논문 2006-43TC-6-3

무선 센서 네트워크에서의 효율적 Broadcast Authentication 방안

(An efficient Broadcast Authentication Scheme for Wireless Sensor Networks)

문 형 석*, 이 성 창**

(Hyung seok Moon and Sung chang Lee)

요 약

자원 제한적인 노드들로 구성되는 무선 센서 네트워크의 보안 알고리즘은 짧은 패킷 길이와 메모리, 컴퓨팅 능력, 전력 등의 자원 문제 때문에 기존의 보안 알고리즘을 적용하기가 힘들다. 주로 센서의 자원 사용이 상대적으로 덜하고, 키 길이가 짧은 공유키 기반의 알고리즘이 많이 사용되고 있지만 베이스스테이션의 브로드캐스트 패킷에 대한 인증을 위해서 단순히 전체 노드가 동일한 공유키를 가지는 방식은 적합하지 못하다. 최근 센서 네트워크에 적합한 형태의 브로드캐스트 인증 알고리즘으로, one-way 해쉬 함수를 이용한 키 체인생성과 키 체인의 각 키를 이용한 Message Authentication Code 생성, 지연된 키 공개를 이용한 알고리즘이 제안 되었다. 이러한 방식은 무선 센서 네트워크 환경에 적합한 인증 방식을 제공하지만 브로드캐스트 율, 키 체인 레벨 등, 네트워크의 각 조건에 따라 비효율적인 결과를 초래하기도 한다. 본 논문에서는 키 체인 링크 및 주기적 키 공개 방식을 이용하여 낮은 인증 딜레이를 보장하며, 패킷 송수신량과 수신 노드의 메모리 및 컴퓨팅 리소스를 효율적으로 사용할 수 있도록 개선된 브로드캐스트 인증 알고리즘을 제안하고, TinyOS의 TOSSIM으로 그 성능을 검증한다.

Abstract

It is difficult to apply conventional security algorithms to the wireless sensor networks composed of nodes that have resource constraints such as memory, computing, power resources limitation. Generally, shared key based algorithms with low resource consumption and short key length are used for broadcast packets in authentication of base station. But it is not suitable that all the nodes hold the same shared key only for packet authentication. Recently, broadcast authentication algorithm for sensor network is proposed, which uses key chain generation by one-way hash function, Message Authentication Code generation by each keys of the key chains and delayed key disclosure. It provides suitable authentication method for wireless sensor networks but may leads to inefficient consequence with respect to network conditions such as broadcast ratio, key chain level, and so on. In this paper, we propose an improved broadcast authentication algorithm that uses key chain link and periodical key disclosure. We evaluated the performance of proposed algorithm using TOSSIM(TinyOS Simulator) in TinyOS. The results show that the proposed algorithm ensures low authentication delay, uses memory and computing resource of receiving nodes efficiently and reduces the amount of packet transmitting/receiving.

Keywords: Wireless Sensor Networks, Broadcast Authentication, Message Authentication Code.

* 학생회원, 한국항공대학교 대학원 정보통신공학과
(Department of Information and Telecommunication Engineering, Graduate School of Hankuk Aviation University)
** 평생회원, 한국항공대학교 항공전자 및 정보통신공학부
(School of Avionics and Telecommunications, Hankuk Aviation University)
※ 이 논문은 2004년도 한국항공대학교 교비지원 연구비에 의하여 지원된 연구의 결과임.
접수일자: 2006년3월8일, 수정완료일: 2006년6월11일

I. 서 론

기존의 센서 네트워크에 대한 연구는 센서 노드의 제한된 리소스를 효율적으로 이용하여 적대적 환경에서 토폴로지를 유지하고 원하는 응용을 구현하는데 주안을 두고 진행되어 왔다. 그러나 최근 홈 네트워크를 중심으로 본격적인 유비쿼터스 네트워크를 이용한 서비스가

표 1. 대표적인 센서 노드인 SmartDust[6] 노드의 구성
Table 1. Composition of SmartDust Node as a representative sensor node.

CPU	8-bit, 4MHz
Storage	8KB instruction flash 512 bytes RAM 512 bytes EEPROM
Communication	916 MHz radio
Bandwidth	10Kbps
OS	TinyOS
OS code space	3500 bytes
Available code space	4500 bytes

실제 생활에 적용되면서 센서 네트워크에서의 보안 문제로 연구의 초점이 옮겨가고 있다.

