지그비 홈 네트워크에서의 다중신원(Multiple Identities)노드 탐지 1)

이규호[1], 임재성[1], 김동규[1], 전상규[2], 양성현[2]

[1]아주대학교 정보통신전문대학원

[2]광운대학교 전자전기공학부

Multiple Identities Node Detection in Zigbee Home Network

Kyu-Ho Lee[1], Jae-Sung Lim[1], Dong-Kyoo Kim[1], Sang-Kyoo Jeon[2], Sung-Hyun Yang[2]

[1]Graduate School of Information and Communication Ajou University.

[2]Department of Electrical Engineering, Kwangwoon University.

요 약

홈서비스를 위한 지그비 센서 네트워크는 특정 대상이나 환경으로부터 데이터를 수집하여 그 데이터를 정보 분석이나 서비스 결정 수단으로 이용하기 때문에 데이터수집 과정에서의 효과적인 보안이 요구되어 진다. 지그비 센서 네트워크에의 공격은 정상적인 홈서비스를 방해하여 사용자의 불편을 초래할 수 있다. 이 중 다중신원을 가지는 공격자 노드의 침입은 비정상적인 정보 수집을 초래하여 서비스에서의 잘못된 결정을 유발할 수 있다. 이 다중신원노드의 탐지를 위해 본 논문에서는 DMIN(Detection of Multiple ID Node)이란 기법을 제안한다. 이 기법은 일처리 능력이 제한되어 있는 하나의 센서노드가 여러 신원의 역할을 수행할 때에 생기는 지연시간을 이용하며 이 기법을 이용하여 네트워크의 다중신원노드를 탐지한다.

I. 서론

무선 센서 네트워크는 특정지역이나 환경으로부터 데이터를 수집하기 위해 해당지역에 설치된 센서 노드들이 서로 무선으로 연결되어 통신하는 네트워크를 말한다. 그 중 지그비 프로토콜[1]은 IEEE 802.15.4를 기반으로 하는 무선 센서 네트워크 프로토콜로서 홈 네트워크와 같은 규모가 작은 네트워크에 적합하다.

센서 네트워크로부터 수집된 데이터는 중앙(base station)에 전송되어 사용자(서비스)에게 해당 지역의 정보를 제공해 준다. 이때 공격자에 의한 전송데이터의 위/변조는 중앙에서의 서비스 결정과 관련하여 잘못된 판단을 내리게 할 수 있는 등의 문제(예, 잘못된 온도정보로 인한 난방 중지)를 야기할 수 있다. 따라서 센서 네트워크 보안을 위한 통신의 암호화와 인증이 요구되어 진다. 이는 지그비 기반의 홈 센서 네트워크에서도 마찬가지이다. 지그비 프로토콜에 대한 연구가 계속되어옴에 따라 보안에 대한 강화가 이루어지고 있으나 프로토콜상의 취약점으로 인하여 이를 이용한 공격이 예상될 수 있다.

본 논문에서는 지그비 센서 네트워크를 이용한 홈서비스에 위해를 가할 수 있는 여러 공격들 중, 하나의 노드가 여러 개의 신원정보(identity)를 가지는 다중신원노드를 이용한 공격의 탐지 기법을 제안하고자 한다.

II. 다중신원노드에 의한 위협

다중신원노드는 실제 하나의 노드가 여러 신원정보(Identity)를 가지는 노드를 말하며, 그에 따라 해당 네트워크는 신원의 개수만큼 실제 센서노드가 있는 것으로 착각을 하게 된다. 이 다중신원노드를 이용하여 중앙(base station)에

1) 본 연구는 산업자원부 및 한국산업기술평가원의 성장동력기술개발사업의 연구결과로 수행되었습니다.

서의 정보 분석이나 서비스 결정 수단으로 이용되는 센싱 메시지를 여러 신원에서 보내는 것으로 위장하는 것이 가능해 진다.

