무선 센서 네트워크에서의 해쉬 함수와 식별자를 이용한 인증방안[1]

이은경○ 신수복 예홍진
아주대학교 정보통신 대학원○, 아주대학교 정보통신 전문대학원
wisesea@ajou.ac.kr, watermel@ajou.ac.kr, hjyeh@ajou.ac.kr

An Authentication Method Using Identifier and Hash Function in Wireless Sensor Network

Lee eun gyong○ Shin soo bok Yeh hong jin
Ajou University Graduate Shool of Information&Communication

요 약

무선 센서 네트워크 환경에서의 구성요소간의 상호 인증은 중요하다. μ-TESLA에서의 브로드캐스트 인증은 인증시간의 지연이 발생한다. 지연의 발생은 현재 받은 메시지의 인증이 메시지를 받은 즉시 이루어지지 않고 다음 메시지를 받았을 때 이전의 메시지에 대한 인증이 이루어지기 때문이다. 이는 실시간 처리를 필요로 하는 통신에는 적합하지 않다. 또한 대칭키를 기반으로 인증하는 방법에서는 인증시간의 지연이 발생하지 않지만 인증을 위한 키가 노출되었을 때, 키를 재생성, 분배해야하는 문제가 있다. 본 논문에서 제안하는 인증방안은 식별자와 해쉬 함수를 이용하여 인증시간의 지연이 없는 실시간 인증과 인증에 사용하는 식별자가 노출되었더라도 키의 재생성 및 분배없이 인증을 달성하는 방법을 제시한다.

1. 서 론

무선 센서 네트워크는 초경량 저전력의 센서 노드들로 구성되며 센서 노드들 간의 통신과 센서 노드와 BS(Base Station)간의 데이터 통신이 무선으로 이루어진다. 이런 환경에서 BS와 센서 노드간의 상호 인증은 중요한 보안 요구사항이다[1].

무선 센서 네트워크에서의 상호 인증은 통신 당사자가 정당한지 확인하는 것이다 상호 인증은 크게 두가지로 분류할 수 있는데, 첫 번째는 BS가 센서 노드를 인증하는 것이고 두번째는 센서 노드가 BS를 인증하는 것이다. 이를 위해 BS와 센서 노드는 대칭키를 미리 분배하고 보관하여 인증이 필요한 경우 서로의 키를 이용해 인증하는 방법을 사용한다. 인증을 하기 위한 또다른 방법은 공개키를 이용한 전자서명을 사용하는 것이다.

이러한 인증 서비스를 제공하기 위해서는 키를 생성하고 분배하며 갱신하는 등의 키 관리가 요구된다. 하지만 대칭키나 공개키를 사용하는 방법은 일반적으로 많은 메모리 공간과 복잡한 계산을 필요로 하는데 전력이나 메모리, 프로세서와 같은 자원의 제약이 있는 무선 환경에서는 쉽게 적용하기 어려운 것이 현실이다[2][3].

SPINS에서는 BS와 센서 노드들이 마스터 키를 공유하여 이 마스터 키로부터 다른 키를 유도하여 상호간의 인증을 제공하였고 μ-TESLA 브로드캐스팅 인증을 제공하지만 인증 지연시간이 발생하였다[4].

한편 Henrici와 Mulle는 RFID 환경에서 태그 정보의 익명성을 보장하기 위하여 리더가 태그의 정보를 읽을 때마다 태그에 저장된 ID를 바꾸는 방법을 제안하였다[5]. 비록 RFID 시스템과 무선 센서 네트워크 시스템은 통신 유형이나 보안 요구사항이 서로 다르지만 BS와 센서 노드에 ID를 부여하고 매번 사용할 때마다 해쉬 함수를 이용하여 ID를 변경한다면 BS의 브로드 캐스트 인증은 물론, 각 센서 노드의 인증 문제를 해결하는 데에도 활용할 수 있다는 것에 착안하게 되었다 이때 네트워크 구성 요소에 부여된 ID를 식별자라고 부르기로 한다.

본 논문에서는 대칭키나 공개키 알고리즘을 사용하는 대신에 각자 상대방의 식별자를 이용하여 BS와 센서 노드가 서로를 인증하는 절차를 제안하고자 한다. 본 논문의 구성은 2장에서는 문제정의를 설명하고 3장에서는 기본적인 가정과 구성을 기술한다. 4,5장에서는 식별자를 이용한 상호 인증 방안을 설명한 다음 결론 및 향후 연구과제를 제시한다.

