UWSN을 위한 새로운 Tree기반의 브로드캐스트 인증 기법

*최진춘, *양대헌, **이경희
*인하대학교, **수원대학교 전기공학과

A New Tree-based Broadcast Authentication Scheme for UWSN

*JinChun Choi, *DaeHun Nyang, **KyungHee Lee
*INHA University, **University of Suwon

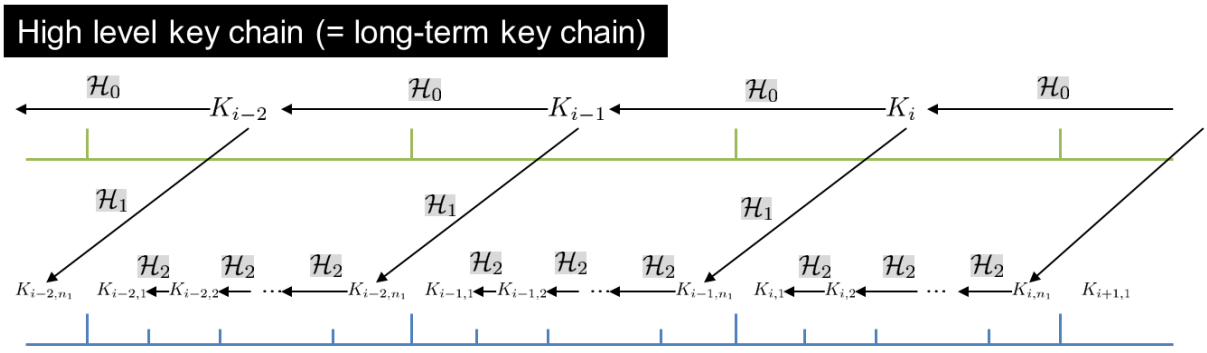
요 약

무선 센서 네트워크에서의 브로드캐스트는 공격자에 의해 다양한 공격을 받을 수 있다. 그 중 BS(Base Station)으로 위장한 공격자가 센서 노드들의 배터리 소모 등의 목적으로 악의적인 메시지를 전송하는 경우 센서 노드들은 이러한 메시지를 그대로 수신하는 것이 아니라 브로드캐스트 인증 기법을 통해 안전한 메시지만을 수신하여야 한다. 이 논문에서는 Tree 기반의 브로드캐스트 인증 기법을 제안하였다.

I. 서론

BS(Base Station)가 상주하지 않는 무선 센서 네트워크(Unattended Wireless Sensor Network)에서 이루어지는 브로드캐스트 메시지는 무선 센서 네트워크의 특성상 공격자가 메시지를 수정하여 재전송하거나 공격자의 의도가 담겨있는 악의적인 브로드캐스트 메시지를 전파하기 쉽다. 따라서 이러한 일들을 막기 위하여 다양한 브로드캐스트의 인증 기법에 대한 연구가 이루어지고 있다. 그 중 하나로 μTESLA[1]가 있다. μTESLA는 BS(Base Station)에서 센서 노드로 브로드캐스트 메시지를 전달할 때 BS가 미리 생성한 해시 체인으로 만들어진 키를 이용하여 MAC을 생성한 뒤 메시지와 함께 붙여서 전송한다. 그리고 센서 노드에게 일정 시간 후에 MAC을 생성할 때 사용한 해시 체인의 이전 값을 키로 전송함으로써 센서 노드는 이전에 전송한 메시지가 BS로부터 전송된 것임을 인증할 수 있다. 하지만 μTESLA에서는 인증에 사용되는 키를 공개하는 데 걸리는 시간, 즉 키 슬롯의 길이와 센서 노드들이 BS로부터 메시지를 받아 동작하는데 걸리는 시간과의 트레이드-오프 관계가 있다. UWSN인 경우에 사용하는 키 슬롯의 길이를 짧게 설정하면 BS의 방문주기에 따라 센서 노드들이 수행해야 하는 해시 함수의 횟수가 증가하게 되며, 해시 함수의 수행 횟수를 줄이기 위해 키 슬롯의 길이를 길게 설정한다면 BS가 방문하여 메시지를 센서 노드들에게 전달하고 인증하는 데에 걸리는 시간이 길어지게 된다. 이는 μTESLA의 특성상 메시지의 MAC을 인증하기 위해서는 최소한 하나의 키 슬롯 시간이 지난 후에 인증키를 전송해야 하기 때문이다.