지그비 홈 네트워크에서 이를 이용하여 정상적인 홈서비스를 제공하지 못하게 하고 댁내 사용자에게 불편을 주는 공격이 가능하다. 기존의 지그비 스펙에서 네트워크에의 신규노드 추가 시 별다른 인증을 거치지 않고 신원을 등록하게 하는 단순한 정책을 악용하여, 공격자는 센서노드를 네트워크에 추가하여 신원을 등록한다. 공격자는 물리주소를 스푸핑(spoofing)하고 같은 센서를 이용하여 또 다른 신원을 등록한다. 이와 같은 과정을 통해 공격자는 하나의 센서를 이용해 여러 개의 신원을 등록하여 다중신원노드를 네트워크에 참여시킬 수 있다. 이후 이 다중신원노드는 중앙에 실제 여러 노드에서 보내는 것처럼 메시지를 보낼 수 있게 되고 이로 인하여 중앙노드에서 수집된 정보의 신뢰성을 떨어뜨릴 수 있게 된다. 예를 들어 지그비 센서 네트워크가 홈 화재방지 서비스를 제공하고 있을 경우 공격자의 다중신원노드는 가짜의 고온 또는 연기정보를 여러 신원을 통해 중앙으로 보내게 되고 중앙에서는 그 메시지를 바탕으로 화재가 난 것으로 착각을 하고 스프링클러를 작동시키는 등의 잘못된 대응을 하게 될 것이다.

III. 기존 연구

이전에도 다중신원노드의 탐지에 대한 연구가 이루어져왔다[3, 4]. [3]은 다중신원노드의 탐지를 위한 메시지를 네트워크에 브로드캐스팅한다. 다중신원노드는 그에 대한 응답을 여러 번에 걸쳐서해야 하기 때문에, 일정 시간 안에 응답메시지를 모두 보내지 못하게 되고, 이러한 노드는 의심을 받게 된다. 이 기법은 중앙에서 전체 네트워크에를 모니터링 해야 하는 오버헤드와 별도의 계산처리과정 없이 바로 응답하는 것으로 인해 응답에 걸리는 대기시간이 짧아서 정상과 비정상의 구분이 모호해 질 수 있는 문제가 있다.

[4]는 이웃 노드 중 다중신원 노드가 있는지 탐지하기 위한 노드는 각 이웃에 다른 채널의 전파를 할당하고 그 중 랜덤하게 한 채널을 선택하여 메시지를 전송한다. 다중신원노드는 자신이 가진 신원마다 할당된 모든 채널을 통해 전파를 듣고 있을 수 없기 때문에 정상적으로 자신이 가지고 있는 신원들에 대한 모든 응답을 할 수 없게 된다. 이 기법은 각 이웃노드와 다른 전파 채널을 사용하는 것이 가능한 하드웨어가 필요하고, 어느 채널을 통해 전파를 듣고 있느냐에 따라 정상 이웃으로부터의 메시지 전송을 놓칠 수 있는 문제가 있을 수 있다.

본 논문에서 제안하는 기법은 키를 이용한 암,복호화 처리를 통해 응답대기시간을 늘려 정상과 비정상의 시간 차이가 크며, 새로운 노드의 진입 시에 부모노드에서 자신의 자식노드들에 대한 탐지 테스트만을 수행함으로써 네트워크 전체에 미치는 오버헤드가 작다.

IV. 제안하는 탐지 방법

다중신원노드는 여러 신원이 등록되어있지만 실제 센서는 하나이다. 따라서 그 다중신원노드의 일 처리 능력은 한정적이고 그에 따라 여러 신원으로서의 역할을 동시에 수행하는 것에 제한이 따른다. 제안하는 DMIN(Detection of Multiple ID Node) 기법은 이 같은 다중신원노드의 제한을 이용하여 네트워크에 존재하는 신원이 등록된 노드가 실제 하나의 센서인지 확인한다.

1. 가정

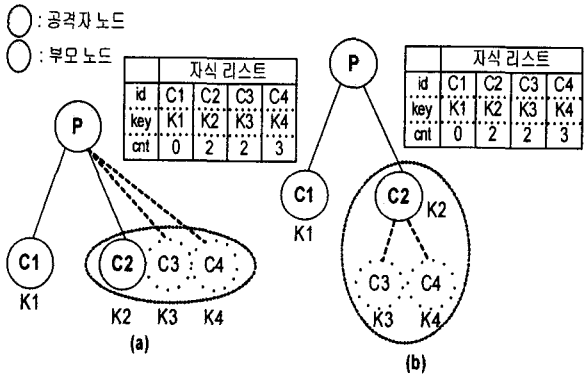
이 기법은 다음을 가정한다.

- 네트워크에 참여하는 새로운 노드 N_i는 기존의 지그비 프로토콜에서 쓰이는 키 이외에 다중신원노드 탐지를 위한 이웃노드 탐지용 키 K_i를 부모노드와 공유한다.
- 각 센서는 하나의 처리장치를 가지고 있어 동시에 여러 작업을 처리 할 수 없다.
- DMIN작업을 하는 동안에는 다른 작업을 하지 않는다.

2. DMIN(Detection of Multiple ID Node)

2.1 다중신원노드 모델

본 논문에서 고려한 지그비 센서 네트워크에서의 다중신원노드 모델은 [그림1]과 같다.

