

WSN에서 그룹 코드 검증 방법에 관한 고찰

*최진춘, *양대현, **이경희

*인하대학교, **수원대학교 전기공학과

Study of Group Code Attestation Scheme in Wireless Sensor Network

*JinChun Choi, *DaeHun Nyang, **KyungHee Lee

*INHA University, **University of Suwon

요 약

무선 센서 네트워크는 그 특성상 센서 노드들이 악의적인 공격자에 의해 공격받기 쉽다. 특히 공격자가 의도한 임의의 동작을 수행하는 오염된 센서 노드(Compromised Sensor Node)를 네트워크 내에 배치하는 등의 공격을 할 수 있다. 이러한 공격을 막기 위한 방법 중 하나로 센서 노드간의 코드 검증을 수행할 수 있다. 이 논문에서는 브로드캐스트를 이용하는 그룹 코드 검증 방법에 대해 논의하였다.

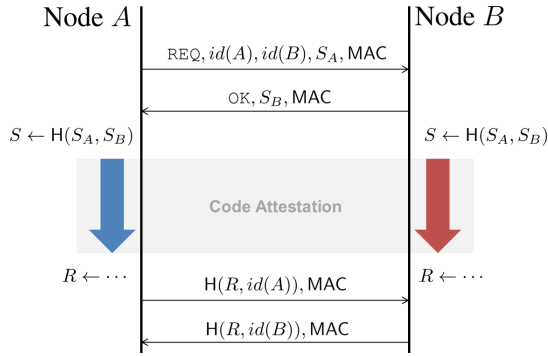
I. 서론

무선 센서 네트워크(Wireless Sensor Network)에서 센서 노드는 넓은 공간에 배치되어 임무를 수행하는 경우가 많다. 이렇게 배치된 센서 노드는 악의적인 목적을 가진 공격자에게 노출되기 쉽다. 공격자는 센서 노드에 접근하여 센서 노드를 무력화 하거나, 센서 노드에 직접 연결하여 공격자가 원하는 임의의 코드를 삽입할 수도 있다. 이러한 공격에 대응하는 방법으로 센서 노드들 간의 검증 기법을 사용하여 임의로 추가된 센서 노드로부터의 공격을 방지할 수 있다. 이 논문에서는 멀티 홉 센서 네트워크에서 센서 노드들 간의 요구와 응답 방식의 코드 검증 기법과 멀티 홉 그룹에서의 코드 검증 기법에 대해 논의하였다. 2장에서는 센서 노드의 코드 검증 기법에 대해 설명하였고 3장에서는 멀티 홉 그룹 코드 검증 기법에 대해 설명하였다. 4장에서는 화이트리스트를 이용한 멀티 홉 코드 검증을 하는 방법에 대해 논의하며, 마지막으로 5장에서는 결론을 맺는다.

II. 센서 노드의 코드 검증 기법

이 논문에서는 공격자가 센서 노드를 공격하기 위해 센서 노드에서 빈 메모리 공간을 얻을 수 없는 코드 검증 기법[1]이 있다고 가정하였다. 또한 모든 센서 노드는 코드 검증에 필요한 코드를 포함한 동일한 실행 코드 영역을 가지고 있고, 모든 센서 노드들 사이에는 두 센서 노드만 알고 있는 공유키가 존재한다고 가정하였다. 마지막으로 모든 센서 노드는 BS(Base Station)의 공개키를 소유하고 있다.

각각의 노드는 [그림 1]의 과정을 통해 서로가 올바른 노드인지 확인할 수 있다. $id(A), id(B)$ 는 각 노드의 id 이고 S_A, S_B 는 각 노드의 공유키이다. 센서 노드들은 이 공유키를 서로 교환한다. R 은 센서 노드가 서로의 코드 검증 기법을 이용해서 만든 값으로 만약 공격자가 배치한 임의의 센서 노드라면 다른 센서 노드들과 같은 R 값을 만들어낼 수 없을 것이다. 최종적으로 센서 노드들은 $H(R, id(A)), MAC$ 과 $H(R, id(B)), MAC$ 을 교환하여 센서 노드간의 검증을 마치게 된다.