센서 네트워크는 특정 응용에 특화된 형태를 가지며 일반적으로 베이스 스테이션(싱크)과 다수의 센서 노드들로 구성되어, 센서 노드가 측정한 정보를 베이스 스테이션이 수집하여 외부로 전달하고 베이스 스테이션이 센서 노드들에게 외부 데이터 및 쿼리를 전달하는 구조를 가진다. 센서 노드들은 메모리, 대역폭, 컴퓨팅 리소스 등에 많은 제약 사항을 가지며(표.1) 센서 네트워크에 적용되는 보안 알고리즘은 이러한 센서 노드의 제약사항하에서 효율적으로 동작하는 구조를 가져야 한다.[7] 본 논문의 주제인 broadcast authentication의 경우, 기존의 인증 알고리즘이 센서 네트워크에 적용될 수 없는 가장 큰 이유는 패킷의 오버헤드이다. 기존의 인증 알고리즘에서 널리 사용되는 전자서명 방식의 경우 패킷 당 약 50~1000 bytes의 오버헤드가 발생하여 약 36byte의 패킷길이를 가지는 센서 네트워크에는 적용할 수 없다. 따라서 센서 네트워크에 적용되는 보안 알고리즘은 기존의 방식과 다른 새로운 접근 방식이 필요하며 UC Berkeley[5]에서 제안한 SPINS[1](Security Protocol for Sensor Networks)는 현재까지 가장 센서 네트워크 환경에 적합한 보안 솔루션을 제공하는 알고리즘이라 할 수 있다. SPINS는 베이스 스테이션과 센서 노드 간에 미리 공유된 마스터 키를 이용하여 필요한 대칭키를 생성하며. 데이터의 무결성, 기밀성 및 인증기능을 제공하는 SNEP (Sensor Network Encryption Protocol)와 브로드캐스트 인증 기능을 제공하는 μTESLA (micro Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol) 두 블록으로 구성되어 있다. 본 논문에서는 μTESLA의 단점들을 보완한 Multilevel μTESLA[3] 알고리즘을 기반으로 베이스 스테이션의 브로드캐스트 패턴에 따른 성능을 평가하고, 브로드캐스트 패킷이 전체 채널 대역폭의 10%이하를 차지하는 일반적인 응용에서 개선된 성능을 제공하는 새로운 브로드캐스트 인증 알고리즘을 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 μTESLA, Multilevel μTESLA등의 관련 기술에 대하여 간단히 소개하고, Ⅲ장에서는 제안하는 알고리즘이 소개되며, Ⅳ장에서 제안 알고리즘과 Multilevel μTESLA의 성능이 시뮬레이션을 통해 비교 및 분석되었다. 끝으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. Related Works

1. An Overview of uTESLA

SPINS의 브로드캐스트 인증기능을 담당하는 μTESLA는 자원이 풍부한 일반적인 네트워크 환경에서 사용되는 인증 알고리즘인 TESLA[2][8]를 센서 네트워크에 적용할 수 있도록 경량화한 알고리즘이다. μTESLA의 주 아이디어는 one-way hash 함수를 이용한 키 체인의 생성과 키 체인을 이용한 구간별 MAC (Message Authentication Code)생성 및 지연된 키 공개 방식을 사용하는 것이다. 베이스 스테이션은 랜덤하게 선택된 K_n과 one-way hash 함수 H를 이용하여 키 체인 ($K_0 \sim K_n$)을 생성한다. 베이스 스테이션은 각 노드에게 K_0(commitment)를 포함한 초기 파라미터를 전달하고, 이후 start time 부터의 시간을 일정 구간으로 나누어 각 구간에서 키 체인의 키 K_i을 이용하여 브로드캐스트 패킷의 MAC을 생성한다. 수신 노드는 수신된 패킷의 MAC 키를 알지 못하므로 패킷을 바로 인증할 수 없다. 베이스 스테이션은 이전에 사용된 키 체인의 키를 일정 딜레이 이후에 공개하고, 공개된 키를 받은 수신노드는 키 생성에 사용된 해시 함수 H를 이용하여 수신 노드가 가지고 있는 commitment 또는 인증된 키 K_j (j<i)와 비교하여 키를 확인한다. 이후 이 키를 이용하여 버퍼에 저장된 브로드캐스트 패킷 중 해당 구간에 수신된 패킷을 인증하게 된다. 그림 1은 μTESLA동작의 한 예를 보여주는 것으로 P_1, P_2는 K_1, P_3는 K_2를 각각 패킷의 MAC 키로 사용하고 구간3에서 K_1을 공개하여 P_1, P_2가 인증되게 된다. one-way hash 함수를 이용한 키 체인의 생성과 지연된 키 공개 방식을 이용하는 μTESLA알고리즘은 패킷 당 8~10 byte 정도의 오버헤드만을 유발하며, 일정 딜레이 이후 효과적인 인증기능을 제공한다.