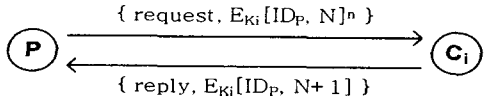


[그림 1] DMIN에서의 다중신원노드 모델

[그림1]의 (a)는 공격자가 P노드의 자식으로 C2, C3, C4 세 개의 신원을 등록한 것이고, (b)는 공격자가 C2하나의 신원을 P에 등록하고 C3, C4가 C2아래에 있는 것처럼 P에게 알리는 형태의 다중신원노드이다. (a), (b) 두 경우 모두에서, C2, C3, C4는 실제 하나의 센서이다. 부모노드 P는 자신의 2홉 이내의 자식노드 리스트를 가지고 있고 DMIN을 위한 키 K_i를 각 자식노드 C_i와 공유하고 있다.

2.2 DMIN을 이용한 다중신원노드 탐지

부모노드 P는 다중신원노드 탐지를 위해 TTL값이 2인 브로드캐스트 메시지를 보낸다. 이때 이 DMIN요청메시지는 메시지 타입과 자식노드와 공유하고 있는 키 리스트 중 하나를 랜덤하게 선택하여 n번 암호화 한 $E_{Ki}[ID_P, N]^n$을 포함한다. 여기서 ID_P는 P의 ID를 의미하며 N은 P에 의해 생성된 난수를 의미한다. 암호화를 n번함으로 해서 응답메시지 처리에 걸리는 시간을 늘려서, 정상과 비정상 응답과의 시간차이를 더욱 확연이 할 수 있다. 메시지를 받은 자식노드들은 P와 공유하고 있는 키 K_i을 이용하여 n번 복호화 한다. 그 결과를 이용해 자식노드는 N+1 값과 P의 ID를 K_i로 암호화하여 노드P에게 응답메시지를 보낸다.



[그림 2] DMIN에서의 메시지 교환

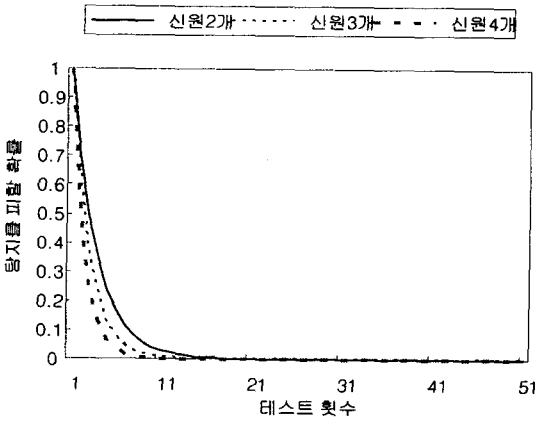
부모노드 P는 키 K_i에 해당하는 자식노드 C_i로부터의 응답메시지만을 기다린다. 만약 C_i로부터 일정시간(t_w) 안에 응답메시지가 오지 않으면 P노드는 비정상으로 판단하고 해당 C_i노드의 카운트(count)를 증가 시킨다. 응답메시지 안에 정상적인(N+1)값이 들어 있지 않아도 마찬가지이다.

자식노드 C_i가 신원이 하나여서 부모노드 P와 공유하는 키를 하나만 가지고 있는 정상노드라면, 자신의 키로 암호화된 DMIN요청메시지를 n번 복호화 하여 응답메시지를 보낼 수 있다. 하지만 다중신원노드와 같이 여러 개의 신원을 가지고 있다면 DMIN요청메시지가 어느 키로 암호화된 것인지 알 수 없고 P노드가 어느 노드에 대한 응답을 기다리는지 알 수 없기 때문에, P노드에 응답하기 위해서는 가지고 있는 키들로 정상적으로 복호화 될 때까지 여러 번 확인을 해야 한다. 따라서 C_i는 t_w안에 정상적인 응답메시지를 P에게 보낼 수가 없고, 결국 P는 해당자식노드를 비정상으로 판단하고 카운트를 증가시킨다. 여러 번의 DMIN요청메시지를 보낸 후 부모노드 P의 자식리스트 중 카운트 값이 임계값을 넘으면 해당 자식의 신원은 다중신원노드로 판단하고 네트워크에서 제외시킨다. 그 후 네트워크 관리자는 해당 센서를 확인하여 제거할 수 있다.

