Distribution in Truly Ad-Hoc Networks," IEEE SAINT'03, pp. 342-346, Jan. 2003.
[20] D. Boneh, et al., "Identity-based Encryption from the Weil Pairing," CRYPTO 2001, vol. 2139, pp. 213-229, Aug. 2001.
[21] l. zHOU, ET AL., "Securing Ad Hoc Networks," IEEE Network Magazine, 13(6), Nov./Dec. 1999.
[22] L. Venkatraman et al., "A Novel Authentication Schemes Ad Hoc Networks," IEEE WCNC' 2000, vol.3, pp. 1268-1273, 2000.
[23] C. Park, K. Kurosawa, T. Okamoto, and S. Tsujii, "On key distrubution and authentication in mobile radio networks," Advances in Cryptology - euroCrypt'93, pp. 461-465, 1993, INCS Volume 765, Springer-verlag.
[24] D. Carman, P. Kruus, and B. Matt, "Constraints and approaches for distributed sensor network security," Tech. Rep. 00-010, NAI Labs, September 2000. http://download.nai.com/products/media/nai/zip/nailabs-report-00-010-final.zip
[25] Network simulator. Available in http://www.isi.edu/nsnam/ns, January 2003.

정 윤 수
1998년 2월 청주대학교 졸업(이학사) 2000년 2월 충북대학교 대학원 전자계산학과 졸업(이학석사). 2003년 3월~현재 충북대 전기전자컴퓨터공학부 전자계산학과 박사수료. 관심분야는 암호이론, 정보보호, Network Security, 이동통신보안, 전자상거래보안

황 윤 철
1994년 한남대학교 전자계산공학과. 1996년 한남대학교 전자계산공학과(공학석사) 1999년~현재 충북대 전기전자컴퓨터공학부 전자계산학과 박사수료. 관심분야는 인터넷, 정보보호, Network Security

이 건 명
1990년 한국과학기술원 전산학과 학사 1992년 한국과학기술원 전산학과 석사 1995년 한국과학기술원 전산학과 박사 1995년 5월~1996년 4월 프랑스 INSA de Lyon 연구원. 1996년 5월~1996년 8월 미국 PSI 연구원. 1996년 9월~현재 충북대학교 컴퓨터과학과 조교수. 관심분야는 에이전트 시스템, 전자상거래, 무선 인터넷 응용, 데이타 마이닝, 소프트 컴퓨팅

이 상 호
1976년 숭실대학교 전자계산학과 졸업 1981년 숭실대학교 전자계산학과 졸업(MS). 1989년 숭실대학교 전자계산학과 졸업(PHD). 1976년 1월~1979년 5월 한국전력 전자계산소. 1981년 6월~현재 충북대학교 전기전자컴퓨터공학부 교수. 관심분야는 Protocol Engineering, Network Security, Network Management, Network Architecture