정보산업동향

무선 센서 네트워크의 최신 보안 기술 연구 동향

목 차

김미희 · 김지선 · 김아름 · 채기준
(노스캐롤라이나주립대학 · 이화여자대학교)

1. 서 론

언제 어디서나 네트워크와 시스템을 자유롭게 사용할 수 있는 환경인 유비쿼터스 시대가 도래하면서 이와 관련된 IT 기술 및 네트워크 활용 분야에 대한 연구가 활발히 진행되고 있고 그 규모와 범위는 더욱 커지게 될 것으로 예상된다. 그중 센서 네트워크는 유비쿼터스 환경 구축의 기반이 되는 기술로서 없어서는 안 될 필수적인 분야 중 하나로 이에 대한 관심이 증가되고 있고 그 연구의 중요성이 강조되고 있다.

센서 네트워크는 유무선 네트워크 인프라에 작은 크기의 다양한 센서노드를 설치하고 이를 통해서 주변 환경에 대한 다양한 정보를 수집하여 이를 분석하는 역할을 수행한다. 현재 군사, 의료, 차량, 위치 인식 등 다양한 응용분야에서 활용되고 있으며 이에 대한 연구도 활발히 진행중에 있다. 이와 같은 센서 네트워크 기술 연구에 있어서 기반 기술 연구와 함께 센서를 통해 수집된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크상에서의 보안 메커니즘이 연구되어 적용되어야 한다. 특히, 국방, 위험지역 상태 모니터링, 헬스 케어 응용에서는 보안의 중요성이 더욱 커진다.

무선 센서 네트워크에서 다양한 보안 기술 및 효율적인 침입 탐지 대응 기법을 설계하고 센서 네트워크에 적용하기 위해서는 다음과 같은 사항들을 고려해야 한다. 센서 네트워크의 경우 각 센서노드가 가지는 기억공간 및 계산능력의 제약으로 인해 기존 유무선 네트워크에서의 보안 기술과 침입 탐지 시스템을 그대로 적용하는 것은 불가능하다. 그렇기 때문에 무선 센서 네트워크에 적합한 보안 기술 및 침입 탐지 대응 기술들이 필요하며 특히 다수의 센서노드를 배치하기 위해서 범위성(scalability) 제공 및 가격 또한 최소화해야 하므로 경량화된 보안 기법들이 제공되어야 한다.

본 논문에서는 센서 네트워크의 자원 제약성과 비정형적인 특성을 포함한 특성 및 보안 취약성을 기술하며 이에 따른 다양한 보안 이슈들을 조사한다. 이러한 분류에 대해 최근 3,4년 동안 진행되어 온 보안 기술 연구 동향을 비교 분석한다. 이를 통해 센서 네트워크에서의 보안 메커니즘에 대한 향후 연구 방향을 제시함으로써 효율

성 및 안정성을 제공할 수 있는 메커니즘에 관한 연구를 촉진하고 센서 네트워크의 활용도를 제고하자 한다.

본 연구의 구성은 다음과 같다. 1장의 서론에 이어서 2장에서는 센서 네트워크의 보안 취약성 및 보안상의 기본적인 요구사항을 조사 기술한다. 3장에서는 보안 이슈를 안전한 애그리게이션, 로컬라이제이션, 라우팅, 리프로그래밍과 침입 탐지/대응 기술 및 침입 탐지 구조로 분류하여 각각의 기술을 분석한다. 4장에서는 향후 연구 방향 및 제언을 기술하고 마지막으로 5장에서 결론을 맺고자 한다.

2. 센서 네트워크 보안 취약성 및 요구사항

무선 센서 네트워크는 전송 방식의 특성상 일반적인 유선 네트워크에 비하여 더 많은 보안 취약점을 내포하고 있다. 유선 네트워크의 경우 물리적으로 연결이 되어 있어야 네트워크에 참여가 가능하지만, 무선 센서 네트워크는 전파를 통하여 모두에게 전달할 수 있으므로 네트워크에 접속이 수월하며 전송 데이터가 모두에게 오픈되어 있다. 그렇기 때문에 무선 센서 네트워크의 안전한 통신을 위해서는 기본적으로 데이터를 암호화하거나 인증을 적용해야 하는데 기존 유선 네트워크에서 쓰이는 암호화나 인증 방식을 그대로 적용하기엔 센서 에너지나 메모리 공간이 충분하지 않기 때문에 적절하지 않으며 그 비용이 많이 들게 된다.

