계층적 센서 네트워크를 위한 개선된 키 관리 기법

이원진*° 김현성** 김은주* 전일수*
*금오공과대학교 전자통신공학과, **경일대학교 컴퓨터공학부
{wjlee°.candycore, isjeon}@kumoh.ar.kr, kim@kiu.ac.kr

Improved Key Management Scheme for Hierarchical Sensor Network

Won-Jin Lee*° Hyun-Sung Kim** Eun-Ju Kim* Il-Soo Jeon*
*Dept. of Electronic Engineering, Kumoh National Institute of Technology
**School of Computer Engineering, Kyungil University

요 약

최근 Chen등[1]은 계층적 센서 네트워크 환경을 위한 키 관리 기법을 제안하였다. 본 논문에서는 Chen등의 기법이 센서 노드의 추가와 재배치 시 직계 부모 노드가 양단키(pair-wise key)를 생성해서 새롭게 추가와 재배치되는 자식노드에게 아무런 보안기법 없이 양단키를 전송하므로써, 보안에 취약함을 보여준다. 이러한 문제를 해결하기 위해 본 논문에서는 싱크노드가 추가 및 재배치되는 센서 노드의 양단키를 사전에 생성하여 전송하고 추가 및 재배치되는 노드의 부모노드에게 생성한 키를 전송하는 개선된 키 관리 기법을 제안한다.

1. 서 론

오늘날 센서 네트워크는 다양한 어플리케이션에서 이용되고 있다. 센서 네트워크는 자원이 제한된 작은 센서 노드들로 구성된다. 이러한 센서 노드들은 MEMS (Micro-Electro-Mechanical System) 기술과 디지털 공학, 무선통신 등의 기술 발전으로 인해 크기가 매우 작아지고 향상된 무선 통신 능력을 가지게 되었다[2].

점차 센서 네트워크 기반의 서비스에 대한 기술이 구체화되어지면서 센서 네트워크상에서 보안에 대한 필요성이 대두되었고 이에 보안 기술에 대한 연구[3-8]가 활발해지고 있다. 이러한 센서 네트워크를 구성하기 위해 가장 먼저 고려해야 할 보안 요구 사항은 암호학적 키 설정 문제이다. 이러한 키는 센서 노드 사이의 인증이나 센서 노드 사이에서 교환되는 정보의 보호를 제공하는데 사용된다.

센서 네트워크 환경에 대한 키 관리 기법들[4,5,7,8]이 다양하게 제안되었다. 센서 노드는 저전력, 저비용, 좁은 범위의 특징을 가지며 파워, 메모리 용량, 연산처리 능력 등과 같은 물리적 제약을 가지므로, 전통적인 키 관리 기법을 적용하기 힘들다. 센서 네트워크 환경에서의 초기 키 관리 기법은 센서 네트워크 전체가 하나의 키를 공유하는 것이다. 그러나 이 방법은 네트워크 내의 단지 하나의 노드가 공격당함으로써 공유된 비밀키가 드러날 수 있고, 이에 따라 안전한 통신을 할수 없게 된다. 키 관리기법의 또 다른 방법은 하나의 양단키를 링크키(link key)들을 설정하는 데 사용하는 방법이 있다. 그러나 이 방법도 초기 키 설정 이후, 새로운 노드의 추가가 불가능하다는 단점이 존재한다[4][5].다른 키 관리 기법으로는 사전에 각각의 노드의 쌍 사이에 유일한 대칭키를 공유하는 방법이 있다. n개의 노드를 가지는 센서 네트워크에서, 각각의 노드는 n-1개의 키를 저장해야 하고, n(n-1)/2개의 키들이 설정되어야 한다. 이 방법은 전체 노드의 키를 저장해야 하는 메모리 요구사항 때문에, 센서 네트워크 환경에서는 비현실적이다[6]. 현재 많이 연구되고 있는 키 관리 기법은 랜덤키 사전 분배(random key predistribution)를 유망한 양단키 설정 스킴으로 간주하는 키 관리 기법들[4,5,7,8]을 제시하고 있다. 하지만, 이 방법은 노드 전복(compromise) 공격에 취약하다. 뿐만 아니라, 최적의 라우팅 루트로 통신할 수 있는 두 개의 노드가 양단키를 가지고 있지 않은 경우에는 비효율적인 루트로 돌아가야만 하는 문제점이 존재한다.