이 논문의 2장에서는 기존의 브로드캐스트 인증 기법에 대해 알아보고, 3장에서는 이 논문에서 제안하는 트리 기반의 브로드캐스트 인증 기법에 관하여 설명하였다. 마지막으로 4장에서는 결론을 맺는다.



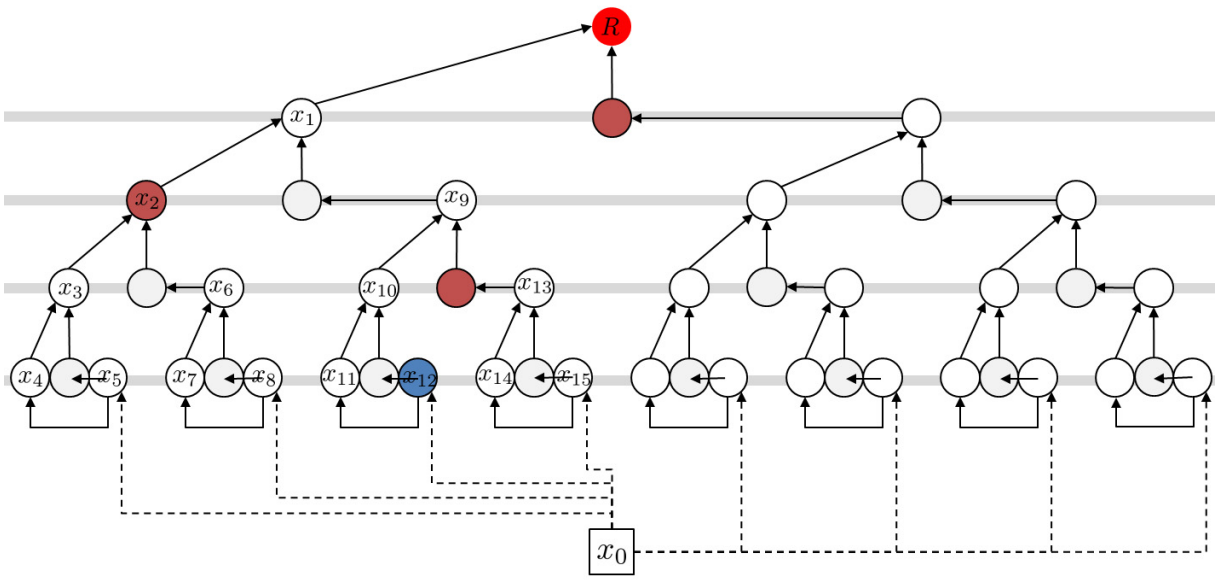
[그림 1] 멀티레벨 μTESLA

II. 기존의 브로드캐스트 인증 기법

기존에 무선 센서 네트워크에 존재하는 브로드캐스트 인증 방법으로는 서론에서 다룬 바 있는 μTESLA가 있다. 그리고 μTESLA에서 해시 체인이 길어질 때의 문제점을 해결하기 위한 방법 중 하나로 멀티레벨-μTESLA[2]가 있다. 이것은 [그림 1]과 같이 구성되어 있으며 해시 체인이 극단적으로 길어지는 경우에 유용하게 사용된다. 또 다른 방법으로는 DoS공격에 안전한 브로드캐스트 인증 기법[3]이 있다. 이 기법은 기존의 멀티레벨-μTESLA가 DoS공격 대상이 될 수 있음을 지적하며 제안되었다. 이 기법에서는 μTESLA의 파라미터로 머클 해시 트리(Merkle Hash Tree)[4]를 사용하였다. 이렇게 하면 μTESLA에서의 인증 지연 시간을 없앨 수 있기 때문에 DoS공격을 방지할 수 있다.