V. 분석

부모노드 P에서 응답메시지를 기다리는 일정시간 T 는 {(n + 1)*e + α}이다.(n: 암호화횟수, e: 암호화시간, α: 전파시간(propagation delay)) 다중신원노드일 경우 응답메시지가 P에 도착되는 시간은 {(k*n + 1)*e + α}이고(k: 키 적용횟수) 따라서 정상노드와 비정상 노드의 응답시간의 차이는 [(k-1)*n*e]이 된다. 이때 정상적으로 시간T안에 응답메시지를 보낼 확률은 (1/신원의 수)이다. 그러나 DMIN에서 메시지를 한 번

만 보내는 것이 아니므로 다중신원노드가 가진 신원에 대한 요청 메시지마다 정상적인 시간 안에 응답을 할 확률은 (1/키의 수)^r 로 더욱 작아진다. 여기서 r은 부모노드에서 요청한 탐지 테스트 횟수이다.



[그림 3] 다중신원노드가 탐지되지 않을 확률

부모노드 P의 자식노드 수가 k개이고 그 중 다중신원노드에 포함된 자식의 수는 m개라고 하자. 이 때 하나의 DMIN요청메시지로 다중신원노드가 탐지될(카운트가 증가할) 확률은 (m/k) * {(m-1)/s} = (m-1)/k 이다. 따라서 탐지되지 않을 확률은 [(k-m-1)/k]이다. 부모노드가 메시지를 여러 번 보내어 r번 테스트를 한다면, [(k-m-1)/k]^r 으로 탐지되지 않을 확률이 점점 낮아지게 된다. [그림3]은 k=10이고 다중신원노드의 신원이 2개, 3개, 4개일 때의 테스트횟수에 따른 다중신원노드가 탐지되지 않을 확률이다. [그림3]에서 보는 바와 같이 테스트를 20회 하기 이전에 거의 0의 확률로 낮아지고, 10회 이전에 신원2개, 3개, 4개의 각 다중신원노드가 탐지되지 않을 확률은 0.03, 0.006, 0.001로 아주 낮아진다.

DMIN에서는 요청메시지를 한번만 암호화 하는 것이 아니라 n번 할 수 있게 하였다. n이 커질수록 정상 응답과 비정상 응답과의 시간차이가 더욱 확연히 난다. 이는 탐지의 정확성에 영향을 미칠 것 이다. 하지만 n이 커질수록 암호화로 인한 시간과 리소스의 소모가 생긴다.

또한 메시지 전송 시 네트워크 정체(congestion)나 패킷손실로 인한 오탐(false positive)이 발생 할 수도 있다. 이는 카운트 임계값을 높이면 줄일 수 있겠으나, DMIN탐지를 위한 테스트횟수가 증가하여 오버헤드가 많아질 수 있다. 응답노드에서 응답메시지에의 타임스탬프추가를 통해 줄일 수 있겠으나 이는 노드들의 시간 동기화를 필요로 한다.

VI. 결론

지그비 센서 네트워크를 이용한 홈서비스 제공에 있어 데이터의 신뢰성 보장은 매우 중요한 사안이다. 공격자가 지그비 스펙의 취약점을 이용하여 등록한 다중신원노드는 수집된 데이터의 신뢰성을 떨어뜨리는 위/변조된 데이터를 전송하게 되고 그에 따라 홈서비스는 오작동을 하게 된다. 본 논문에서 제안한 DMIN은 이러한 공격을 막기 위해 네트워크에 새로 참여하는 노드들에 대한 테스트를 실시하고 그에 따라 다중신원노드를 탐지할 수 있게 한다.

공격노드의 정확한 탐지를 위해 실시하는 여러 번에 걸친 테스트로 인한 오버헤드를 줄이고, 동시에 오탐률(false positive)을 줄일 수 있는 방안은 향후 연구 과제이다.

[참고문헌]

[1] Zigbee alliance. http://www.zigbee.org.

[2] Naveen Sastry, David Wagner, "Security considerations for IEEE 802.14.4 networks", Proceedings of the 2004 ACM workshop on Wireless security, 2004

[3] J. R. Douceur, "The Sybil attack", In First International workshop on peer-to-peer Systems(*IPTPS'02*), 2002

[4] J .Newsome, E. Shi, "The Sybil Attack in Sensor Networks: Analysis & Defenses", Proceedings of the third international symposium on Information processing in sensor networks(*IPSN'04*), 2004

[5] I. Khalil, S. Bagchi, "DICAS: Detection, Diagnosis and Isolation of Control Attack in Sensor", Proceeding of the First International conference on Security and Privacy for Emerging Areas in communication Networks(*SECURECOMM'05*), 2005