무선 센서 네트워크의 내부 공격자에 대한 전송경로 상에서의 대응 기법*

정현호O 박석
서강대학교 데이터베이스 연구실
{neoaristoO, spark}@sogang.ac.kr

A countermeasure on routing paths against inner attackers in Wireless Sensor Networks

Jung, HyunhoO Park, Seog
Database Lab., Sogang Univ.

요 약

센서 네트워크를 구성하는 센서 디바이스 상에서 보안을 유지하는데 있어서 가장 까다로운 점은 센서 노드상에서 활용할 수 있는 대역폭, 에너지, 저장용량 등과 같은 리소스가 다른 컴퓨팅 장비보다 월등히 적다는 점이다. 따라서 공격자는 센서 네트워크의 위와 같은 약점을 활용하는 다양한 공격을 시스템에 가할 수 있는데 그 중 대표적인 방법이 시스템에 침투한 내부공격자에 의해서 변경된 가비지 데이터를 전송하게 함으로써 정상적인 노드들의 리소스를 낭비하게 하는 공격 방식이다. 따라서 본 논문에서는 기존의 연구됐던 보안 방식들이 내부공격자에 의한 전송계층상에서 취약한 점이 있음을 발견하고 접근 제어(access control)를 이용해서 이를 보완할 수 있는 방안을 제시한다. 이렇게 제시된 방안을 기존의 종단간 보안 프로토콜과 조합하면 아주 적은 양의 추가적인 오버헤드만으로 내부공격자에 대한 내구성을 더욱 강하게 할 수 있음을 실험을 통해 검증할 수 있다.

1. 서 론

센서 네트워크를 구성하는 센서 디바이스의 경우 안정적이거나 신속한 통신을 보장 받을 수 없는 환경을 갖게 되며 에너지나 저장용량과 같은 리소스 또한 일반적인 개인용 컴퓨터에 비해 매우 부족한 수준만을 보장 받는다. 위와 같은 시스템상의 배경을 바탕으로 센서 네트워크에 보안 메카니즘을 적용하기 위해 많은 연구들이 수행되었다. SPINS와 In-Network Security는 센서 네트워크 보안관련 연구 중 가장 대표적인 내용으로 둘의 공통점은 매우 적은 리소스만을 이용해서 보안 메커니즘을 운영할 수 있게끔 설계된 점이다.

하지만 두 가지 방식의 메커니즘 모두 내부 공격자가 존재하는 상황에서 전송 경로상에서 발생할 수 있는 공격에 대한 효과적인 방어 기법에 대해서 제시하고 있지 못하고 있다. 내부 공격자의 경우 매우 민감하고 중요한 키나 코드와 같은 정보를 가지고 있으므로 시스템을 공격하기 위해서 변경되거나 임의적으로 조작된 데이터를 합당한 절차에 걸쳐 전송하는 것이 가능하다. 이럴 경우 종단 노드에서 데이터의 변경이나 불법적인 투입여부를 판단할 수 있다 하더라도 중간 노드상에서 데이터를 전송하는데 필요한 에너지와 Bandwidth가 낭비되는 피해를 막지는 못과 내부 공격자에 의한 피해를 최소화할 수 있는 방안을 제시한다.

2. 관련연구

2.1. SPINS[3]

SPINS는 크게 양단(End-to-End) 통신상에서 데이터 confidentiality, authentication, integrity를 보장할 수 있는 SNEP과 데이터 브로드 캐스트에 대해서 authentication를 보장할 수 있는 μ TESLA 두 개의 세부 프로토콜로 구성된다.

먼저 살펴볼 SNEP 프로토콜에 가장 큰 특징은 전송되는 데이터의 주체인 전송자와 수신자간에 전송되는 데이터 블록 계수를 암호화와 인증 절차에 사용한다는 점이다. 따라서 추가적인 전송 오버헤드 없이도 데이터의 안전성을 배가시킬 수 있는 장점을 갖을 수 있다. μ TESLA는 한 노드에서 다수의 노드로 데이터를 전송하는 브로드캐스트 통신에 적용되는 보안 프로토콜로서 delayed 키 공개 방식을 사용함으로써 센서 디바이스와 같이 협소한 리소스만을 보장하는 시스템에 적합한 보안 방식이다.