또한 센서 네트워크의 원활한 운용을 위해 제안되고 있는 다양한 메커니즘들, 예를 들어 라우팅, 로컬라이제이션, 애그리게이션, 리프로그래밍 등이 초기에 효율성만을 고려해 제안되었는데, 이러한 경우 제안된 메커니즘 자체의 보안 취약점을 내포할 수 있어서 이를 악용한 공격들이 가능하다. 예를 들어, 동적인 라우팅을 수행해야만 하는 센서 네트워크의 특성상 라우팅 변조를 통한 공격에 의해 전 네트워크의 정상적인 센싱 데이터의 전송을 와해시킬 수 있다. 또한 운영 중인 센서노드의 코드를 변경하는 리프로그래밍 응용에서 공격자가 원하는 코드로의 코드 분배가 가능할 수도 있다. 그외 무선 센서 네트워크에서 가해질 수 있는 다양한 공격이 존재한다. 웜홀 및 싱크홀 공격은 루트를 조작하여 전송되는 센싱 데이터의 스니핑, 변조, 드롭과 같은 공격을 자유롭게 수행할 수 있으며, 서비스 거부 (Denial of Service) 공격은 네트워크에서 센서간의 통신이나 서비스의 원활한 제공을 막을 수도 있고 센서에서 가장 중요한 자원인 에너지의 빠른 고갈을 유도하여 네트워크 수명을 단축시킬 수 있다.

앞서 설명한 다양한 보안 취약점을 보완하기 위해 센서 네트워크에서의 메커니즘 고안 시, 요구되는 보안 요구사항들은 다음과 같다. 센서 네트워크는 이웃으로부터 읽어온 정보를 누설해서는 안 되며, 전달되는 정보의 안전을 위해 무선 센서 네트워크 안에 안전한 채널을 만들어 기밀성(Confidentiality)을 제공해야 한다. 악의가 있는 노드들은 패킷 안에 데이터를 조작하거나 다른 내용을 추가시켜 패킷을 손상시킬 수 있으므로 무결성(Integrity)을 제공해야 하며, 데이터의 최신성을 유지하고 공격자가 재생 공격을 할 수 없도록 신선성(Freshness)을 제공해야 한다. 에너지 제한적인 노드 특성상 다양한 가용성 측면의 취약성을 내포하고 있으므로 가용성(Availability) 제공이 중요하다. 분할된 센서 네트워크는 멀티 홉 라우팅, 키 관리, 센서 사이에 믿을만한 연결을 위해 자가 조직화(Self organization), 자가 치유가 가능해야 한다. 대부분의 센서 네트워크 장치들은 시간 동기화의 여러 형태에 의존하므로 시간 동기화(Time synchronization) 기능을 제공해야 하고, 공격자가 데이터 패킷을 주입할 수 있으므로 수신자는 올바른 송신자로부터 온 데이터인지 보장할 수 있도록 인증 (Authentication) 기능이 제공되어야 한다.

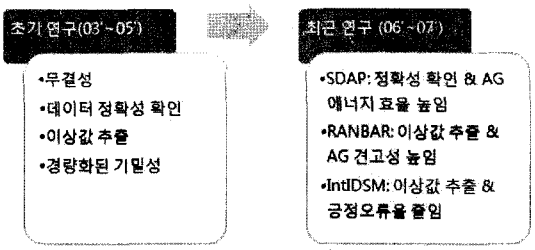
3. 센서 네트워크의 보안 기술

센서 네트워크의 원활한 운용을 위해 제공되는 다양한 메커니즘에 대해 안전성 제공은 필수적이며, 이에 대한 연구인 1) 안전한 애그리게이션, 2) 안전한 로컬라이제이션, 3) 안전한 라우팅, 4) 안전한 리프로그래밍 기술이 연구되고 있고, 센서 네트워크의 취약점을 악용하는 5) 다양한 공격에 대한 대응 및 이에 대한 침입 탐지 구조에 대한 연구가 활발히 진행되고 있다. 본 장에서는 최근 진행되고 있는 센서 네트워크의 보안 기술 동향을 비교 기술하여 분석하고자 한다.