III. 제안하는 트리 기반의 브로드캐스트 인증 기법

이 논문에서는 UWSN 환경에서의 트리 기반의 브로드캐스트 인증 기법에 대해 연구하였는데, μTESLA를 사용할 때 해시 체인을 사용하는 대신 해시 트리를 사용하였다. 기존의 기법[3]과는 다르게 [그림 2]와 같이 트리를 구성하였다. 트리에서 우측 가지에 연결된 노드 사이에 링크를 하나 추가하여 사용하며 이 링크의

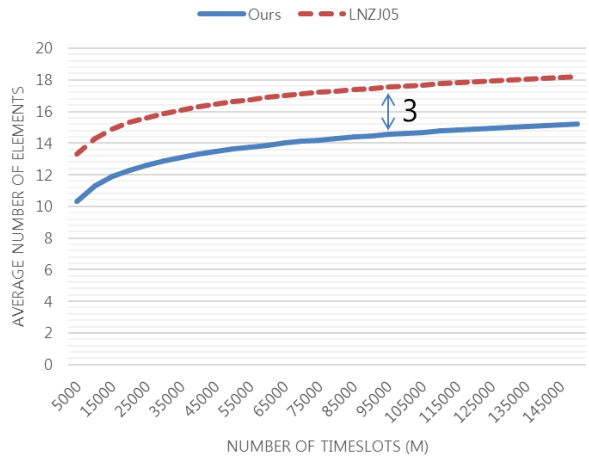


[그림 2] 트리 기반의 브로드캐스트 인증 기법

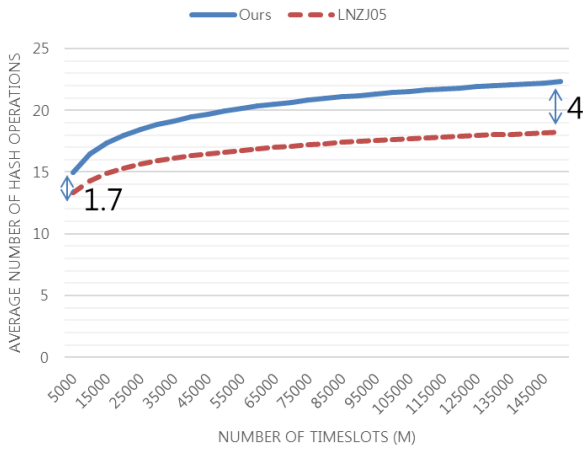
수는 ℓ으로 표현한다. [그림 2]의 트리는 $\ell = 1$인 트리의 모습이다. 트리의 루트 값인 R은 각각 센서 노드들이 미리 가지고 있는 값으로 센서 노드가 받은 키가 BS로부터 전송받은 키인지 인증할 때 사용하며, x_0값은 해시를 구성하는 초기 값으로 트리의 리프 노드들은 x_0으로부터 각각 다른 형태로 패딩된 값으로 구성한다. 리프 노드 중에서 x_{12}값을 키로 사용하기 위해서는 x_{12}와 x_{12}를 해시하여 나온 결과 값인 x_{11}값, 그리고 x_{13}을 해시하여 나온 값, x_2값, x_1의 형제 노드에 있는 값을 사용하여 만든 값을 루트에 있는 값 R과 비교하여 인증과정을 수행할 수 있다. 이는 만약 원래 기법에서 x_{12}를 키 값으로 사용하기 위해서 전송해야 하는 형제 노드인 x_{11}값을 전송할 필요 없이 x_{12}로부터 해시 연산을 통해 만들어낼 수 있으므로 전송해야 하는 메시지의 개수가 줄어들게 된다. 따라서 이러한 방법을 사용하면 [그림 3]에서처럼 $\ell = 1$인 경우에는 기존의 기법[3] 보다 평균 사용되는 원소의 개수가 3개 적어진다. 이는 한 번에 전송할 수 있는 패킷의 크기가 제한적인 무선 센서 네트워크에서 보내는 패킷의 개수를 줄일 수 있는 장점이 있다. 하지만 이 역시 트레이드-오프 관계에 있는 변수가 있는데 [그림 4]의 그래프를 보면 평균 해시 연산 횟수가 기존의 기법보다 최소 1.7회부터 사용되는 키 슬롯이 많아질수록 늘어나게 된다. 이는 무선 센서 네트워크의 구성에 따라 사용되는 평균 원소의 개수를 줄여서 네트워크의 혼잡 상황을 피해야 될 때에는 사용하기에 적합할 것이며, 해시 함수의 연산의 횟수가 센서 노드의 수명이나 네트워크의 운영에 영향을 작게 미치는 경우에는 이러한 기법을 사용할 때 얻는 이점이 클 것으로 보인다.