2. 문제정의

무선 센서 네트워크에서는 BS와 센서노드들간의 통신

1 본 연구는 지식경제부 및 정보통신연구진흥원의IT핵심기술개발사업의 일환으로 수행하였음 [2008-S-027-01, IP 기반 센서네트워크 기술개발]

에서 악의적인 공격자가 침투하여 네트워크 전체적인 신뢰도와 성능의 저하를 일으킬 수 있다. 즉 센서노드로 위장하여 BS에 잘못된 정보를 제공하므로 센서 네트워크의 센싱 정보의 신뢰도를 떨어뜨리거나 BS로 위장하여 센서노드로부터 오는 정보를 수집하거나 반복적인 브로드 캐스트를 통해 저전력 환경하에서의 무선 센서 네트워크의 성능을 저하 시킬 수 있다. 따라서 센서 네트워크에서 성능향상과 신뢰도를 높이기 위하여 각 구성요소간의 상호 인증은 매우 중요하다. 이를 위해 기존에는 사전에 대칭키를 분배하여 저장하고 있다가 이를 이용해 상호인증을 하였다. 하지만 이와같이 대칭키를 이용한 인증은 키가 노출되었을때 네트워크 전체의 인증 기능을 상실하게 되며 새로운 인증키의 생성 및 분배에 대한 오버헤드를 초래하게 된다. 대칭키 분배없이 해쉬함수를 이용한 인증방법으로 μ-TESLA가 제안되었는데 이는 인증 지연시간이 발생한다. 인증지연은 실시간 인증이 필요한 경우에는 적합하지 않다. 따라서 대칭키나 공개키 알고리즘 없이 실시간으로 BS와 센서 노드간의 안전한 인증을 위한 방법이 필요하다.

3. 시스템의 가정 및 구성

3-1. 시스템 구성

본 논문에서 고려하는 무선 센서 네트워크는 여러 개의 BS과 각 BS와 통신하는 여러 개의 센서노드가 존재하는 네트워크 환경이다. 모든 센서노드는 하나의 BS와 통신하며 각 BS는 서로 통신이 가능하다고 가정한다.

그림1은 무선 센서 네트워크의 구성을 나타낸다. 본 논문에서는 BS와 그와 직접 통신하는 센서 노드간의 인증문제를 다룬다. BS와 센서 노드의 구성은 기본적으로 동일하나 BS가 센서 노드보다 큰 저장 공간을 갖고 있고 전력이 풍부하다. 센서노드의 구성은 주변 환경으로부터 센싱하기 위한 센싱 유닛과 프로세서, 메모리, 통신장치, 전력공급 장치가 있다. 제안하는 방안을 달성하기 위해 다음의 구성요소를 추가한다.

각 구성 요소는 자신의 식별자를 저장하는 메모리가 존재하며, 이 메모리는 읽기와 쓰기가 가능하다. 또한 현재의 식별자에서 다음의 식별자를 생성하기 위한 해쉬 함수인 Generator(G)가 있다. Generator(G)는 BS와 센서 노드에서 동일한 연산을 수행한다.

3-2. BS와 센서 노드의 구성에 대한 가정

1) BS와 센서 노드는 각자가 고유한 식별자를 갖고 있다.
2) 공격자는 센서 네트워크의 통신 내용을 도청함으로 정보를 얻어낼 수 있다. 즉 인증에 사용되는 식별자를 알아낼 수 있다.
3) BS와 센서 노드는 일대일 통신을 하며 센서 노드간의 통신을 고려하지 않는다.
4) BS는 센서 노드보다 큰 전력을 공급받을 수 있으며, 센서 노드보다 많은 저장 공간을 갖고 있다.
5) BS는 자신과 통신하는 모든 센서 노드의 식별자를 저장하고 있다.
6) 센서 노드는 자신의 식별자와 BS의 식별자를 저장하고 있다.

