무선 센서 네트워크에서 효율적인 오용키 탐지 기법†

김종명*, 한영주**, 박선호*, 정태명***
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 컴퓨터공학과
***성균관대학교 정보통신공학부
e-mail : {jmkim, yjhan, shpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

An Efficient Misused Key Detecting Method in Wireless Sensor Networks

Jong-Myoung Kim*, Young-Ju Han**, Seon-Ho Park*, and Tai-Myoung Chung***
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
**Dept. of Computer Engineering, Sungkyunkwan University
***School of Information Communication Engineering, Sungkyunkwan University

요 약

무선 센서 네트워크에서 보안 서비스를 제공하기 위하여 키 관리 방법에 대한 연구가 많이 진행되어 왔다. 대부분 센서 노드의 자원적인 제약사항으로 인해 공개키 방법보다는 대칭키 방법을 이용하기 위한 연구가 진행되었으며 그 결과 센서 노드 사이에 대칭키를 공유하여 기밀성, 인증 그리고 무결성 등의 보안 서비스를 제공할 수 있게 되었다. 하지만 센서 노드의 저장 공간의 제약으로 인해 모든 노드와의 대칭키를 저장할 수 없어 대부분의 센서 네트워크에서의 키 관리 메커니즘들은 확률적인 방법을 이용하여 키를 공유하도록 한다. 이 경우 확률적으로 공격자가 네트워크에 물리적 노드 획득 공격을 감행할 경우 공격자에게 타협되지 않은 정상 노드 사이의 키를 얻을 수 있다. 공격자는 이러한 키를 이용하여 센서 네트워크의 정상적인 동작을 방해할 수 있으며 특히 센서 네트워크 어플리케이션의 동작에 있어서 치명적인 영향을 줄 수 있다. 본 논문에서는 이렇게 공격자에게 드러난 키를 통해 공격자가 공격을 감행한 경우 해당 오용키를 효율적으로 파악하고 정상 노드 사이의 대칭 키를 안전한 키로 대체하는 방법을 제안한다.

1. 서론

최근 무선 통신 기술과 저전력 기술의 발전으로 인해 무선 센서 네트워크의 현실화에 대한 가능성이 높아지고 있다. 특히, 생태계 모니터링, 군사적 목적, 의료목적, 홈 네트워크 그리고 유비쿼터스 환경 등 다양한 영역에서 무선 센서 네트워크가 활용되고 연구되고 있다[1][2].

무선 센서 네트워크는 하나 이상의 BS(Base Station)와 제한된 계산 능력, 저장공간 그리고 에너지를 가지며 값이 싼 다수의 센서 노드들로 구성되며 주로 특정 지역에 분포되어 정보를 수집한다. 이러한 센서 노드는 물리적으로 공격자가 공격하기 쉬운 취약한 지역에 분포될 수 있으며 이 경우 무결성, 가용성, 인증 및 신뢰성 등의 보안 서비스가 필수적으로 제공되어야 한다.

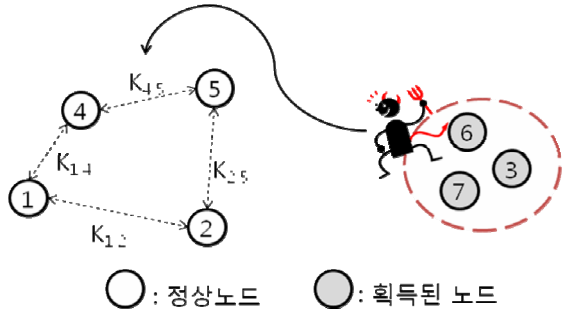
보안 서비스를 제공하기 위한 가장 기본적인 요소는 키 관리 방법이다. 하지만 센서 노드의 자원적인 제약사항으로 인하여 기존의 KDC(Key Distribution Center) 방법과 공개키 방식의 키 관리 방법은 센서 네트워크에 적용하기에 한계가 존재한다. 특히 공격자가에게 취약한 지역에 센서 노드가 분포되기 때문에 공격자는 센서 노드를 물리적으로 획득하여 해당 센서 노드의 키를 획득할 수 있다. 이러한 특징을 고려한 센서 네트워크의 키 관리를 위해 많은 메커니즘들이 제안되어 왔다. 센서 네트워크의 키 분배 기법의 기원은 Gilgor 가 제안한 random key distribution 방법[3]에서 기인하며 이는 일정한 키 풀을 생성하고 각 센서 노드에 키 풀로부터 일정수의 키를 사전 분배함으로써 센서 노드들 사이에 일정한 확률로 키를 공유할 수 있도록 한다. 이 방법은 공격자가 물리적 공격을 통해 노드를 획득할 경우 해당 노드가 지니는 키가 노출되어 네트워크의 다른 노드들을 위협할 수 있다는 단점이 있다. 이러한 문제점을 해결하기 위해 Chan 은 q-composite random key distribution 방법[4]을 제안하였다. Chan 의 방법은 두 노드가 q 개의 공유키를 가질 경우에만 통신을 허용하여 공격자가 해당 노드와 통신을 하기 위해서는 q 개의 키를 획득해야하