IV. 결론

본 논문에서는 무선 센서 네트워크에서의 브로드캐스트 메시지 인증에 있어서 기존의 기법을 분석하고, 트리 기반의 브로드캐스트 메시지 인증 기법을 제안하였다. 기존의 μTESLA를 적용하였을 경우에는 키 슬롯의 길이에 따라서 센서 노드들이 처리해야 하는 해시 연산의 수가 급격하게 늘어날 수 있는 문제점이 있었다. 이것을 해결하기 위한 방법으로 멀티레벨-μTESLA를 사용할 수 있는데, 멀티레벨-μTESLA는 High-level 키 체인과 Low-level 키 체인을 사용함으로써 많은 해시 체인을 사용할 때에도 운영할 수 있다. 하지만 이는 μTESLA의 특성상 존재하는 인증하는 키의 노출되는 시간이 지연되는 문제 때문에 발생할 수 있는 DoS공격에 대해 취약하게 된다. 이 논문에서는 UWSN 환경에서 발생하는 브로드캐스트 메시지를 인증하는 방법으로 μTESLA에서 사용하



[그림 3] 평균 원소 개수 비교



[그림 4] 평균 해시 연산 비교

는 해시 체인 대신 해시 트리를 이용한 기법을 제안하였다. 제안한 기법은 무선 센서 네트워크 내에서 전달되는 패킷의 개수가 네트워크의 운영에 중요한 역할을 하는 경우에 브로드캐스트 메시지 인증에 사용하는 원소의 개수를 줄일 수 있고, 원소의 개수를 줄임으로써 네트워크에서 사용되는 패킷의 평균 개수를 줄일 수 있다. 앞으로의 연구에서는 네트워크 시뮬레이터를 이용하여 μTESLA 등의 기법과 이 논문에서 제안하는 기법을 시뮬레이션 하여 비교·분석 할 수 있을 것이다.

[참고문헌]

[1] A. Perrig, R. Canetti, J.D. Tygar and D. Song, "The TESLA broadcast authentication protocol" Proceedings of RSA CryptoBytes'02, 2002.

[2] Liu, D., Ning, P., "Multilevel μTESLA: Broadcast authentication for distributed sensor networks." ACM Transactions on Embedded Computing Systems (TECS), 3(4), 800-836, 2004

[3] Liu, D., Ning, P., Zhu, S., & Jajodia, S., "Practical broadcast authentication in sensor networks." Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on (pp. 118-129). IEEE. Jul, 2005.

[4] R. Merkle, "Protocols for public key cryptosystems," Proceedings of the IEEE Symposium on Research in Security and Privacy, Apr 1980.