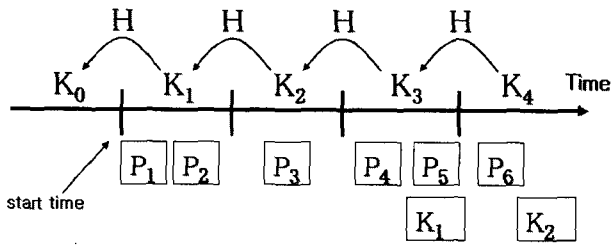

그림 1. μTESLA의 키 체인 사용 예
Fig. 1. An Example of key-chain in the μTESLA.

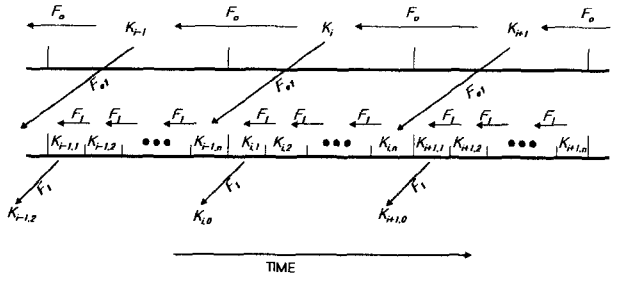

그림 2. Multilevel μTESLA의 2-level 키 체인 사용 구조
Fig. 2. Construction of 2-level key-chain in the Multilevel μTESLA.

2. An Overview of Multilevel uTESLA

μTESLA는 알고리즘에 필요한 초기 파라미터를 각 노드에게 개별적으로 전달한다. SPINS에서는 베이스 스테이션과 센서 노드의 unicast 통신 패턴의 보안 기능을 담당하는 SNEP를 이용하는데, 이 경우 센서 노드들의 수에 따라 초기 파라미터를 분배하는데 많은 시간이 걸리게 된다. 또한 베이스 스테이션이 생성한 키 체인의 길이에 따라 알고리즘의 수행시간이 한정되게 된다. Multilevel μTESLA는 초기 파라미터의 분배를 unicast 대신 broadcast 방식을 이용하는데 초점을 두고 제안된 일련의 스킴을 소개한다.

먼저 Multilevel μTESLA는 베이스 스테이션이 생성한 키 체인을 직접 패킷의 MAC 키로 사용하지 않고, 또 다른 키 체인을 생성하는데 사용한다. 즉, 베이스 스테이션이 초기에 생성한 키 체인의 길이가 n인 경우 또 다른 m길이의 하위레벨 키 체인이 n개 생성될 수 있다. 이 경우는 2레벨의 키 체인을 사용하는 것으로 실제로 패킷의 MAC 생성에 사용되는 키는 각 체인의 commitment를 제외한 $n\times(m-1)$개가 된다. 그림2의 예에서 총 3개의 one-way 해시 함수(F_0, F_{01}, F_1)를 사용하여 2레벨의 키 체인을 구성한 예를 보여준다. 이때 하위 레벨 키 체인이 직접 패킷의 MAC 생성에 사용되는 키이다. 사용된 하위 레벨의 키들은 일정 딜레이 이후 브로드캐스트 되는 데이터 패킷에 포함되어 수신노드들에게 분배 되게 된다. 또한 Multilevel μTESLA는 하위 레벨의 키 체인 commitment를 분배 하는데 사용되는 패킷(*CDM, Commitment Distribution Message*)을 따로 사용한다.

$$CDM_i = i \,|\, K_{i+2,0} \,|\, MAC_{K'_i}(i \,|\, K_{i+2,0}) \,|\, K_{i-1}$$

CDM_i는 상위 한 구간에서 중복해서 브로트캐스트 되는데, 이는 무선 채널의 손실에 의해 CDM_i에서 분배하는 i+2구간의 키 체인 commitment인 $K_{i+2,0}$이 전달되지 못할 경우 상위 i 구간동안의 모든 브로드캐스트 메시지가 인증 받지 못하기 때문이다. 이렇게 동일한 CDM이 상위 한 구간동안 중복 브로드캐스트 되는 경우 CDM_i를 수신한 공격자가 생성한 위조된 CDM''_i에 의해 DOS 공격이 가능해진다.