† "본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-C1090-0801-0028)

는 제약사항을 두어 Gilgor 방법의 단점을 해결하고 있다. 이 후 노드 획득 공격에 강한 키 분배 방법에 연구가 계속되었으며 으며 Liu 와 Ning 은 t 차 이변수 다항식과 2 차원 격자 기반의 키 분배 방법[5]을 제안하였다.

그러나 위의 키 관리 방법들은 공통적으로 공격자가 일정 수 이상의 센서 노드를 공격하여 해당 노드의 키를 알아낸 경우 공격자가 공격하지 않은 다른 센서 노드들 사이의 대칭키 역시 획득할 수 있다는 단점이 존재한다. 최근 Liu 와 Dong[6]은 공격자가 이와 같은 방법으로 획득한 키를 통하여 네트워크에 잘못된 데이터를 삽입하여 어플리케이션에 치명적인 오류를 야기하려는 공격을 감행할 경우, 오용된 키를 탐지하고 이를 안전한 키로 교체함으로써 공격자가 더 이상 네트워크에 공격을 하지 못하도록 하는 방법을 제안했다. 본 논문에서는 Liu 와 Dong 의 방법을 발전시켜 무선 센서 네트워크에서 에너지 효율적인 오용키 탐지 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 관련연구로써 Liu 와 Dong 의 오용키 탐지 방법에 대해 간략히 살펴본다. 3 장에서는 본 논문이 제안하는 에너지 효율적으로 오용키를 탐지하는 방법에 대해 설명한다. 4 장에서는 본 논문에서 제안하는 방법과 Liu 와 Dong 의 방법을 비교하여 효율성을 증명한다. 마지막으로 5 장에서는 본 논문의 결론과 앞으로의 향후 연구에 대해서 이야기 한다.



(그림 1) 오용키의 예

2. 관련 연구

일반적으로 널리 알려진 센서 네트워크에서의 키 관리 기법은 확률적인 방법을 이용하거나 t 차 이항 방정식을 이용하여 확률적으로 노드 사이의 대칭키를 형성한다. 이 때 두 노드 사이에 공유키가 존재하지 않을 경우 주변 노드의 도움을 통해 패스키를 설정하는 것이 일반적이다. 하지만 대부분의 키 관리 방법[3,4,5]에서 공격자가 일정 수 이상의 센서 노드를 공격하여 해당 노드의 키를 알아낸다면 공격하지 않은 정상 노드 사이의 대칭키를 쉽게 획득하여 네트워크를 공격할 수 있다는 문제가 있다. 즉, (그림 1)에서와 같이 공격자가 노드 3, 6, 7 을 획득하여 정상 노드 4 와 5 사이의 대칭키 $K_{4,5}$ 를 알아낼 수 있다. 특히 대칭키 $K_{4,5}$ 를 이용하여 잘못된 데이터를 삽입하여 네트워크를 공격한 경우 어플리케이션의 동작에 치명적일 수 있다. Liu 와 Dong 은 이러한 센서 네트워크 키 관리 기법의 문제점을 보완할 수 있는 방법을 제안하였다.