3.1 안전한 애그리게이션 기술

애그리게이션 또는 퓨전 기술은 센서 네트워크에서 에너지 효율적인 정보 전달을 위해 전달 정보를 모아 보내는 가장 기본적인 메커니즘으로서 센서 네트워크 연구 초기부터 많은 연구가 진행되었다. (그림 1)과 같이 안전한 애그리게이션 및 전달된 정보의 정확성을 위해 초창기 진행되었던 연구로는 애그리게이션 되는 정보의 무결성 제공 방법[1], 위협 받은 퓨전노드의 값 이상(abnormal)을 체크할 수 있도록 증인노드를 만들고 이를 통해 보팅(voting) 혹은 MAC (Message Authentication Code) 확인 과정을 수행하는 증인기반 데이터 정확성 확인 기법[2], 공격자에 의해 이상 정보 추가에 따른 애그리게이션값 오류 유도 공격에 대한 이상값 추출 방법[3] 등이 제안되었다. 또한 안전한 정보 전달을 위해 암호화 기술을 적용하면 애그리게이션 수행 시 수신된 메시지의 복호화를 수행해야 하므로 에너지 소비가 많아지는데, 이에 대해 특별히 복호화 방법을 알지 못하더라도 두 개의 암호문을 통해 그에 상응하는 두 개의 평문을 가져올 수 있는 준동형 암호 방법을 적용한 경량화된 기밀성 제공 기법[4]이 제안되었다.

이러한 기본적인 안전한 애그리게이션 연구에 기반하여 최근 진행되고 있는 관련 연구로는 효율성을 고려하여 애그리게이션을 수행하며 전달 정보 오류를 유발하는 공격에 안전한 SDAP 방법[5], 향상된 이상값 추출 방법 RANBAR[6], 시스템 모니터링과 침입탐지 기능을 결합한 데이터 정확성 확인 기법[7]이 제안되었다.



(그림 1) 안전한 애그리게이션 기술 동향

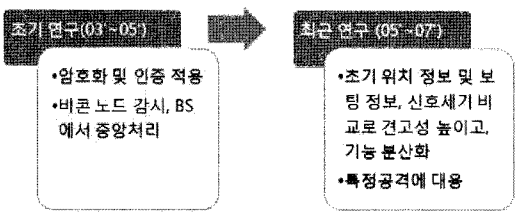
3.2 안전한 로컬라이제이션 기술

로컬라이제이션은 센서노드의 위치를 결정하는 기술로서 크게 직접방식과 간접방식으로 나누고 있다. 직접방식은 절대적인 위치를 사용하는 것으로 수동으로 위치를 구성해 주는 것과 GPS를 가지고 위치를 정하는 방식이 있다. 간접방식은 근처 노드의 상대적인 위치를 사용하는 것으로 레인지기반(Range-based) 방식과 레인지프리(Range-free) 방식이 있다. 레인지기반 방식은 노드 사이의 거리를 계산하기 위해 절대적인 길이나 각도 등을 사용한다. 예를 들어 ToA(Time of Arrival), TDoA(Time Difference of Arrival), AoA (Angle of Arrival), RSSI (Received Signal Strength Indicator) 등의 값을 사용하여 거리를 측량한다. 레인지프리 방식은 절대적인 거리나 각도 등의 정보 없이 위치를 측량하는 방법이다.

로컬라이제이션 분야에서 중요한 연구 요소는 에너지 효율성, 정확성, 보안이다. 이 중 에너지 효율성과 정확성에 관련한 연구는 많이 진행되어 왔지만, 보안에 대한 연구는 최근에 주목 받고 있다. 로컬라이제이션 기술 중 직접방식에서

는 센서에 직접 GPS를 부착해야 하기 때문에 비용이 많이 들어 센서 네트워크에 적용하는데 문제가 있다. 따라서 센서 네트워크에서의 로컬라이제이션 기술은 간접방식에 대한 분야가 주로 연구되고 있고, 그 중에서 레인지기반 추정은 별도의 하드웨어와 조정처리(coordination)가 요구되어 많은 비용이 요구되므로 레인지프리 기반 위치 추정 방식[9]이 최근에 더 많이 선호되어 연구되고 있다.

(그림 2)에 보이는 것처럼 초기 안전한 로컬라이제이션 연구는 단순한 암호 및 인증 적용이나 감시에 의한 중앙처리 등으로 간단히 안전성을 제공하였다. 이에 최근 연구에서는 초기 위치 정보를 기반하거나 보팅 정보, 신호세기 비교 등으로 위치정보의 진위를 각 센서노드가 검사하여 위치정보의 정확성 및 안전성을 높였고[8], 로컬라이제이션에서 가장 큰 위협이 될 수 있는 웜홀 공격을 탐지하기 위한 연구[9]가 진행되었다.