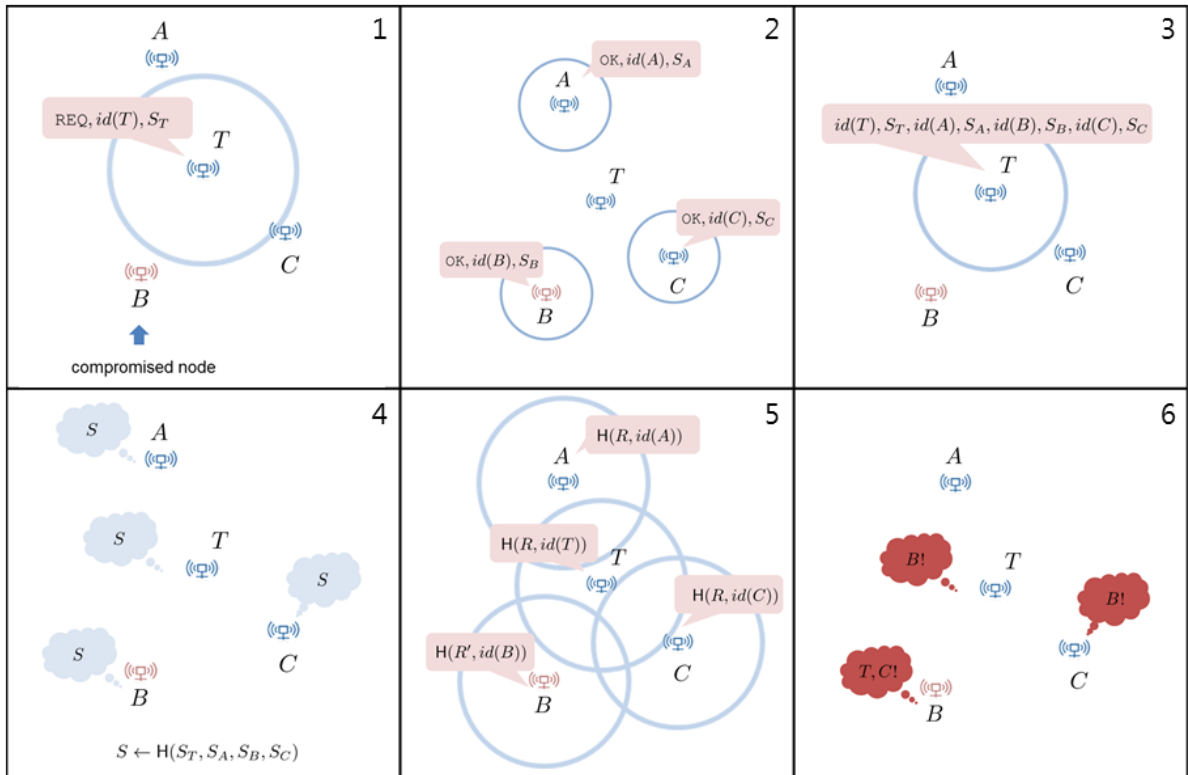


[그림 1] 요구-응답 방식의 코드검증 기법

III. 멀티 홉 그룹의 코드 검증 기법

멀티 홉 기반의 환경에서는 기존의 단일 홉에서의 일대일로 이뤄지는 코드 검증이 아니라 센서 노드간의 검증 기법에서 MAC을 사용하지 않고, 메시지 전달 형태가 유니캐스트가 아닌 브로드캐스트로 전달된다. [그림 2]와 같은 과정을 통해 그룹 코드 검증이 진행된다.

먼저 T는 BS역할을 하며 A, B, C 각 노드들에게 코드 검증을 요청하는 메시지를 보낸다. 여기서 B 노드는 악의적인 사용자에게 오염된 노드라고 가정한다. T로부터 메시지를 받은 노드들은 자신의 id와 공유키를 브로드캐스트 해 준다. 그러면 T는 브로드캐스트 된 메시지들을 기반으로 T를 포함한 각 센서 노드들의 id와 공유키를 브로드캐스트 해준다. 그러면 각 센서 노드들과 BS는 $S \leftarrow H(S_T, S_A, S_B, S_C)$ 를 계산해낼 수 있고, 이를 이용해 코드 검증을 한다. 그리고 계산한 R값과 자신의 id를 해시 함수에 넣어 만든 값을 브로드캐스트 한다. 이렇게 하면 정상적인 센서 노드인 A와 C는 올바른 R 값을 계산할 수 있으므로 T와 C는 B로부터 받은 $H(R', id(B))$ 를 통해 B가 오염된 노드라고 판단할 것이다. 오염된 센서 노드인 B는 자신이 계산한 값인 R' 으로는 주변의 노드인 T와 C를 정상적이지 않은 노드라고 판단할 것이다.

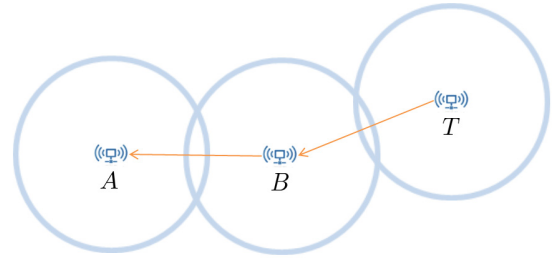


[그림 2] 그룹 코드 검증 과정

IV. 화이트 리스트를 이용한 멀티 홉 코드 검증

무선 센서 네트워크에서 그룹 코드 검증 방법 중 하나로 각 센서 노드들이 화이트리스트를 공유함으로써 센서 노드들 간의 검증을 할 수 있다. 여기서 사용되는 화이트리스트에는 센서 노드의 id값과 마지막으로 자신과 코드 검증을 한 시간, 홉 카운트 값을 사용한다. 이러한 화이트리스트는 마지막으로 이뤄진 코드 검증 시간과 홉 카운트를 기준으로 하여 기준보다 오랜 시간 동안 검증이 행해지지 않았다면, 또는 기준보다 많은 홉 카운트를 가진 노드라면 화이트리스트에서 삭제하는 방법으로 화이트리스트 자체가 지속적으로 커지는 것을 방지한다.