* 본 연구는 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초기술연구 지원사업(B1220-0401-0358)의 연구 결과의 일부임.

한다[1,2].

따라서 본 논문에서는 위와 같은 기존 연구에서의 취약점을 해결하기 위하여 전송 경로상에서의 접근제어 기법 네트워크 시스템에 최적화된 보안 프로토콜을 제공한다. 이것은 기존의 μ TESLA 브로드캐스트 방식이 갖고 있었던 시간적인 제약조건을 개선하는데 대표자와의 홉 수에 따라 각기 다른 키를 이용해서 암호화하는 것을 운영상의 주요한 특징으로 갖고 있다.

3. 내부 공격자에 대한 전송 경로상에서의 대응 기법

3.1 기존 연구의 문제점 및 연구동기

센서 네트워크의 특성상 센서 노드는 매우 제약적인 에너지와 bandwidth만을 보장 받게 된다. 이런 상황에서 시스템을 파괴시키는데 목적을 갖고 있는 공격자의 경우 센서 노드의 에너지를 낭비하게 하고 bandwidth를 소모하게 하는 공격을 가함으로써 상당한 효과를 얻을 수 있게 된다. 더군다나 센서 네트워크는 개방형 구조를 갖으므로 공격자가 물리적으로 시스템에 접근하는 것을 막을 수 있는 방법이 없다. 따라서 공격자 자신이 조종할 수 있는 센서 노드를 시스템에 투입하거나 정상적인 센서 노드를 개조함으로써 키 값이나 실행 코드 등의 중요한 정보를 합당한 절차를 통해 얻어낼 수 있는 내부 공격자가 얼마든지 존재할 수 있는 상황이다. 하지만 기존에 제시된 방안들은 내부 공격자의 존재를 가정하지 않거나 내부 공격자가 수행하는 공격에 대한 대처 방안 혹은 내부 공격자를 보다 빠르게 식별할 수 있는 알고리즘을 제시하지 못하고 있다.

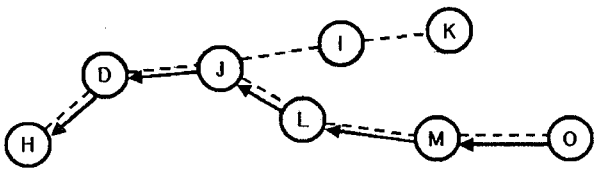

그림 1. 내부 공격자가 침투한 네트워크

그림 1.의 상황을 예로 들면, 노드 O에서 노드 D로 데이터 전송을 할 때 내부 공격자인 노드 L을 라우팅 경로상 지나치게 된다. 이때 내부공격자 L이 전송되는 데이터 컨텐츠 일부를 변경하거나, 데이터 헤더의 전송 목적 노드를 D에서 H로 변경한다 해도 기존의 보안 프로토콜은 데이터가 종단 노드에 도착해서야 데이터가 변경 되었음을 확인할 수 있으므로 데이터 전송에 참여했던 모든 중간 노드에서는 데이터를 전송하는데 필요한 에너지나 bandwidth를 낭비하게 되는 결과로 이어지게 된다. 기존 프로토콜이 이런 취약성을 갖게 되는 이유는 내부 공격자가 가진 권한을 이용해서 전달된 데이터를 변경하고 접근할 수 있는데 이를 전송 경로 중간에서 견제할 수 있는 방안을 제시하지 못하고 있기 때문이다.

2.2 In-Network [4]

In-Network 보안은 그룹 단위로 작업을 진행하는 센서

3.2 변경 제어 권한의 분배 기법

본 절에서는 내부 공격자가 존재하더라도 전송 경로상에서 발생할 수 있는 데이터 컨텐츠나 헤더의 변경으로 인한 피해를 최소화할 수 있는 방안에 대해서 제시하고자 한다. 제안하는 기법은 기초적으로 SPINS프로토콜을 바탕으로 설계가 되었으며 목적 노드에 도착해서야 변경 여부를 확인할 수 있는 기존 방안에 덧붙여 패킷 integrity를 확인할 수 있는 권한을 전송 경로 중간 여러 노드에 나눠줌으로써 공격을 받은 패킷을 발견하면 바로 드랍할 수 있는 방식을 주요하게 적용하고 있다.