(그림 2) 안전한 로컬라이제이션 기술 동향

3.3 안전한 라우팅 기술

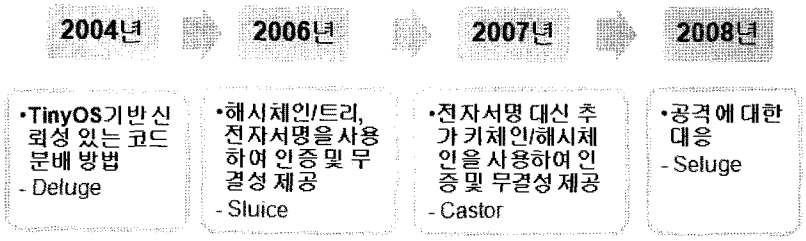
라우팅에 대한 공격은 정보전달의 흐름을 변경하거나 정보 자체가 전달되지 못하도록 만들 수 있기 때문에 공격자에게 이용되기 쉽고, 그래서 안전한 라우팅 기술에 대한 연구는 다른 보안 메커니즘에 비해 활발히 진행되어 왔다.

최근에도 안전한 라우팅 기술이 연구되고 있고, 대부분의 안전한 라우팅 기술이 에너지 효율성을 고려하면서 제안되고 있음을 알 수 있다. SEEM[10]은 안전한 라우팅을 위해 단지 신뢰된 베이스 스테이션이 패스를 선택해 주기 때문에 라우팅 공격을 막을 수 있으나, 많은 노드 수의 네트워크에 적용하기엔 비효율적이다. Curve-Based Secure Routing[11]과 SEEM에서는 확실한 정보 전달을 위해 멀티패스를 적용하였다. Secure Energy-Efficient FBSR[12]은 OHC를 이용하여 안전한 라우팅을 제공하는데 전자는 센싱 정보의 인증을 위하여, 후자는 사용하는 키에 OHC를 적용하여 피드백 메시지의 무결성과 노드인증을 제공하였다. ESecRout[13]에서는 센서노드와 베이스 스테이션 사이에 가지고 있는 공유된 비밀키를 이용하였으나 센서노드 수가 많아지면 비효율적이 될 수 있고, 전자에서는 부가적으로 키 신선성을 제공하기 위해 키갱신 메커니즘을 포함하고 있다. 또한 [12-13]에서는 정보를 암호화하여 기밀성을 제공하였다.

3.4 안전한 리프로그래밍 기술

센서 네트워크는 많은 노드 수로 구성되어 있고 많은 응용에서 외부 환경에 무작위 배포로 배치되어 사용되므로 센서노드에서 실행되는 코드의 기능에 대한 업그레이드나 버그 수정을 위한 코드분배 방법이 원격으로 수행되어야 하며 무선 환경으로 실행코드를 배포해야 하므로 안전성이 특히 중요한 분야라고 할 수 있다.

지금까지 제안된 대부분의 안전한 코드분배 메커니즘[15-17]은 멀티홉으로 구성된 TinyOS 기반 센서노드들에 새로운 코드분배를 수행하는 모듈인 Deluge[14]를 기본으로 하고 있다. Deluge는 전송하고자 하는 전체 코드 이미지를 일정한 크기의 페이지로 나누고, 각각의 페이지는 n개의 패킷으로 나누어 전송한다. 페이지 레벨에서는 순서대로 한 페이지씩 전송 완료한 후 다음 페이지 전송을 수행하고, 패킷 레벨에서 노드는 자신의 이웃 노드들에게 페이지 내의 모든



(그림 3) 안전한 코드분배 메커니즘의 연구 동향

패킷들을 브로드캐스트한다. 이웃 노드들로부터 SNACK (Selective Negative ACK) 메시지를 받은 후 받지 못한 패킷의 셋에 대해서 다시 브로드캐스트하여 전송에 누락된 패킷이 없도록 신뢰성 있는 데이터 전송을 보장한다.

(그림 3)과 같이 지금까지 제안된 안전한 리프로그래밍을 위한 초기의 메커니즘[15]은 인증 및 무결성을 제공하기 위해 해시트리/해시체인 및 전자서명을 사용하였고, 이후 전자서명의 계산 오버헤드를 줄이기 위해 추가 해시트리나 키체인을 사용하는 방안[16]이 제안되었다. 최근에는 공격에 대한 대응 메커니즘[17]으로 향상되었다.