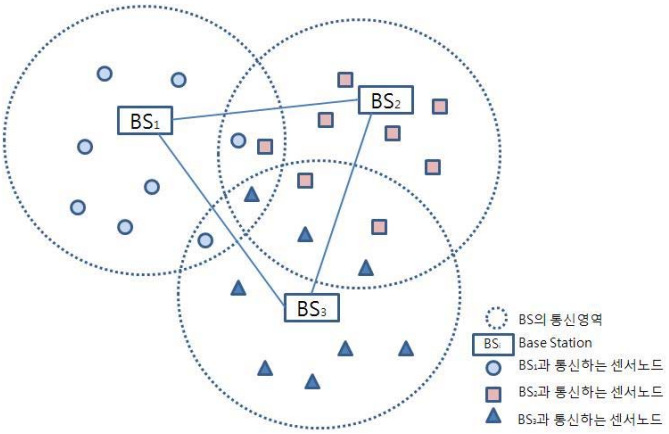

그림 1 센서 네트워크 구성

그림 2와 그림3은 BS와 센서 노드의 구성도이다. BS와 센서 노드의 구성에서 BS는 주변 환경에서 환경을 센싱하는 기능이 필요 없으므로 Sensing Unit이 없다. BS에서 Storage(Sensor Node)는 모든 센서 노드의 식별자를 저장하고 있고, 센서노드에서 Storage(Sensor Node)는 자신의 식별자를 저장하고 있다. BS와 센서 노드에서 Storage (Base Station)은 BS의 식별자를 저장한다.

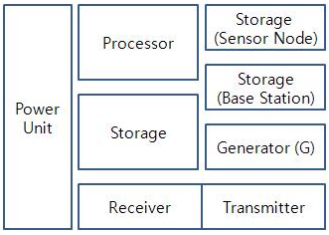

그림 2. BS의 구성도

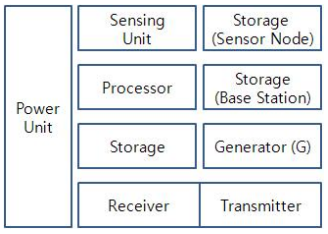

그림 3. 센서노드의 구성도

4. Notation 및 Operation

4-1. Notation

S_0 : Base Station

S_i : 센서노드 $(1 \le i \le n, i$는 정수$)$

S_0^0 : Base Station의 초기 식별자

S_i^0 : 센서노드 S_i의 초기 식별자

G : 다음 식별자를 생성하는 해쉬함수

S_0^p : Base Station의 p번째 변환된 식별자

$S_0^p = \underline{BRACE}\, pG \circ \cdots \circ G(S_0^0)$

S_i^q : 센서노드 S_i의 q번째 변환된 식별자

$S_i^q = \underline{BRACE}\, qG \circ \cdots \circ G(S_i^0)$

$S_i^{j+1} = G(S_i^j)$: Generator(G)에 의해 다음 식별자 생성

$S^j{}_{i\ (Sensor/BS)}$: $i=0$이면 BS의 식별자, $i \neq 0$이면 센서 노드의 식별자를 나타낸다. j의 값은 초기부터 j번째 생성된 식별자를 나타낸다. 괄호안이 $Sensor$이면 센서의 저장 공간에 저장된 BS 혹은 센서노드의 식별자를 BS이면 BS에 저장된 식별자를 나타낸다.

4-2. Operation

BS와 n개의 센서 노드는 서로 다른 초기 식별자 ($S_0^0, S_1^0, S_2^0 \cdots S_n^0$)를 갖고 있다. 본 논문에서 고려하는 인증을 위한 통신은 2가지이다. 센서 노드에서 BS로, BS에서 모든 센서 노드로의 통신간의 인증이다.

센서 노드에서 BS로 통신할 때, 센서 노드는 자신의 식별자를 다음의 식별자로 변경하여 전송하고 저장하고 있는 BS의 식별자는 변경하지 않는다. 마찬가지로 BS에서 센서 노드로 통신할 때에는 BS는 자신의 식별자를 다음에 생성될 식별자로 변경하지만 보관하고 있는 센서 노드의 식별자는 변경하지 않는다. BS는 초기에 설정된 BS와 센서노드의 식별자에서 자신의 식별자는 초기 설정된 $S^0_{0\ (BS)}$로 모든 센서 노드의 식별자는 Generator(G)을 통해 다음 식별자인 $S^1_{i\ (BS)}$로 바꾸어 저장한다. 센서 노드는 각자의 자신의 초기 식별자인 $S^0_{i\ (Sensor)}$와 BS의 다음 식별자인 $S^1_{0\ (Sensor)}$을 저장한다. 이는 통신할 때마다 송신자는 자신의 다음 식별자를 생성하여 그 식별자와 메시지를 전송하므로 수신자는 송신하는 센서 노드의 다음 식별자를 저장하고 있어야 식별자를 통해 어디로부터 온 메시지인지를 확인할 수 있다. 센서 네트워크가 초기에 구성되었을 때 BS와 센서노드의 식별자의 초기화는 위와 같은 방식으로 이루어지고 BS와 센서노드가 상호 인증을 위한 통신을 할 때의 식별자 변환 과정은 다음과 같다.