핵심 원리는 다음과 같다. 센서 노드 u 가 v 에게 메시지 M 을 전송 할 경우, u 와 v 는 변수 $C_{u,v}$ 를 유지하고 있으며 초기값은 0 으로 동일하다. 이 때 메시지 M 을 전송하기에 앞서 새로운 $C_{u,v}=H(M||C_{u,v})$값을 계산한다. 또한 CV(Committing Value)인 $V=H(C_{u,v}||K_u)$를 새로운 $C_{u,v}$ 값과, u 와 BS 가 공유한 대칭키 K_u 를 통해 계산하고 최종적으로 M 과 V 를 노드 v 에게 전송한다. 이 때 M 과 V 는 노드 v 와 u 사이의 대칭키 $K_{u,v}$ 를 통해 보호받는다. 노드 v 는 M 과 V 를 수신하고 자신의 $C_{u,v}$ 를 $H(M|| C_{u,v})$로 갱신한다. 또한 u 와 v 사이의 대칭키 $K_{u,v}$ 가 오용되었는지를 판단하기 위해 일정 확률에 따라 현재의 노드 u 의 ID 와 $C_{u,v}$ 그리고 V 를 BS 에게 전송하고 이들은 $H(C_{u,v}||K_u)$를 계산하여 수신된 V 값과 동일한 지를 확인한다. 이 때 결과 값이 다르면 대칭키 $K_{u,v}$ 가 공격자에 의해 오용되었다고 판단하고 새로운 키를 생성하여 K_u 와 K_v 를 통해 새로운 대칭키를 전송한다.

앞서 소개한 알고리즘은 BS 가 오용키를 탐지하도록 하기 때문에 중앙 집중적인 특징을 가지게 되어 센서 네트워크에 적용하기 힘들다. 이에 Liu 와 Dong 은 BS 대신 오용키를 1 차적으로 탐지를 하는 오용키 탐지 노드를 소개함으로써 무선 센서 네트워크에 적합하도록 분산된 형태의 오용키 탐지 방법을 제안하였다. 이 방법은 정상 노드 사이의 키가 공격자로 인해 오용될 경우 완벽하게 오용키를 탐지할 수 있다.

3. 제안하는 기법

이번 장에서는 Liu 와 Dong 의 방법을 에너지 효율적으로 개선하여 오용키를 탐지하는 방법을 소개한다. Liu 와 Dong 의 방법에서는 u 가 v 에게 메시지를 전송할 경우 항상 V_1 과 V_2 를 함께 전송해야 했으며 메시지를 수신한 v 는 일정확률 p 에 오용키 탐지를 위한 메시지를 생성하고 이를 오용키 탐지 노드에게 전송했었다. 그러나 V_1 과 V_2 가 항상 전송되어야 한다는 점은 메시지의 길이가 상대적으로 작은 센서 네트워크의 입장에서 매우 큰 오버헤드이다. 본 논문에서는 V_1 과 V_2 에 대한 전송 자체를 일정확률 p 를 따르게 함으로써 효율적으로 오버헤드를 줄이고 있다. 본 논문에서 제안하는 오용키 탐지 기법은 총 3 개의 단계로 구성된다.

3.1. 사전 조건

분산된 형태의 탐지를 위해 Liu 와 Dong 이 소개한 오용키 탐지 노드를 이용한다. 각 센서 노드 u 는 목적 지역에 분포되기 전 BS 와의 대칭키 K_u 를 할당받는다. 이는 대부분의 키 관리 방법에서 기본이 되는 조건이다. 또한 오용키 탐지 노드 i 는 모든 센서 노드 u 에 대해 u 와의 대칭키인 $H(K_u||i)$를 저장한다. 오용키 탐지 노드는 센서 노드가 주변에서 최소한 한 개 이상 찾을 수 있도록 분포 시킨다. 목표지역에 분포된 후, 각 센서 노드 u 는 자신의 주변에 있는 오용

키 탐지 노드에 대한 ID 목록 (u)를 만들어 주변 노드 v 에게 알린다. 센서 노드가 최초로 배포될 때에는 공격자가 아직 센서 노드 사이의 대칭키를 알지 못하기 때문에 안전하게 오용키 탐지 노드 목록 (u)를 전송할 수 있다.