$$CDM''_i = i \,|\, K''_{i+2,0} \,|\, MAC''_{K'_i}(i \,|\, K_{i+2,0}) \,|\, K_{i-1}$$

위조된 CDM''_i를 수신한 노드는 다음 상위구간의 CDM_{i+1}에서 공개하는 K_i를 받기 전까지는 위조된 CDM_i를 구별할 수 없다. Multilevel μTESLA에서는 이러한 DOS 공격에 대응하기 위하여 베이스 스테이션에서는 한 구간에서 중복 브로드캐스트 되는 CDM의 개수를 조절하고, 수신노드에서는 Multiple Buffer Random Selection 기법을 사용하여 DOS 공격의 성공률을 일정 수준 이하로 줄인다. Multilevel μTESLA의 이러한 전략은 μTESLA를 바탕으로 알고리즘의 수행시간을 확장하고, 센서 네트워크 환경에 적합한 형태의 인증 기능을 제공하지만, 베이스 스테이션과 센서 노드들 간에 다양한 통신 패턴이 존재하고 베이스 스테이션의 브로드캐스트 데이터율이 일정 수준 이하일 때는 필요 이상의 오버헤드가 발생하며 키 체인 레벨의 증가에 따른 CDM패킷의 증가 등의 비효율적 결과를 나타낼 수 있다.

본 논문에서 제안하는 알고리즘은 Multilevel μTESLA를 바탕으로 일반적인 센서 네트워크 응용에서 베이스 스테이션의 브로트캐스트 패턴을 감안하여 안정된 인증 딜레이를 제공하고 센서 노드의 자원 이용률을 효율적으로 개선한 알고리즘을 소개한다.

III. Solution Approach

Multilevel μTESLA는 멀티레벨의 키 체인을 사용하여 전체 알고리즘의 수행시간을 확장하였고, 최하위 레벨의 키 체인을 제외한 상위 각 레벨에서 CDM을 사용하여 키 체인 commitment와 상위 구간의 키를 공개 하도록 하였다. 이러한 구조는 앞서 언급한 바와 같이 μTESLA의 단점을 보완한다. 그러나 멀티레벨의 키 구조를 사용함에 따라 각 레벨의 개별적인 키 공개 및 CDM 분배가 이루어져야 하며, DOS 공격에 대응하기 위한 CDM의 중복으로 인하여 낮은 브로드캐스트 데이터율에서는 패킷 송수신량 및 인증 딜레이에서 매우 비효율적인 결과를 나타내게 된다.

먼저, Multilevel μTESLA에서 CDM위조에 의한 DOS 공격에 대응하기 위하여 상위 한 구간에서의 CDM 중복 횟수는 아래의 식에 의해 결정된다.