4-2-1 센서 노드에서 BS로의 통신

센서 노드는 주변의 환경에서 BS로부터 센싱 정보에 대한 요청이 들어왔을 때, 센싱한 정보를 BS로 전송하여야 한다. 센서노드 S_i는 식별자 $S^q_{i\ (Sensor)}$를 갖고 있을 때, 센서노드는 BS와의 통신을 위해 Generator(G)로 현재의 식별자에서 다음 식별자인 $S^{q+1}_{i\ (Sensor)}$로 바꾸고 생성된 식별자로 BS에 메시지를 전송한다. BS는 센서 노드로부터 받은 메시지가 정상적인 센서노드로부터의 메시지임을 인증되면 BS에 저장된 S_i의 식별자 $S^{q+1}_{i\ (BS)}$을 Generator(G)에 의해 $S^{q+2}_{i\ (BS)}$로 바꾼다. 이때 무선 환경에서는 메시지의 분실이 발생할 우려가 있다. 이 경우 각 센서노드의 식별자는 계속 변하지만 BS에 저장되어 있는 센서노드의 식별자는 변경되지 않는다. 즉 센서 노드와 BS가 저장하고 있는 식별자의 동기화가 필요하다. 메시지의 분실이 발생하였을 때 BS는 기대하고 있는 식별자를 받지 못하게 되는데 이 때, BS는 저장하고 있는 센서노드의 식별자를 최소 k번 Generator(G)를 실행하여 동일한 식별자를 갖는 센서노드를 확인한다. 여기서 k는 센서네트워크의 전송 신뢰도에 따른 값으로 통신 성공확률에 따른 값이다.

4-2-2. BS에서 모든 센서 노드로의 통신

BS에서 모든 센서 노드로의 통신은 자신의 식별자 변경의 공지, 혹은 각 센서 노드에게 센싱 데이터의 요구 등에 의해 이루어진다. 이 때, BS는 현재 자신의 식별자 $S^p_{0\ (BS)}$를 $S^{p+1}_{0\ (BS)}$로 변경하고 모든 센서 노드에게 공지 및 요구 메시지를 전송한다. 센서 노드가 받은 메시지가 정상적인 BS임을 인증되면 BS로부터 메시지를 받은 각 센서 노드도 각 저장하고 있는 BS의 식별자를 $S^{p+1}_{0\ (Sensor)}$에서 $S^{p+2}_{0\ (Sensor)}$로 변경한다. 메시지의 분실이 발생하였을 경우 식별자의 동기화를 위한 처리는 센서노드에서 BS로의 통신에서와 동일한 방법으로 실행한다.

5. 가변 식별자를 이용한 인증방법

본 논문에서의 가변 식별자는 각 노드의 식별은 물론 대칭키/공개키 알고리즘을 사용하지 않는 인증을 위한 키로 사용한다. 이는 인증을 위한 키관리의 오버헤드를 해소할 뿐만 아니라 수신자는 송신에 사용된 식별자를 통해 실시간 인증이 가능하다. 따라서 BS와 각 센서 노드에게 부여된 식별자는 구별이 가능하여야 하고 Generator(G)을 통해 생성되는 다음 식별자는 모든 센서 노드가 서로 다르게 생성되어야 한다.

5-3-1. 인증의 필요성

본 논문에서 제안하는 무선 센서 네트워크에서 인증은 2가지로 나뉘는데, 하나는 BS가 센서 노드를 인증하는 것이고, 다른 하나는 센서노드가 BS를 인증하는 것이다. BS의 센서 노드에 대한 인증이 필요한 이유는 공격자에 의해 네크워크에 삽입된 악성 센서 노드를 판별하여 잘못된 센싱정보의 수집을 방지하고 네트워크의 안정성을 도모함이다. 센서 노드가 BS를 인증하는 것 또한 공격자가 BS로 가장하여 주변의 센서 노드로부터 데이터를 수집하는 위장 공격을 방지하기 위함이다.