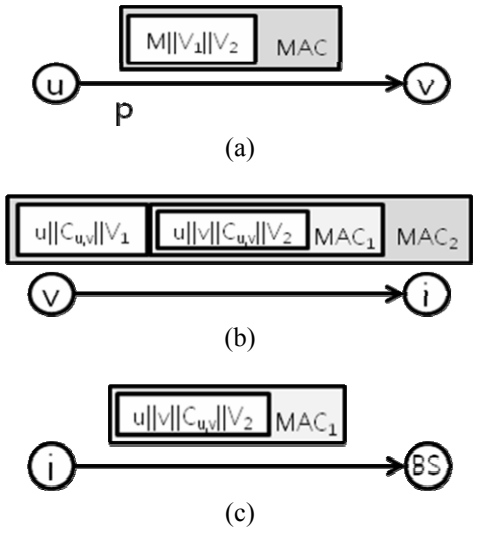
3.2. 동작 과정

3.2.1. 첫 번째 단계: 오용키 추적

공격자에게 타협하지 않은 정상 센서 노드 u 와 v 에 있어서 u 가 v 에게 대칭키 $K_{u,v}$ 를 이용하여 통신을 할 경우 두 노드는 변수 $C_{u,v}$ 를 내부적으로 유지한다. 역 방향 통신의 경우에도 역시 변수 $C_{v,u}$ 를 유지한다. $C_{u,v}$ 의 초기 값은 0 이며 u 가 v 에게 메시지 M 을 전송할 때 마다 u 는 $C_{u,v}$ 를 다음 수식에 따라 갱신한다.

$$C_{u,v} = H(M \| C_{u,v})$$

노드 v 역시 메시지 M 을 수신할 때 마다 $C_{u,v}$ 를 위의 수식에 따라 갱신한다.



(그림 2) 오용키 탐지

3.2.2. 두 번째 단계: 오용키 탐지

메시지 M 을 전송할 때 마다 일정 확률 p 에 따라 노드 u 는 v 에게 (그림 2-a)와 같이 메시지를 전송한다. 이 때 V_1 과 V_2 는 다음 수식에 따라 계산되며 MAC 은 $K_{u,v}$ 를 통해 생성되며 이 때 i 는 (v)에 있는 ID 중 하나이다.

$$V_1 = H(Cu,v \| H(K_u \| i))$$
$$V_2 = H(Cu,v \| K_u)$$

V_1 과 V_2 를 받은 노드 v 는 메시지 M 을 이용하여 $C_{u,v}$ 를 새로운 값으로 갱신한 후 (그림 2-b)와 같은 메시지을 생성하여 오용키 탐지 노드 i 에게 전송한다. 이 때 MAC_1 은 K_v 를 이용하여 생성되며 MAC_2 는 $H(K_v||i)$를 이용하여 만들어진다.

오용키 탐지 노드 i 는 메시지를 수신한 후 메시지의 $u||C_{u,v}||V_1$ 정보와 노드 u 와의 대칭키 $H(K_u||i)$를 이용하여 $V_1=H(C_{u,v}||H(K_u||i))$를 확인한다. 이 값이 서로 다르다면 공격자가 대칭키 $K_{u,v}$ 를 통해 잘못된 데이터를 삽입했다는 의미이며 이 경우 $K_{u,v}$ 를 오용키로 판단하고 (그림 2-c)와 같이 메시지를 전송한다. 이는 v 로 부터 받은 메시지에 캡슐화 되어 있던 메시지이다.

3.2.3. 세 번째 단계: 키 재설정

BS 는 (그림 2-c)와 같이 메시지를 수신한 후 노드 아이디 u 와 v 를 통해 K_u 와 K_v 를 찾고 K_v 를 이용하여 MAC_1 을 확인하고 $V_2=H(C_{u,v}||K_u)$를 확인한 후 새로운 대칭키 $K_{u,v}$ 를 생성하여 K_u 와 K_v 를 이용하여 전송한다.

3.3. 보안 분석

공격자는 K_u, $H(K_u, i)$에 대한 값을 획득할 수 없기 때문에 V_1 과 V_2 그리고 MAC_1 과 MAC_2 를 생성할 수 없다. 따라서 일단 오용키 탐지를 위한 메시지가 생성된 경우 이를 위· 변조 할 수 없다. 또한 u 와 v 는 공격자에게 타협하지 않은 정상 노드이기 때문에 정상적으로 오용키 탐지 메시지를 생성하고 오용키 탐지 노드에게 이를 전송하게 된다.