$$Rc \geq (1-Rd)(1-\sqrt[m]{1-P}) \quad (1)$$

식(1)에서 Rc, Rd는 각각 채널의 전체 가용 대역폭에서 CDM 과 브로드캐스트 데이터가 차지하는 비율을 말한다. m은 Multiple Buffer Random Selection 알고리즘에서 사용되는 수신 노드의 CDM 버퍼수를 나타내며, P는 수신노드가 인증된 CDM가질 확률의 최소값을 나타낸다. 즉, 수신노드가 인증된 CDM을 가질 확률이 최소한 99%이상을 보장 한다고 할 때, P는 0.99가 된다. 이 식은 전체 채널에서 CDM이 차지하는 비율, 즉 CDM의 중복횟수는 Rd에 의해 결정되며 Rd가 낮을수록 Rc의 값은 커진다. 일반적으로 센서 네트워크를 구성하는 센서 노드는 매우 빈약한 자원을 가지며, 특히 배터리에 의한 전원공급이 대부분이므로 일반적으로 전력 소모가 큰 패킷의 송수신을 최소화 하도록 응용 및 라우팅을 설계한다. 베이스 스테이션의 브로드캐스트 데이터를 최소화 할 경우 Multilevel μTESLA에서는 CDM의 송신 횟수가 증가하게 되므로 비효율적으로 자원을 사용하게 된다. 또한 MAC생성 시 사용된 최하위 레벨의 키는 일정딜레이 이후 브로드캐스트 되는 데이터 패킷에서 공개 되므로 데이터 패킷의 브로드캐스트 율이 낮거나 일정하지 못한 경우 안정된 인증 딜레이를 얻기 힘들다. 제안하는 알고리즘은 이러한 문제점을 해결하기 위하여 멀티레벨로 구성된 키 체인을 하나의 레벨로 사용하도록 하여 CDM을 없애고, MAC에 사용된 키 공개를 각 구간 당 한 번씩 브로드캐스트 되는 KDM (Key Distribution Message)에서 수행하도록 한 개선된 Multilevel μTESLA알고리즘을 제안한다. 베이스 스테이션에서 랜덤하게 선택된 K_n을 통해 $K_0 \sim K_n$의 키 체인을 생성하고, 이 키들을 통해 또 다른 키 체인을 생성하도록 하는 것이 Multilevel μTESLA의 키 체인구조이다. 이는 한번 생성된 키 체인길이에 의해 제한되는 알고리즘 수행시간을 연장할 수 있도록 한다. 제안하는 알고리즘에서는 최상위 키 체인을 생성한 후 하위 레벨의 키 체인 생성 시, 최상위 키 체인을 직접 하위레벨 키 체인의 마지막 키 $K_{n,m}$으로 사용하여 하나의 키 구조로 만든다. 그림 3은 2레벨의 예로, 베이스 스테이션은 랜덤하게 선택된 $K_{n,m}$과 one-way 해시 함수 H_2를 이용하여 상위레벨 키 체인 $K_{m,n} \sim K_{0,n}$을 만든다. 키 체인에서 commitment를 제외한 모든 키 들은 다시 H_1을 통해 하위레벨 키 체인을 생성하며, 레벨에 상관없이 commitment를 제외한 모든 키들은 직접 MAC생성 시 사용된다. 이때 각 구간 당 하나씩 키가 사용된다면, 브로드캐스트 데이터가 없는 경우에도 키는 계속 업데이트 되며, 브로드캐스트 데이터 율이 낮은 경우 키 체인의 낭비로 이어진다. 일반적으로 베이스스테이션의 브로드캐스트 데이터 율이 높지 않다고 간주하여 제안하는 알고리즘은 각 구간에서 브로드캐스트 데이터가 있는 경우에만 키를 업데이트 한다. 그림4에서는 2레벨 키 체인을 사용한 예를 보여준다. 첫 번째 구간에서 데이터가 브로드캐스트 된 후, 두 번째 구간에서는 브로드캐스트 데이터가 없으므로 키 갱신은 일어나

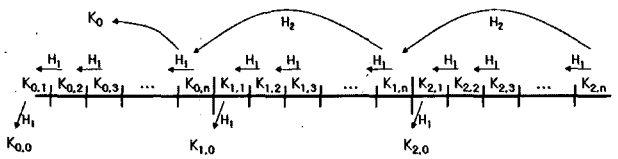

그림 3. 제안된 알고리즘의 키 체인구조 (2레벨 예)
Fig. 3. The key-chain structure of proposed algorithm.

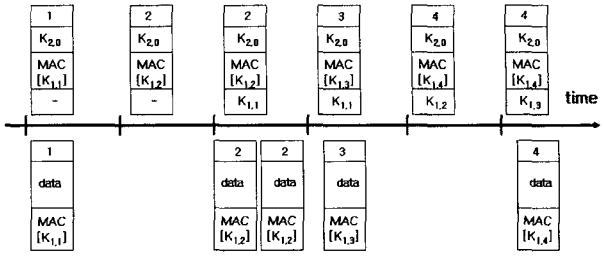

그림 4. 2-레벨 키 체인 구조를 사용한 제안된 알고리즘 동작 예
Fig. 4. An example of proposed algorithm using 2-leve key-chain.

지 않는다. 세 번째 구간에서 데이터가 브로드 캐스트 되며, 각 MAC 키는 KDM에 의해 최소 1구간의 딜레이 이후 공개 된다. μTESLA와 마찬가지로 키 공개 딜레이는 초기 파라미터 분배 시 결정하게 되며, 하위 1구간당 한 번씩의 주기적 키 공개를 한다. 제안된 키 체인 구조 및 키 공개과정은 안정된 인증 딜레이를 제공할 수 있고, 낮은 브로드캐스트 데이터율에서 패킷 송수신량을 줄일 수 있다.