5-3-2. BS가 센서 노드를 인증

1. 센서 노드 S_i는 자신의 식별자 $S^q_{i\ (Sensor)}$를 Generator (G)를 통해 다음 식별자 $S^{q+1}_{i\ (Sensor)}$로 변환한다. ($S^{q+1}_{i\ (Sensor)} = G(S^q_{i\ (Sensor)})$)

2. 식별자 $S_i^{q+1}{}_{(Sensor)}$로 BS에게 인증메시지를 전달한다.

3. BS는 저장하고 있는 인증하고자 하는 센서 노드의 식별자 $S_i^{q+1}{}_{(BS)}$와 센서로부터 받은 식별자 $S_i^{q+1}{}_{(Sensor)}$를 비교하여 일치하는가를 확인한다.

4. 3에서 비교한 값이 일치하면 정상적인 센서노드에서 온 메시지임을 인증한다.

5. 일치하지 않으면 저장하고 있는 센서노드의 값을 Generator(G)을 통해 최소 k번까지 생성되는 값과 비교하여 수신된 센서 노드의 식별자와 동일한 값이 존재하는지 확인한다.(k값에 대한 결정은 인증의 신뢰도 관련이 있다.)

6. 5에서 동일한 값이 존재하면 정상적인 센서노드에서 온 메시지임을 인증한다.

7. 5에서 동일한 값이 존재하지 않으면 비정상적인 센서노드에서 온 메시지이므로 인증하지 않고 받은 메시지를 폐기한다.

8. 6에서 인증이 완료되면 BS에 저장하고 있는 센서노드의 식별자를 G에 의해 생성된 식별자로 업데이트 한다.

9. 4 또는 6에서 인증되면 그 때의 센서 노드의 식별자를 저장하고 인증되었음을 통보한다.

그림 4는 수신자의 송신자로부터 수신된 식별자의 인증을 위한 순서도로 수신된 식별자 $S_i^j{}_{(rec)}$와 수신자에 저장된 식별자 $S_i^t{}_{(str)}$의 일치여부와 일치하지 않을 경우 수신된 식별자 $S_i^j{}_{(rec)}$와 Generator(G) 식별자 $S_i^{t+k}{}_{(str)}$의 일치여부를 통해 인증을 하는 순서도이다.

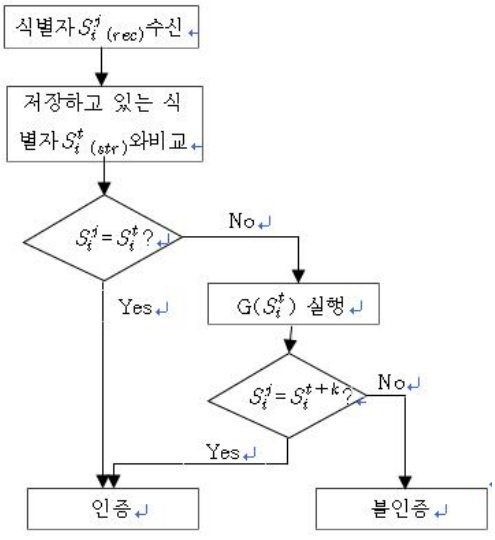

그림 4 인증 순서도

그림 5는 BS의 센서노드 인증에 대한 간략한 프로토콜이다.

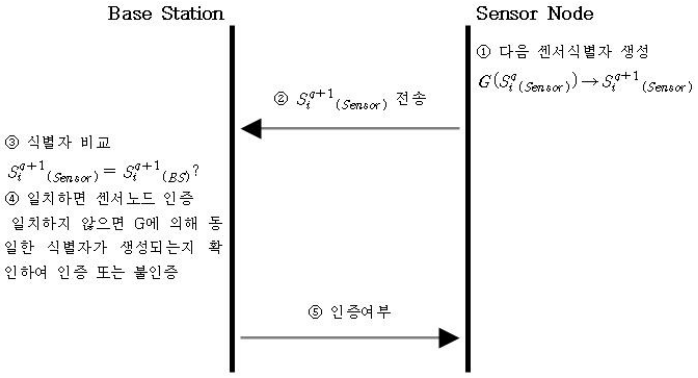

그림 5 BS의 센서노드인증

5-3-3. 센서 노드가 BS를 인증

센서노드가 BS를 인증하는 과정은 BS가 센서노드를 인증하은 과정과 동일하다. 그림 6은 센서노드의 BS에 대한 인증에 대한 간략한 프로토콜을 나타낸다.