이러한 화이트리스트를 운영하는 방법으로는 블룸필터나 카운팅-블룸필터[2]를 사용할 수 있다. 블룸필터를 사용한다면 주변 노드의 수가 많은 경우에 기존의 화이트리스트를 사용할 때 보다 더 작은 크기의 화이트리스트를 유지할 수 있으며, 각각의 노드에서 화이트리스트에 있는 노드를 신뢰할 수 있는 남은 시간을 관리하기 때문에 노드들 사이에 기준 시간을 정해서 시간 동기화를 하지 않아도 된다. 이 논문에서는 카운팅-블룸필터를 화이트리스트 관리

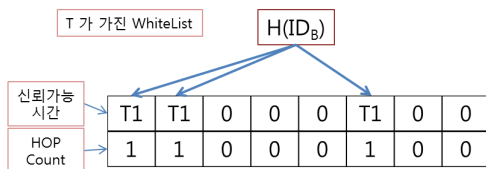


[그림 3] BS와 센서 노드들의 배치

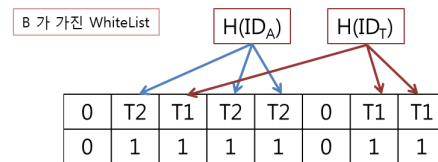
에 사용하였다.

[그림 3]에서 T는 BS의 역할을 하며, A, B노드는 서로 한 홉 간격으로 배치되어 있다. 이때 T가 가지는 화이트리스트는 [그림 4]와 같다. [그림 4]에서 T가 가진 화이트리스트에는 한 홉 거리에 있는 B 노드의 정보가 저장되어 있다. T1 값은 T와 B가 코드 검증을 마친 뒤 신뢰할 수 있는 시간을 뜻한다.

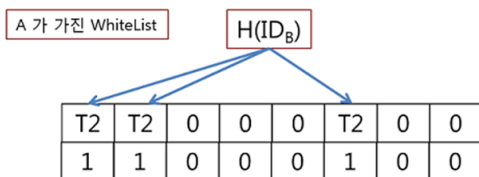
[그림 5]에서는 B의 화이트리스트에는 B와 한 홉 간격에 있는 T와 A의 정보를 볼 수 있다. [그림 6]에는 A가 가진 화이트리스트의 모습을 볼 수 있다. A의 화이트리스트에는 A와 한 홉 거리에 있는 B의 정보가 저장되어 있다. 여기서 B가 B의 화이트리스트 정보를 A에게 전달하여 B가 신뢰하고 있는 T에 대한 정보를 A에게도 전파할 수 있다. 화이트리스트가 카운팅-블룸필터로 구성되어 있기 때문에 A는 [그



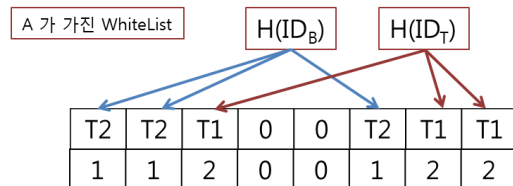
[그림 4] T가 가진 화이트리스트



[그림 5] B가 가진 화이트리스트



[그림 6] 업데이트 전의 A의 화이트리스트



[그림 7] 업데이트 된 후의 A의 화이트리스트

림 7과 같이 B로부터 T의 신뢰정보를 받아서 화이트리스트를 업데이트 할 수 있다.

V. 결론

본 논문에서는 무선 센서 네트워크에서의 화이트리스트를 이용한 그룹 코드 검증 기법에 대해 논의하였다. 화이트리스트를 카운팅-블룸 필터를 활용하여 운영함으로써 기존의 화이트리스트 운영보다 더 적은 크기의 화이트리스트를 활용할 수 있으므로 이는 센서 네트워크의 특성상 가질 수밖에 없는 문제점 중 하나인 저장량의 메모리에 대한 부담을 덜 수 있을 것으로 보인다. 다만 이러한 방법을 사용할 때 블룸 필터의 특성인 긍정오류에 대한 문제를 최소화 하도록 해시함수의 수와 화이트리스트의 크기에 대한 고찰이 충분히 이루어져야 할 것이

다. 이후의 연구에서는 네트워크 시뮬레이터 등을 이용하여 이러한 무선 센서 네트워크에서의 화이트리스트를 이용한 그룹 코드 검증 기법을 활용한 시나리오의 동작을 시뮬레이션 할 수 있을 것이다.

[참고문헌]

- [1] 최영근, 강전일, 양대현, 이경희, “무선 센서 네트워크에서의 메모리 공간 삭제를 이용한 선행 코드-검증 기법”, 한국정보보호학회논문지, 17(4), pp. 37-46, 2007년 8월.
- [2] Broder, A., & Mitzenmacher, M. “Network applications of bloom filters: A survey.”, Internet Mathematics, 1(4), 485-509. 2004.