최근에는 Chen등[1]이 계층적 구조의 센서 네트워크 환경에서 4가지 형태의 키를 이용하여, 부모와 자식사이의 통신과 같은 그룹 멤버간의 통신을 보여주었고, 노드 추가, 재배치, 삭제의 경우 키 관리 기법을 제안하였다.

본 논문에서는 Chen등[1]이 제시한 키 관리 기법에서 새로운 센서 노드의 추가(addition) 및 재배치(replacement) 경우 보안에 취약함을 보이고, 또한 그 취약함을 해결하기 위한 개선된 키 관리 기법을 제안한다. 본 논문에서는 센서 네트워크 환경에 새로운 센서 노드가 배치되기 전에 싱크노드가 먼저 추가 및 재배치되는 센서 노드의 양단키(pair-wise key)를 사전에 생성하여 추가 및 재배치되는 센서 노드에게 전송하고 그 노드는 키를 저장한다. 그리고 싱크노드는 새롭게 추가 및 재배치되는 노드의 부모 노드에게 생성한 양단키를 전송하여 추가 및 재배치를 할 때 안전한 양단키 전송을 수행 한다 .

본 논문의 구성은 다음과 같다. 2장에서는 키 관리 기법과 Chen[1]등이 제시한 기법에 대해서 살펴보고, 3장에서는 기존의 문제점을 해결하기 위한 개선된 키 관리 기법을 제안하고, 4장에서는 기존의 연구와 본 논문에서 제시한 기법을 비교 분석한다. 마지막으로 5장에서는 결론을 제시한다.

2. 관련연구

본 장에서는 Chen[1]등이 제시한 키 관리 기법에 대해 살펴본다.

Chen등[1]은 계층적 센서 네트워크에서 키 관리기법을 제시하였다. 그림 1은 Chen등이 제시한 계층적 센서 네트워크의 기본 구조이며, 그림 1에서 하나의 타원형은 그룹을 의미한다. 그리고 같은 그룹 내의 그룹 멤버는 직접적인(directly)통신이 가능하고, 자식 노드들과 부모 노드 사이에서도 직접적인 통신이 가능하다고 가정하였다.

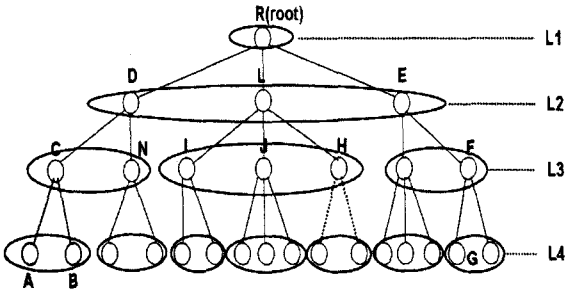


그림 1. Chen등이 제시한 계층적 센서네트워크의 구조

Chen등의 키 관리 기법은 대칭키 암호화 방식을 기반으로 하는 사전 키 분배 방식 이용하고, 대칭키 암호화 방식을 이용하여 안전한 통신을 제공한다. 키 관리 기법은 다음 4 가지 형태의 키를 사용한다.

- 그룹키(Group key) : 각각의 그룹은 그룹 멤버 노드 간의 통신을 위한 유일한 하나의 키이다.
- 상위레벨 양단키(Uplevel Pair-wise key) : 루트 노드(root node)를 제외한 그룹의 각 멤버 노드들이 자신의 부모 노드와 공유하는 하나의 비밀키이다.
- 하위레벨 그룹키(Downlevel Group Key) : 종단노드(leaf node)를 제외한 모든 센서 노드들은 자신의 자식 노드들간의 통신을 위한 유일한 하나의 키이다.
- 하위레벨 양단키(Downlevel Pair-wise Key) : 종단노드를 제외한 모든 센서 노드들은 자신과 각각의 자식 노드들에 대해 하나씩 공유하는 비밀키이다.