다음 장에서는 인증 딜레이와 일정량의 브로드캐스트 데이터를 보내는데 필요한 패킷 수 및 전체 패킷에서 실제 데이터가 차지하는 비율을 시뮬레이션을 통해 Multilevel μTESLA와 비교한다.

Ⅳ. 시뮬레이션

본 장에서는 TOSSIM[4]을 이용한 시뮬레이션을 통하여 제안된 알고리즘과 Multilevel μTESLA의 성능을 비교 분석한다.

시뮬레이션 환경은 Multilevel μTESLA와 마찬가지로, 하나의 베이스 스테이션과 다수의 센서 노드로 구성된 네트워크 환경에서, 베이스 스테이션과 센서 노드간의 무선 채널은 10Kbps이며 TinyOS의 36byte packet 구조를 사용한다고 가정한다. 첫 번째로 일정시간동안 베이스 스테이션에서 센서 노드로 브로드캐스트된 데이터 패킷의 인증 딜레이를 측정하였다.

1. 일정 시간동안 데이터 패킷의 인증 딜레이

그림 5는 채널의 손실율이 10%이며 브로드캐스트 데이터가 전체 채널의 5%를 차지하는 가정 하에 일정 시간 동안의 인증 딜레이를 보여준다. 결과에서 확인할 수 있듯이 Multilevel μTESLA에서 최하위 레벨의 마지막 구간에 사용된 키 공개 패킷이 손실 되었거나, 이후 일정시간 동안 브로드캐스트 데이터가 없어서 키가 공개되지 못 할 경우 상위 한 구간 이후 공개되는 CDM에 의해 인증 될 경우 인증 딜레이는 사실상 인증자체가 무의미해 질 정도로 높아진다. 특히 무선 센서 네트워크에서 베이스 스테이션의 브로드캐스트 데이터가 주로 경로 설정을 위한 beaconing 분배를 위해 사용된다고 할 경우 상위 한 구간에 해당하는 인증 딜레이는 인증 자체를 무의미 하게 한다. 그림 6은 Multilevel μTESLA에서 그림5의 결과와 같이 상위 한 구간 이후의 인증 기능을 제거한 경우의 인증 딜레이를 측정 하였다. 결과에서 알 수 있듯이 키 공개를 브로드캐스트 데이터

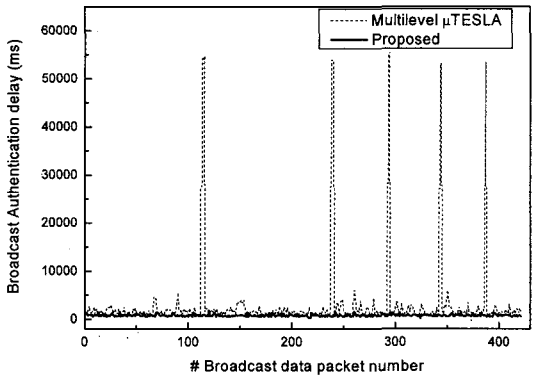

그림 5. 일정시간 동안 수신한 각 패킷의 인증딜레이
Fig. 5. Authentication delay for each received packet during a certain period of time.

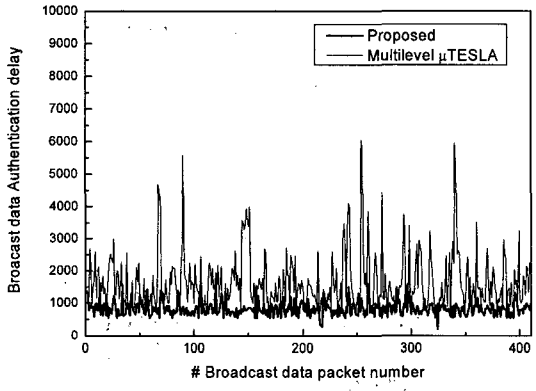

그림 6. 상위 구간 키 체인에 의한 인증을 제외한 일정 시간 동안 수신한 각 패킷의 인증딜레이
Fig. 6. Authentication delay for each received packet except authentication by high level key-chain during a certain period of time.

패킷에 의존하는 Multilevel μTESLA와 달리 구간 당 한 번씩의 일정한 키 공개가 이루어 질 경우, 훨씬 안정된 인증 딜레이를 얻을 수 있음을 확인하였다.