3.5 침입 탐지/대응 기술 및 침입 탐지 구조

3.5.1 침입 탐지/대응 기술

센서 네트워크상에서의 다양한 위협들 중 주요 공격으로 서비스거부 공격이 존재한다. 서비스거부 공격은 센서의 배터리 한계점을 악용하여 쉽게 무선 센서 네트워크의 안전성을 무너뜨릴 수 있고, 각 계층별로 가능하다[18]. 물리 계층에서 공격자는 채널에 잼(jam) 신호를 전송함으로써 노드의 합법적인 트래픽을 방해할 수 있다. 재밍 공격을 "탐지"하는 방법, 공간적인 후퇴를 통하여 재밍된 지역으로부터 노드들이 철수할 수 있게 하는 "회피" 방법, 보다 더 강력한 에러 검출 코드를 통해 에러를 검출하고 정상 패킷을 선별하여 성공적인 패킷의 가능성을 증가시키는 "경쟁"의 방법으로 연구되어 왔다.

에너지가 중요 요소 중에 하나인 센서 네트워크에서는 링크/MAC 계층에서의 서비스거부 공격에 많은 취약점을 내포하고 있다. 슬립거부 공격은 MAC 계층에서 공격자가 노드가 Sleep 상태로 변환되는 것을 방해하여 노드의 에너지 소비를 가속화 시키는 방법으로 서비스 거부의 특화된 공격이다. 센서 네트워크에서 제안된 주요 MAC 프로토콜들, 예를 들어 S-MAC, T-MAC 등도 슬립거부 공격의 취약점이 내포되어 있다. 링크 계층의 강화된 인증은 슬립거부 공격을 예방할 수 있는 대응 방안이다. 패킷에 순차적으로 시퀀스 번호를 부여하여 anti-replay를 실현하는 것 또한 다른 대응 방안이다. 그 외에도 대칭 키, 참견이 되는 채널의 저항력과 탄성력을 강화시킴으로써 공격에 대응할 수 있다.

네트워크 계층에서는 스푸핑, 재생 공격 등이 발생할 수 있고 이에 따른 대응 방안으로는 인증과 anti-replay 등이 있다. 헬로우 플러딩 공격은 재생된 헬로우 패킷을 끊임없이 노드에 전송하여 원래 노드와 직접통신을 불가능 하게 만들거나, 멀리 있는 공격자가 강한 강도의 신호로 헬로우 패킷을 전송하여 가까운 곳에 위치하지 않은 공격자에게 패킷을 전송하게 되는 공격이다. 이외 특별한 책임을 갖는 노드(예: 클러스터 헤드)를 타겟으로 정하고 식별하기 위해 트래픽 패턴을 분석하는 homing 공격, 특정 루트에 악의적인 노드를 포함시켜 그 곳을 지나가는 모든 패킷을 드랍시키는 블랙홀 공격이 있다. 헬로우 플러딩 공격의 경우 쌍방향 인증과 지역적 정보

를 고려한 라우팅을 통해 그 피해를 경감시킬 수 있고 homing 공격은 헤더 인증 및 더미 패킷을 활용하여 공격자의 트래픽 분석을 무력화하고 피해를 경감시킬 수 있다. 블랙홀 공격의 경우는 다양한 경로의 라우팅을 통해 공격당한 경로 외에도 패킷들이 이용할 수 있는 경로를 제공하여 공격에 대응할 수 있다.

전송 계층에서는 TCP SYN(synchronize) 플러딩 공격과 위조된 시퀀스 번호와 컨트롤 플래그를 통해 비동기화 공격을 발생할 수 있다. TCP SYN(synchronize) 플러딩 공격에 대한 대응책으로는 클라이언트의 TCP SYN 메시지로부터 정보를 인코딩하고 SYN쿠키를 활용할 수 있다. 비동기화 공격의 경우는 헤더와 패킷 전체를 인증함으로써 서비스거부 공격을 예방할 수 있다.

응용 계층에서 overwhelming 공격은 베이스 스테이션에 대량의 트래픽을 전송하여 네트워크를 전복시키는 방법이다. 이 공격을 통해 네트워크의 대역폭이 소비되고 노드 에너지를 감소시킨다. 데이터 애그리게이션 등을 통하여 공격을 경감 시킬 수 있다.