키를 분배할 때 주요하게 고려할 사항은 각 노드가 제한적인 양의 패킷에 대해서만 변경 권한을 갖어야 하는 점과 전송 경로 곳곳에 배치되어 공격을 감시할 수 있어야 하는 점이다. 따라서 베이스 스테이션은 서로 통신하는 노드들의 수에 비하여 극히 적은 비율의 키 set을 구성하고, 이 set 중에 임의로 하나를 선택해서 각 노드에 분배하는 방식으로 패킷에 대한 변경 권한(Rkey)을 위임할 수 있게 된다.

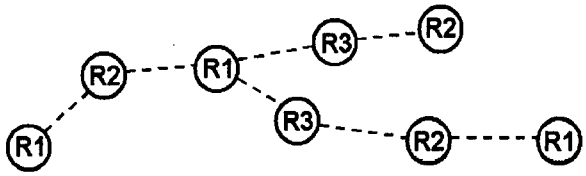

그림 2. 변경 제어 권한 분배 구조

위의 그림 2.와 같이 전송 경로 중에 여러 노드가 같은 종류의 변경 제어키를 갖게 되는 구조를 가지므로 수시로 데이터 변경 여부를 검출할 수 있게 된다. 아래 그림 3.은 실제로 메시지가 전송되는 포맷을 나타낸 그림이고 그림 4.는 위와 같이 setup된 변경 제어키를 이용해서 전송 경로 중간에 여러 노드에서 메시지의 변경 여부를 확인할 수 있는 알고리즘을 나타내고 있다.

header, data_cipher, MAC(Rkey,header|data_cipher)

그림 3. 전송 데이터 포맷

```
rcv header,data_cipher,MAC from qw

RkeyList(header) →
        mac_code=createMAC(Rkey, header|data_cipher)
        if mac_code ≠ MAC
        REPORT packet to BS
if DES(header) = p →
        decr. (Ekey, data_cipher)

NXT(header) = z →
        send header,data_cipher,MAC to z
rcv REPORT event in base station →
        suspectNodeList=analy.(packet)
        monitoring(suspectNodeList)
```

그림 4. 변경 데이터 검출 알고리즘

3.3 변경 제어 알고리즘의 검증

제안한 알고리즘의 성능을 검증하기 위해서 그림 1.과 같은 상황에서 내부 공격자의 대한 대처 과정을 살펴본다. 그림 5.는 알고리즘의 구동 과정을 단계별로 나타낸 모식도이다. Rkey2를 가진 소스 노드 O에서 데이터 전송을 할 경우 내부 공격자 L이 목적 노드를 H로 변경하는 공격을 하더라도 Rkey2에 대한 변경 제어 권한이 없으므로 공격자 이후 노드에서 변경을 검출할 수 있게 되어 단순히 종단 노드에서 변경 여부를 확인할 수 있는 보안 알고리즘에 비해 추가적인 리소스의 낭비를 막을 수 있음을 확인할 수 있다.

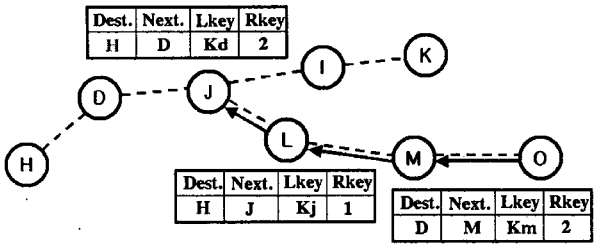

그림 5. 제안 알고리즘의 운영1

다음에 그림 6.의 상황은 앞서 살펴본 그림 5.와는 달리 전송 소스 노드와 내부 공격자가 같은 변경 제어 권한(Rkey)을 갖는 경우이다. 이 때 내부 공격자는 전송되는 데이터뿐만 아니라 Rkey를 이용해서 MAC코드 마저 변경할 수 있으므로 기존 알고리즘과 같은 수준의 피해를 입게 된다. 그렇지만 제안 기법에서는 전송 경로와 사용된 Rkey를 이용해서 내부 공격자의 범위를 축소할 수 있게 된다. 그림 6.에서는 소스 노드 O와 목적 노드 H사이에서 Rkey2를 사용하는 노드로 L과 O 노드만을 모니터링 함으로써 내부 공격자를 식별하는데 따르는 리소스와 시간을 절약할 수 있는 장점을 제공하게 된다.