만약 A가 다른 그룹의 G에게 전송을 하기 위해서는 4개의 양단키와 D와 E 사이의 하나의 그룹키를 다음과 같이 이용한다. 그림 1에서 이러한 키들을 이용한 통신 형태를 볼 수 있다.

$$A \rightarrow \{C\} : \{m\}_{K_{AC}}$$
$$C \rightarrow \{D\} : \{m\}_{K_{CD}}$$
$$D \rightarrow \{E\} : \{m\}_{K_{G(DE)}}$$
$$E \rightarrow \{F\} : \{m\}_{K_{EF}}$$
$$F \rightarrow \{G\} : \{m\}_{K_{FG}}$$

위에 4가지의 키는 센서 네트워크 환경에 배치되기 전에 사전 분배 된다. 센서 노드의 추가 및 재배치가 필요한 경우 노드의 키 생성 , 삭제 및 갱신은 다음과 같다.

- 센서 노드의 추가
  그림 1에서 새로운 노드 H가 $L3$ 위치에 추가 되었다고 할 때, 부모 노드 L은 H와의 하위레벨 양단키(K_{LH})를 생성해서 H에게 전송한다. 또한 H는 기존 그룹 멤버(노드) I, J와 통신을 위해서 그룹키($K_{G\{IJ\}}$)를 L로부터 전송 받는다. 이때 L은 H와 공유하는 하위레벨 양단키(K_{LH})로 그룹키($K_{G\{IJ\}}$)를 암호화해서 전송한다. 그리고 H의 자식 노드는 양단키와 그룹키의 정보를 사전에 저장하고 배치된다.

$$L \rightarrow \{H\} : \{K_{G\{IJ\}}\}_{K_{LH}}$$

- 센서 노드의 재배치(교체)
  그림 1에서 기존의 노드 C가 새로운 노드 M으로 재배치된다고 할 때 부모 노드 D는 새로운 자식 노드 M과 공유하는 하위레벨 양단키(K_{DM})를 전송하고, M과 N사이에 새로운 그룹키($K_{G\{MN\}}$)를 생성하여 전송하는데, 이때 M, N과 공유하는 각각의 양단키로 암호화해서 전송한다.

$$D \rightarrow \{M\} : \{K_{G\{MN\}}\}_{K_{DM}}$$
$$D \rightarrow \{N\} : \{K_{G\{MN\}}\}_{K_{DN}}$$

여기에서 M이 자식 노드 A, B를 가질 경우에, 각각의 하위레벨 양단키(K_{MA} K_{MB})와 그룹키$K_{G\{AB\}}$를 변경해서 전송한다.

$$M \rightarrow \{A\} : \{K_{G\{AB\}}\}_{K_{MA}}$$
$$M \rightarrow \{B\} : \{K_{G\{AB\}}\}_{K_{MB}}$$

3. 개선된 키 관리 기법

본 장에서는 Chen등[1]이 제시한 기법이 가지는 보안의 취약점과 이를 개선한 계층적 센서 네트워크에서 키 관리 기법을 제안한다. 제안한 키 관리 기법은 센서 노드 추가 경우에는 하위레벨 양단키 전송 단계와 그룹키 전송 단계로 구분된다. 그리고 센서 노드 재배치 경우에는 재배치 된 노드의 키 관리 단계가 포함된 세 단계로 구분한다.

3.1 Chen등의 보안 취약점

Chen등이 제시한 키 관리 기법 중에서 센서 노드의 추가 및 재배치 시에 보안의 취약점이 다음과 같이 발생한다.

- 센서 노드의 추가 경우
  새로운 센서 노드의 추가 시 부모 노드는 하위레벨 양단키를 생성하여, 자식노드에게 전송하고, 자

식노드는 전송 받은 양단키를 저장한다. 여기서 부모 노드가 양단키를 생성해서 자식노드에게 전송 할 때, 아무런 보안기법 없이 양단키를 전송하기 때문에, 보안에 취약하다.

- 센서 노드의 재배치 경우
  기존의 센서 노드를 새로운 센서 노드로 교체 할 경우에도 센서 노드의 추가와 같은 보안의 취약점이 발생한다. 즉 부모 노드는 하위 레벨 양단키를 생성해서 교체될 센서 노드에게 전송 할 때, 보안기법 없이 양단키를 전송하므로, 보안의 취약점이 존재한다. 또한 교체된 센서 노드가 자식 노드를 가지는 경우에도 자식 노드에게 양단키 전송할 때도 같은 보안의 취약점을 가진다.