2. 브로드캐스트 데이터의 평균 인증 딜레이

이번 실험은 베이스스테이션의 브로드캐스트 데이터율 따른 평균 인증딜레이를 측정하였다. 실험 1과 마찬가지로, Multilevel μTESLA는 상위 한 구간 이후에 이전구간의 인증을 지원하지 않는 경우 (Multilevel μTESLA2) 도 실험에 포함 하였다. 그림7은 전체 채널에서 브로드캐스트 데이터가 차지하는 비율 (본문에서 Rd)에 따른 일정 시간동안의 평균 인증 딜레이를 보여준다. 제안된 알고리즘의 경우 앞서 언급한 바와 같이 일정한 키 공개가 이루어지므로 베이스 스테이션의 브

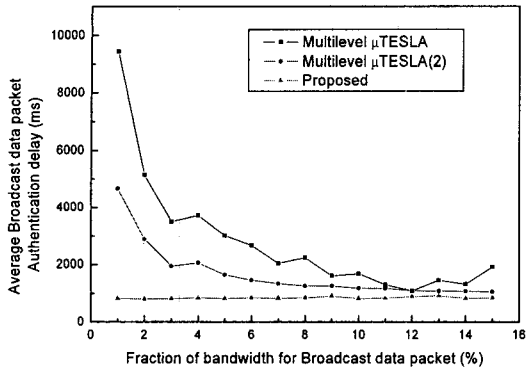

그림 7. 베이스 스테이션의 브로드캐스트 율에 따른 평균 인증 딜레이

Fig. 7. Average authentication delay according to broadcast ratio of base station .

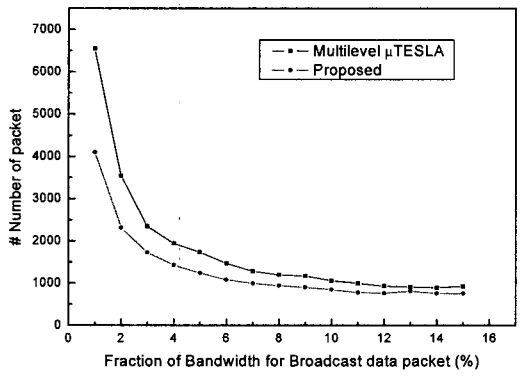

그림 8. 500개의 브로드캐스트 데이터 패킷을 송신하는데 필요한 전체 패킷 수

Fig. 8. Total number of packets required to transmit 500 broadcast data packets.

로드캐스트 데이터율과 상관없이 일정한 인증율을 보이는 반면, Multilevel μTESLA는 베이스 스테이션의 브로드캐스트 패턴에 따라 인증딜레이가 변화하므로 일정한 인증 딜레이를 기대하기 어려우며, 베이스 스테이션의 브로드캐스트 횟수를 줄일수록 인증딜레이는 늘어나게 된다. 마찬가지로 브로드캐스트 횟수가 줄어들수록 Multilevel μTESLA의 경우 중복 CDM의 개수가 늘어나는데, 이러한 결과는 그림 8에서 알 수 있다. 그림 8은 Rd가 1~15%까지 변화하는 동안 500개의 데이터 패킷을 보낼 때 필요한 패킷의 개수를 나타낸다. 제안된 알고리즘의 매 구간 KDM을 브로드캐스트 하는 경우 비슷하거나 더 적은 패킷으로 안정된 인증 딜레이를 제공함을 알 수 있다.

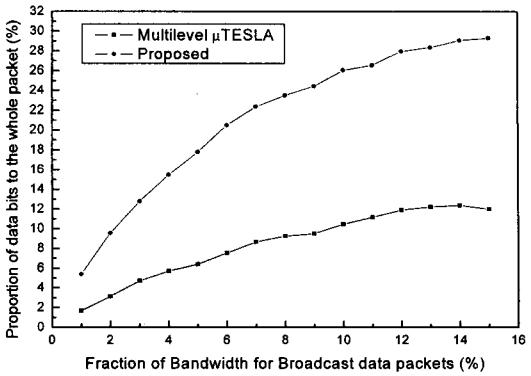

그림 9. 500개의 브로드 캐스트 데이터를 송신하는 동안 노드가 수신한 전체 패킷에서 데이터(byte)가 차지하는 비율

Fig. 9. A proportion of real data to whole received packets during transmitting 500 broadcast data packets.