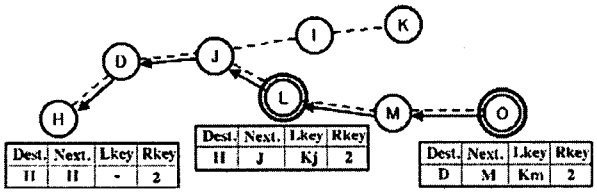

그림 6. 제안 알고리즘의 운영2

4. 평가 및 성능분석

성능 평가에 사용된 주요 매개 변수로는 시스템을 구성하는 노드 수와 공격자의 공격 유형이 있다. 먼저 노드 수는 30, 50, 100, 200, 300, 400, 500, 600개로 시스템을 변경해가며 평가하고 실험을 위해 구현된 내부 공격자의 공격 유형은 여러 연구 자료를 통해 제시된 방법 중 Misdirecting, flipping bit attack과 같이 전송 경로상에서 발생되는 공격에 국한해서 실험한다. 다음의 그림 7.은 TinySec[1]과 제안 기법을 TOSSIM에서 구동하여 내부 공격자가 식별되는 시뮬레이션 시간을 나타내는 그래프이다. 결과 그래프에서 볼 수 있듯이 30개의 노드로 실험을 시작하면서부터 제안기법이 TinySec보다 내부 공격자를 빠르게 식별할 수 있음을 확인할 수 있다. 이는 각 노드에 변경 제어 권한을 다르게 분배함으로써 모니터링 해야 할 대상을 TinySec에 비해 상당부분 줄임으로써 보다 빠르게 내부 공격자를 식별해 냄으로 분석할 수 있다.

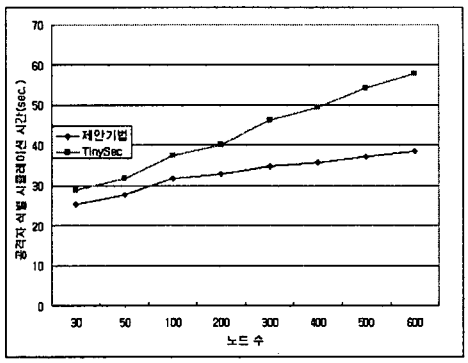

그림 7. 노드 수에 따른 공격자 식별 시간의 비교

5. 결론 및 추후연구

본 논문에서는 내부 공격자의 전송되는 데이터 변경으로 인한 리소스 낭비를 막기 위해 전송 경로에 있는 노드에 데이터 변경 제어 권한을 나눠줄 수 있는 키 전략을 제시했다. 제시된 방안은 전송 경로에서 헤더를 보호하고 변경이 확인된 패킷을 바로 버림으로써 리소스 낭비를 줄일수 있을 뿐 아니라 내부 공격자를 추적하는데 드는 시간 및 리소스 비용을 상당한 수준으로 줄일 수 있는 것을 실험을 통해 확인할 수 있었다.

하지만 본 논문에서 제안된 방식은 대부분의 처리를 베이스 스테이션에 의존하는 문제점을 내포하고 있다. 따라서 베이스 스테이션에 오버헤드가 커지는 단점이 존재하며, 시스템을 유지 관리하는데 있어서 확장적이지 못한 문제점이 존재한다. 그러므로 내부 공격자에 저항력 있는 보안을 유지할 수 있으면서 동시에 베이스 스테이션에 독립적일 수 있는 프로토콜에 대한 연구가 추가적으로 이루어져야 할 것이다.

참고문헌

1. Karlof, C., Sastry, N., Wagner, D., TinySec: A Link Layer Security Architecture for Wireless Sensor Networks., ACM SenSys' 04, Baltimore, Maryland, Nov. 3-5, 2004

2. A. Perrig, J. Stankovic, and D. Wagner, Security in Wireless Sensor Networks., CACM, Vol. 47, No. 6, Jun., 2004

3. Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen and David E. Culler, SPINS: Security Protocols for Sensor Networks, Wireless Networks 8: pp. 521-534, Sept., 2002

4. J. Deng, R. Han, S. Mishra, Security Support In-Network Processing in Wireless Sensor Networks Processing in Wireless Sensor Networks, In Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks,2003