3.2 제안한 키 관리 기술

본 절에서는 제안된 키 관리 기법을 이용하여 안전한 메시지 전송에 대해 살펴본다. 본 논문에서 최상의 노드를 싱크노드(sink node)라 명칭하고, 싱크 노드 안전하며, 모든 자식 노드들의 양단키를 생성하여 사전에 분배한다고 가정한다.

그리고 기존의 키 관리기법에서처럼 표기법은 다음과 같이 정의한다.

$$s \rightarrow \{d\} : \{m\}_k$$

여기에서 s는 소스 센서 노드, d는 목적지 센서 노드, m은 키 k로 암호화된 메시지이다.

3.2.1 센서 노드의 추가

본 논문에서는 새로운 센서 노드를 센서 네트워크 환경에 추가하기 위해서 다음과 같이 하위레벨 양단키 전송 단계와 그룹키 전송 단계로 구분한다. 특히 Chen등이 제시한 기법의 보안의 취약점을 개선하기 위해서 하위레벨 양단키 전송 단계에서 추가를 원하는 센서 노드와 직계 부모 노드간의 양단키를 싱크 노드가 생성 및 전송하여 안전한 통신을 제공한다.

(1) 하위레벨 양단키 전송 단계

그림 1에서처럼 센서 네트워크 환경에 새로운 센서 노드 H를 추가 할 경우 다음과 같은 과정을 수행한다.

$$R \rightarrow \{H\} : \{K_{LH}\} \quad -①$$
$$R \rightarrow \{L\} : \{K_{LH}\}_{K_{RL}} \quad -②$$

① 새로운 센서 노드의 추가 위해서 먼저 싱크노드 R이 추가될 센서 노드 H에게 직계 부모 노드 L과 공유하는 양단키(K_{LH})를 생성해서, 센서 노드 H에게 배치되기 전에 저장한다.

② 싱크 노드 R은 새롭게 추가될 노드 H의 직계 부모 노드 L에게도 양단키(K_{LH})를 하위레벨 양단키(K_{RL})로 암호화해서 전송한다.

(2) 그룹키 전송 단계

싱크 노드 R로부터 양단키를 받은 노드 H는 양단키를 저장한 후 센서 네트워크 환경에 배치되고 난 후, 다음과 같이 그룹키를 전송한다.

$$L \rightarrow \{H\} : \{K_{G(I,J)}\}_{K_{LH}} \quad -③$$

③ 하위레벨 양단키 전송 단계에서 싱크노드로부터 양단키(K_{LH})를 전송 받은 L은 H에게 같은 그룹 멤버인 I, J와 직접 통신하기 위해 필요한 그룹키($K_{G(I,J)}$)를 전송한다. 이때 양단키(K_{LH})로 하위레벨 그룹키($K_{G(I,J)}$)를 암호화하여 전송한다.

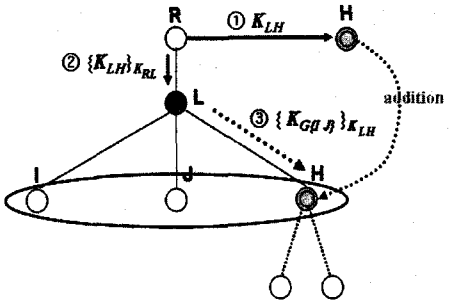


그림 2. 제안한 센서 노드의 추가 기법

3.2.2 센서 노드의 재배치

센서 네트워크 환경에서는 센서 노드가 적의 의해 물리적 위험에 빠졌거나 그 기능을 다하지 못하여 오작동이 생길 경우 센서 노드의 재배치를 수행한다. 센서 노드 재배치의 경우에는 세 단계로 구분하여 키 관리가 이루어지며, 노드의 추가와 삭제가 수행된다.

(1) 하위레벨 양단키 전송 단계

그림 1에서처럼 센서 네트워크 환경에서 기존의 노드 C를 새로운 노드 M으로 재배치하기 위해서는 다음과 같은 과정을 수행한다.

$$R \rightarrow \{M\} : \{K_{DM}\} \quad -①$$
$$R \rightarrow \{D\} : \{K_{DM}\}_{K_{RD}} \quad -②$$

① 안전한 키 전송을 위해 싱크노드 R은 교체될 새로운 노드 M에게 부모 노드 D와 공유하는 양단키(K_{DM})를 생성하여, 센서 노드 M이 배치되기 전에 저장한다.