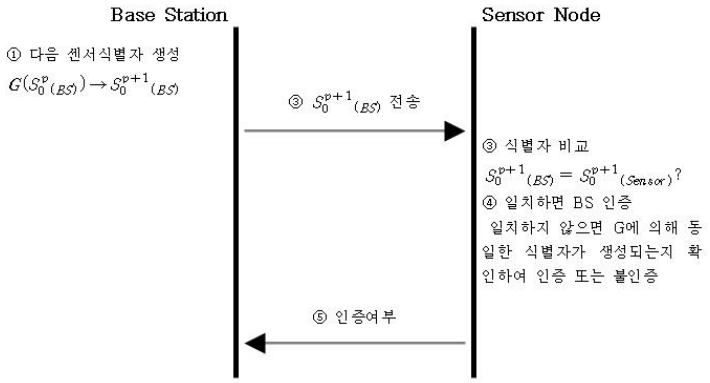

그림 6 센서 노드의 BS인증

6. 인증확률 논의

인증 단계에서 BS가 자신이 저장하고 있는 센서 노드의 식별자와 센서 노드에서 보내는 식별자가 일치하지 않을 경우가 발생하다. 이는 센서 노드로부터 BS로의 전송과정에서 메시지가 전달되지 않을 경우 발생하게 된다. 이때 메시지가 전달되지 않을 확률을 p이라 하고 전송할 때마다 전송에 실패할 확률이 독립적이라 가정할 때, k번 연속적으로 전송에 실패할 확률은 p^k이된다. 만약에 p가 $\frac{1}{2}$이고(전송 실패확률이 $\frac{1}{2}$일 경우), k가 5이면 (저장하고 있는 식별자의 개수), 전송 실패할 확률이 $\left(\frac{1}{2}\right)^5 = \frac{1}{32} \approx 0.031$이므로 매우 낮은 확률을 갖는다. 즉

전송실패 확률이 낮고 k값이 크다면 k번 연속 전송 실패할 확률은 매우 낮게 된다. 따라서 식별자의 값이 일치하지 않을 경우에도 적은 횟수의 G연산으로 인증 확률을 높일 수 있다.

7. 결론 및 향후 연구방향

무선 센서 네트워크는 한정된 자원과 연산 처리 능력을 가지고 있기 때문에 이런 특성에 맞는 통신 방법이 요구된다. 본 논문에서는 가변 식별자를 이용한 상호 인증 방법을 제시하였다. 제시된 방법은 대칭키나 공개키 알고리즘을 요구되지 않으며 공격자의 위장 공격에 대해 저항성을 가진다.

본 논문에서 제안한 방법은 무선 센서 네트워크상의 여러 라우팅을 고려하지 않고 단순히 BS와 센서 노드간의 통신 방안만을 제시하였기 때문에 다양한 라우팅과 네트워크 토폴로지를 적용한 연구가 필요하다.

참고문헌

[1] 김학범, “IP-USN 최신 기술 동향 및 보안요구 사항 분석”, 정보보호학회지 Vol 16, pp.64~73, 2006

[2] 박춘식, “유비쿼터스 센서 네트워크와 시큐리티 고찰”, 한국정보보호학회지, pp.12 ~ 20, 2004

[3] 김신효, 강유성, 정병호, 정교일, “u-센서 네트워크 보안 기술 동향”, 전자통신동향분석 제20권 제 1호, 2005

[4] A. Perring, R. Szewezyk, V. Wen D. Culler, J.D. Tygar, "SPINS : security protocols for sensor networks", Processing of ACM MobiCom'01, Rome, Ital, pp 189-199, 2001

[5] D. Henrici and Paul Muller, "Hash-based enhancement of Location privacy for Radio-Frequency Identification Devices using Varying Identifiers", PerSec'04 at IEEE PerCom, pp.149-153, 2004