3. 노드가 수신한 전체 패킷에서 실제 데이터가 차지하는 비율

마지막으로 그림 9는 베이스 스테이션이 500개의 데이터 패킷을 보내는 동안, 센서 노드가 수신한 전체 패킷에서 실제 데이터가 차지하는 비율을 측정한 결과이다. Multilevel μTESLA의 경우 데이터 패킷이 키 공개를 담당하므로 키 길이에 해당하는 8byte의 영역을 공개되는 키가 차지하게 된다. 또한 앞서 실험에서 확인하였듯이 중복 CDM의 횟수는 일정 수준 이하의 Rd에서는 매 구간 키 공개 패킷을 브로드캐스트 하는 제안된 알고리즘의 방식보다 더 많은 패킷이 필요하게 된다. 따라서 전체 수신된 패킷에서 실제 데이터가 차지하는 비율 면에서 제안된 알고리즘은 더 높은 효율성을 제공한다.

V. 결 론

본 논문에서는 기존에 제안된 Multilevel 키 체인 구조 및 지연된 키 공개 방식을 기반으로 효율적 자원 이용 및 안정된 인증 딜레이를 제공 할 수 있도록 개선된 베이스스테이션의 브로드캐스트 인증 알고리즘을 제안하였다. 센서 노드는 그 특성상 자원 이용의 효율성이 우선시 되어야 한다. 그러나 본격적으로 유비쿼터스 네트워크 서비스가 실용화되는 단계에서 개인 정보 유출, 사생활 침해 등의 보안 문제가 이슈화 되면서 센서 네트워크의 보안 문제는 보안성능과 자원 이용의 효율성 사이에서 적절한 타협점을 찾아야만 한다.

본 논문에서는 일정하고 낮은 인증 딜레이를 보장하며, 수신 노드의 메모리 및 컴퓨팅 능력을 효율적으로 사용하며, 패킷 송수신량이 기존의 알고리즘에 비하여 적은 브로드캐스트 인증 알고리즘을 제안하였다. 또한, 제안된 알고리즘의 성능을 시뮬레이션 결과를 통해 검증하였다.

참 고 문 헌

[1] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks", In Proceedings of Seventh Annual International Conference on Mobile Computing and Networks, Rome, Italy, July 2001.

[2] Adrian Perrig, R. Canetti, Briscoe, J.D. Tygar, and D. Song, "TESLA:Multicast source authentication transform". IRTF draft, draft-irtf-smug-tesla-00.txt, November, 2000.

[3] Donggang Liu, Peng Ning, "Multi-Level μ TESLA: A Broadcast Authentication System of Distributed Sensor Networks", ACM Transaction on Embedded Computing Systems(TECS), vol 3, No 4, pages 800~836, November, 2004.

[4] Philip Levis, Nelson Lee, Matt Welsh, and David Culler, "TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications", Proceedings of the First ACM Conference on Embedded Networked Sensor Systems (SenSys 2003), November, 2003.

[5] Chris Karlof, Naveen Sastry, and David Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks". Proceedings of the 2nd international conference on Embedded networkds sensor systems, pages 132~175, November, 2004.

[6] Kris S. J. Pister, Joe M. Khan, Bernhard E. Boser, "Smart Dust: Wireless Networks of Millimeter-Scale Sensor Nodes", Highlight Article in 1999 Electronics Research Laboratory Research Summary. 1999.

[7] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings for the first IEEE International Workshop on Sensor Network Protocols and Applications (SNPA 2003), pages 113~127, May, 2003.

[8] Adrian Perrig, Rand Canetti, Dawn Song and J. D. Tygar, "Efficient and Secure Source Authentication for Multicast", Proceedings of Network and Distributed System Security Symposium. San Diego, California, February, 2001.

저 자 소 개

문 형 석(학생회원)
2005년 한국항공대학교 정보통신공학과 학사.
2005년~현재 한국항공대학교 정보통신공학과 석사과정
<주관심분야 : 센서 네트워크, 홈 네트워크, UWB>

이 성 창(평생회원)
1976년~1983년 경북대학교 전자공학과 학사.
1983년~1985년 한국과학기술원 전기 및 전자 공학과 석사.
1985년~1987년 한국과학기술원 시스템공학센터 연구원
1987년~1991년 Texas A&M University 공학박사
1992년~1993년 한국전자통신연구원
1993년~현재 한국항공대학교 정보통신공학과 교수
<주관심분야 : BcN, 홈네트워크, 유비쿼터스 네트워크>