② 싱크 노드 R은 새롭게 교체될 센서 노드 M의 직계 부모 노드 D에게도 양단키(K_{DM})를 하위레벨 양단키(K_{RD})로 암호화 하여 전송한다.

(2) 그룹키 전송 단계

하위레벨 양단키 전송 단계에서 싱크 노드로부터 키 전송 받은 부모 노드D는 자식 노드 M 과 N에게 다음의

키 정보를 전송한다.

$$D \rightarrow \{M\} : \{K_{G(MN)}\}_{K_{DM}} \quad -③$$
$$D \rightarrow \{N\} : \{K_{G(MN)}\}_{K_{DN}} \quad -④$$

③, ④ 부모 노드 D는 같은 그룹 멤버인 자식 노드 M과 N에게 그룹키($K_{G(M,N)}$)를 전송하기 위해서 각각의 자식 노드와 공유하는 하위레벨 양단키(K_{DM}, K_{DN})로 그룹키를 암호화해서 전송한다. 이후 부모 노드 D는 기존에 노드 C와 관련된 키 정보를 삭제한다.

(3) 재배치 된 노드의 키 관리 단계

재배치 된 노드가 하위 자식 노드를 가지고 있을 경우 키 관리 작업을 수행하기 위해 본 논문에서 ①'과 같이 재배치를 원하는 센서 노드는 사전에 싱크 노드로부터 부모 노드와 자식 노드들의 양단키를 분배 받아 재배치되고, 그룹키는 양단키로 암호화해서 전송된다고 가정한다.

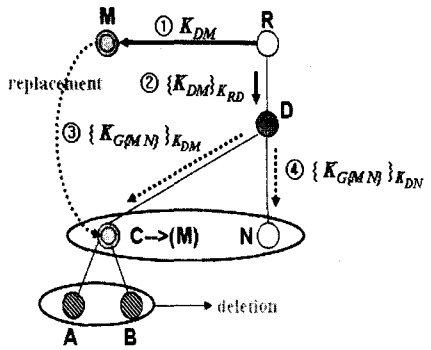
$$R \rightarrow \{M\} : \{K_{DM} \| K_{MA'} \| K_{MB'}\} \quad -①'$$

⑤ 재배치 된 노드 M가 하위 자식 노드를 가지고 있을 경우 기존의 자식 노드 A, B를 삭제되고, 새로운 자식 노드 A', B'가 추가된다. 이때 A', B'노드를 추가하기 위해서, 먼저 싱크노드 R이 추가될 센서 노드 A', B'에게 부모 노드 M과 공유하는 양단키($K_{MA'}$,$K_{MB'}$)를 생성하여, 센서 노드 A', B'에게 배치되기 전에 저장한다.

$$R \rightarrow \{A'\} : \{K_{MA'}\} \quad -⑤$$
$$R \rightarrow \{B'\} : \{K_{MB'}\} \quad -⑤$$

⑥ 이후 M은 새로운 양단키($K_{MA'}$,$K_{MB'}$)로 자식 노드의 그룹키($K_{G(A'B')}$)를 암호화해서 자식 노드에게 전송한다.

$$M \rightarrow \{A'\} : \{K_{G(A'B')}\}_{K_{MA'}} \quad -⑥$$
$$M \rightarrow \{B'\} : \{K_{G(A'B')}\}_{K_{MB'}} \quad -⑥$$



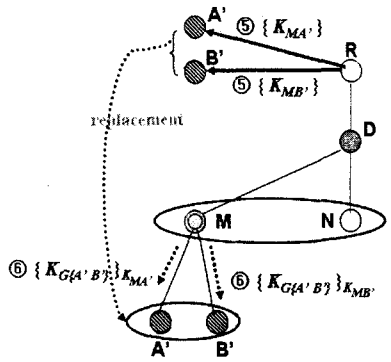


그림 3. 제안한 센서 노드의 재배치 기법

3.5 센서 노드의 삭제

센서 노드의 삭제의 경우는 Chen등이 제시한 방법과 동일하다. 임의의 노드가 삭제 될 경우 직계 부모 노드는 하위 자식 노드의 새로운 그룹키를 생성해서 자식 노드들에게 각각 전송한다. 예를 들어, 그림 1에서 노드 J가 삭제 될 경우 직계 부모 노드 L은 새로운 그룹키($K_{G(IH)}$)를 생성하여, J와 같은 그룹 멤버 노드인 I, H에게 전송한다.