공격자가 $K_{u,v}$ 를 획득했을 경우 전송되는 메시지를 수정할 수 있는 유일한 곳은 (그림 2-a)의 경우이다. 공격자가 오용키 탐지 단계가 수행되지 않도록 하기 위해 (그림 2-a)의 오용키 탐지 메시지를 가로채고 V_1 과 V_2 를 제거하고 M 에 대한 내용만을 전송할 뿐 V_1 과 V_2 를 전송하지 않을 수 있다. 이 경우 노드 v 가 일정 시간 t 에 대한 타이머를 설정하여 이 시간 동안 오용키 탐지를 위한 메시지가 도착하지 않으면 이를 u 에게 요청하고 응답이 없는 경우 키 $K_{u,v}$ 가 오용되었음을 BS 에게 알리는 메커니즘을 이용하여 이러한 공격을 방지할 수 있다.

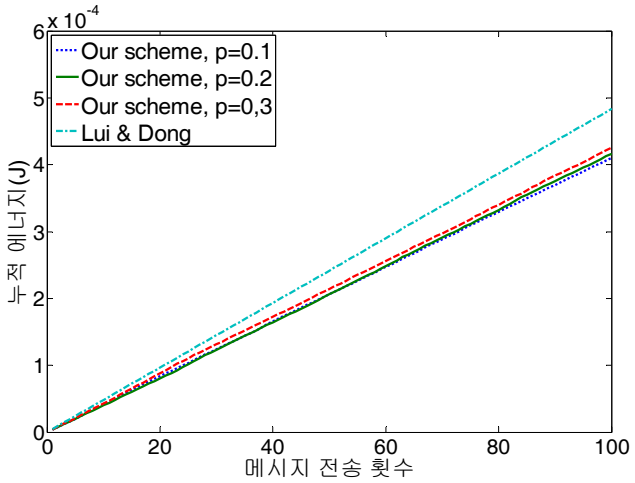
만약 공격자가 오용키 탐지 노드를 획득하여 정상 노드 사이의 대칭키를 오용키로 보고하려는 공격을 수행한다 하더라도 MAC_1 이 K_v 를 통해 생성되기 때문에 이 공격 역시 불가능 하다. 결국 노드 u 와 v 가 공격자에게 획득되지 않은 정상 노드일 경우 오용키 탐지 메커니즘은 정상적으로 동작하게 된다.

4. 성능 평가

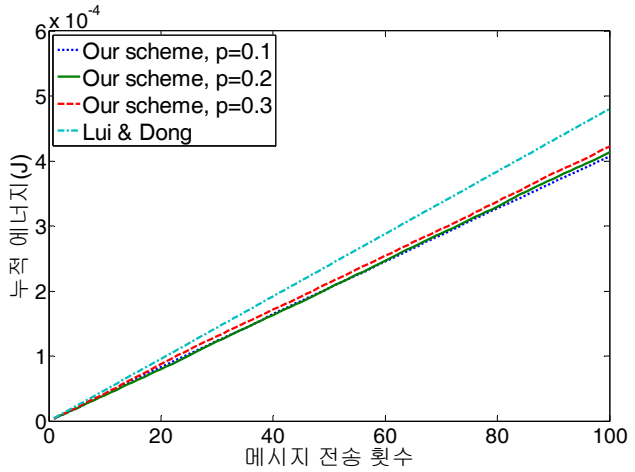
센서 네트워크에서 전송되는 메시지가 대부분 수집된 단일 정보 혹은 병합된 값을 전송한다는 것을 생각한다면 메시지 M 의 길이는 일반적으로 매우 짧을 것이며 매 통신마다 V_1 과 V_2 를 전송한다는 것은 큰 오버헤드이다. 만약 V1 과 V2 의 크기가 각각 α byte 라 한다면, 본 논문에서 제안하는 방식은 Liu 와 Dong 의 방식에 비해 전송되는 메시지 마다 평균적으로 2* α *(1-p)byte 의 오버헤드를 줄이게 된다.

(그림 3)은 평균 전송되는 메시지의 크기가 80byte 이고 α 가 8byte 일 때 전송되는 메시지의 개수에 따른 센서 노드 u 와 v 에서 소비된 에너지에 대한 시뮬레이션 결과를 보여주고 있다. 시뮬레이션은 Matlab

을 통해 이루어졌으며 전송 시 소비되는 에너지를 계산하기 위해 [7,8,9]에 소개된 Radio 모델을 적용하였다. 시뮬레이션 결과 송·수신 노드 u, v 모두 p=0.1 일 경우의 Liu 와 Dong 의 방법에 비해 에너지 소비가 약 14% 줄어들었다.



(a) 송신 노드 u 에서 소비된 에너지



(b) 수신 노드 v 에서 소비된 에너지

(그림 3) u 와 v 에서의 에너지 소비

5. 결론

무선 센서 네트워크에서 보안 서비스를 제공하기 위해서는 키 관리 방법이 필수적이다. 하지만 센서 노드의 특징으로 인해 센서 네트워크에서의 대부분의 키 관리 방법은 공격자가 몇몇 노드를 획득하여 해당 노드의 키를 알아낼 경우 공격자에게 획득되지 않은 정상 노드 사이의 대칭키를 공격자가 획득할 수 있다는 문제점이 존재했다.

본 논문에서는 정상 노드 사이의 대칭키를 공격자가 획득하여 이를 통해 비정상적인 메시지를 삽입하거나 전송되는 메시지를 수정했을 경우 공격자에게 드러나 키를 에너지 효율적으로 탐지할 수 있는 방법에 대해 소개했다. 오용키 탐지를 위한 메시지를 매번 생성하지 않고 일정 확률 p 에 따라 생성함으로써 오용키 탐지에 있어서 오버헤드를 크게 줄일 수 있었다.

앞으로 센서 네트워크에서 오용키 탐지 기법의 오버헤드를 줄여 에너지 효율을 더욱 극대화 시킬 수 있는 방법에 대해 연구를 진행할 것이다. 또한 널리 알려진 키 관리 기법들에 이를 적용함으로써 그 연구를 구체화할 계획이다.

참고문헌

[1] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, “Habitat Monitoring: Application Driver for Wireless Communications Technology”, In Proceedings of the ACM SIGCOMMWorkshop on Data Communications in Latin America and the Caribbean, San Jose, Costa Rica, 2001.

[2] Jalal A., Anand R., Roy C.l and M. Dennis Mikunas, “Cerberus: A Context-Aware Security Scheme for Smart Spaces”, Pervasive Computing and Communications, 2003. (PerCom 2003). Proceedings of the First IEEE International Conference on 23-26, pp.489-496, March 2003.

[3] L. Eschenauer and V. Gligor, “A Key Management Scheme for Distributed Sensor Networks”, Proc. 9th ACM Conf. Comp. and Commun. Sec., pp. 41-47, Nov. 2002.

[4] H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks”, Proc. IEEE Sec. and Privacy Symp., pp. 197-213, 2003.

[5] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks”, CCS ’03, Proceedings of the 10th ACM conference on Computer and communications security. New York, NY, USA: ACM Press, pp. 52-61, Oct. 2003.

[6] D. Liu and Q. Dong, “Detecting Misused Keys in Wireless Sensor Networks”, IPCCC2007: Perform. Comp. and Comm. Conf., pp.272-280, April 2007.

[7] Mhatre, V., Rosenberg, C., “Design Guidelines for Wireless Sensor Networks: Communication, Clustering and Aggregation”, Ad Hoc. Networks, Page(s): 45-63, 2003.

[8] W. R. Heinzelman, A. Chandarkasan, and Hari Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Microsensor Networks”, IEEE Transactions on Wireless Communications, Page(s): 660-670, 2002.

[9] Yong-Ju Han, Seon-Ho Park, Jung-Ho Eom, and Tai-Myoung Chung, “Energy-Efficient Distance Based Clustering Routing Scheme for Wireless Sensor Networks”, ICCSA2007, LNCS 4706, Part II, pp. 195–206, 2007.