$$L \rightarrow \{I\} : \{K_{G(IH)}\}_{K_{LI}}$$
$$L \rightarrow \{H\} : \{K_{G(IH)}\}_{K_{LH}}$$

4. 분석

본 장에서는 기존의 Chen등이 제시한 기법과 본 논문에서 제안한 개선된 키 관리 기법에 관하여 다음의 평가 항목으로 분석한다.

- 통신 오버헤드 : 계층적 센서 네트워크에서 센서 노드 추가 및 재배치 경우 양단키와 그룹키 전송에 대한 오버헤드를 분석한다.
- 양단키 전송의 안전성 : 계층적 센서 네트워크에서 센서 노드의 추가 및 재배치를 원하는 센서 노드에게 양단키가 전송되는 경우의 안전성을 분석한다.

표 1. 키 관리 기법에 대한 비교

평가항목 / 키관리 기법	통신오버헤드	양단키 전송의 안전성
Chen등의 기법	$O(1)$	제공안됨
제안된 기법	$O(\log n)$	제공

표 1은 Chen등이 제안한 기법과 본 논문에서 제안한 키 관리 기법에 대한 비교 분석이다.

센서 노드의 개수를 n으로 가정할 때, Chen등이 제시한 기법이 $O(1)$만큼의 통신오버헤드를 가진다면, 본 논본 논문에서 제시한 키 관리 기법은 $O(\log n)$만큼의 통신 오버헤드가 발생한다. 본 논문에서 제안한 기법이 chen등이 제시한 기법에 비해 통신 오버헤드는 존재하지만, 부모 노드와 자식 노드 사이에 양단키 전송의 안전성을 제공하기 때문에, chen등이 제시한 키 관리 기법보다 안전한 통신을 제공한다.

5. 결론

본 논문에서는 계층적 센서 네트워크 환경에서 개선된 키 관리 기법을 제안하였다. 본 논문에서 제안한 키 관리 기법은 Chen등이 제시한 키 관리 기법에서의 센서 노드의 추가 및 재배치 경우 보안의 취약점을 해결하기 위해서 개선된 키 관리 기법을 제시하였다. 제시한 기법은 새로운 센서 노드 추가 및 재배치 경우에 싱크 노드가 추가 및 재배치되는 센서 노드의 양단키를 생성하여 사전에 전송하고, 그리고 싱크노드는 추가 및 재배치되는 센서 노드의 부모 노드에게 생성한 키를 전송하여 추가 및 재배치 노드를 할 때 안전한 양단키 전송을 수행하기 때문에, 기존의 기법보다 높은 안전성을 제공해준다.

[참고문헌]

[1] Xiao Chen, Jawad Drissi, *"An Efficient Key Management Scheme in Hierarchical Sensor Network"*, Mobile Adhoc and Sensor Systems Conference 2005 IEEE International Conference, pp. 6, 2005.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, *"A Survey on Sensor Networks"*, IEEE Communication Magazine, pp. 102-114, August. 2002.

[3] H. Chan, A. Perrig, and D. Song, *"Random Key Predistribution Schemes for Sensor Networks"*, IEEE Symposium on Research in Security and Privacy, pp. 197-213, 2003.

[4] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, *"A Pairwise Key Predistribution Scheme for Wireless Sensor Networks"*, Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), pp. 42-51, Oct. 2003.

[5] W. Du, J. Deng, Y. S. Han, S. Chen and P. Varshney, *"A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge"*, Proceedings of the IEEE INFOCOM'04, pp. 586-597, Mar. 7-11, 2004.

[6] Jose A. Gutierrez, Edgar H. Callaway Jr, Raymond L. Barrett Jr, *"Low-Rate Wireless Personal Area Networks"*, IEEE Std 802.15.4.

[7] D. Liu, and P. Ning, *"Establishing pairwise keys in distributed sensor networks"*, Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 52-61, 2003.

[8] L. Eschenauer and V. Gligor, *"A Key Management Scheme for Distributed Sensor Networks"*, In Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 41-47, 2002.