3.5.2 침입 탐지 구조

유선 네트워크에서의 IDS 구조는 크게 운영체제의 감사흔적, 시스템과 어플리케이션 로그, 시스템콜을 모니터링하는 모듈에 의해 생성된 감사 데이터를 가지고 침입탐지를 하는 호스트기반 IDS와 네트워크 트래픽을 가지고 침입탐지를 수행하는 네트워크기반 IDS로 분류한다. 무선 애드혹 네트워크와 센서 네트워크 특성에 맞추어 연구되고 있는 IDS 구조를 세 가지로 분류할 수 있다. 첫째 Stand-alone IDS 구조[18]에서는 각 노드가 독립적으로 IDS를 운영하고 자신을 위한 공격 탐지 기능을 수행한다. 또한 각 IDS는 어떠한 정보도 공유하지 않고, 다른 시스템과 협력하지도 않는다. 그러므로 이 구조에서는 모든 노드가 IDS를 운영할 능력을 가져야 한다. 둘째 Hierarchical IDS 구조[19]의 경우, 클러스터헤드를 가진 여러 개의 클러스터로 나누어진 계층적인 센서 네트워크를 가정한다. 이러한 네트워크 구조에 맞춰 클러스터 안에서 각 노드는 어떠한 악의적인 행동 탐지를 위한 간단한 감시 역할을 수행하고 이를 클러스터헤드가 취합하여 통합하며, 상위에 있는 싱크노드에 전달하는 계층적인 구조를 나타낸다. 셋째 Distributed & Cooperative IDS 구조[20]에서는 모든 노드 혹은 일부 노드가 자신만의 IDS 기능을 수행하고, 전역의 침입탐지 메커니즘을 수행하기 위해 IDS끼리 서로 협력한다.

4. 향후 연구 방향 및 제언

지금까지 최근 센서 네트워크의 안전한 운용을 위해 연구되었던 메커니즘에 대해 안전한 애그리게이션, 로컬라이제이션, 라우팅, 리프로그래밍, 그리고 침입 탐지/대응 기술 및 탐지 구조로 나누어 비교 설명하였다. 지금까지 분석한 메커니즘들의 특징 및 장단점 비교를 통해 향후 다음과 같은 연구가 진행되어야 할 것이다.

첫째, 많은 노드 수 고려(Scalability)에 의한 안전성 제공 기술이 연구되어야 한다. 환경 감시, 도로 감시 등의 응용에는 센서 네트워크의 크기가 상당히 클 것으로 예상된다. 그러나 기존 메커니즘에서 베이스 스테이션에 의존하거나 노드 수가 많아지는 경우 효율성이 떨어지는 경우가 있다[13]. 이에 대한 고려가 필요하다.

둘째, 네트워크의 노드 밀도에 따라 다른 안전성 제공 기술 연구가 필요하다. 노드 밀도가 높은 경우에는 이웃 노드에 대한 감시에 의해 거짓 정보 및 공격자에 대한 탐지가 상당부분 해결될 수 있지만, 밀도가 낮은 경우에는 감시 대상의 수가 제한되므로 단순히 전송 메시지 감시뿐 아니라 노드간 협력에 의한 안전성제공이 필요하다.

셋째, 안전한 리프로그래밍 기술 연구 부분에 있어서 효율성과 안전성을 동시에 고려한 코드 분배 프로토콜 연구가 필요하다. 지금까지 안전성을 제공하는 코드분배 메커니즘들은 코드 최소화 방안을 고려하지 않은 Deluge를 기반으로 하고 있어서 효율성과 안전성을 동시한 고려한 연구가 진행되어야 한다.

넷째, 단순한 재밍이나 서비스거부 공격이 아닌 코드삽입을 통해 센서노드의 수행 코드를 변경하는 공격에 대한 가능성이 제시되고 있다. 이에 안전한 코드 수행에 대한 연구가 필요하다.

다섯째, 센서 네트워크 응용에 따라 다른 통신 구조를 갖는 경우가 있다. 예를 들어, 메디컬 센서 네트워크의 경우 센서노드의 이동성을 기본으로 하고 있고, 센서노드들로부터의 정보를 단순히 애그리게이션 하는 것이 의미가 없으며, 정보마다 전송의 우선순위 및 전송 주기가 다르다는 특징을 갖고 있어 일반 센서 네트워크와 큰 차이를 보이고 있다. 이처럼 응용에 맞는 맞춤형 안전성 제공 기술 연구가 필요하다.

여섯째, 하드웨어의 발전에 따라 센서노드의 처리 용량도 늘어나고 있지만, 보안 메커니즘 자체의 경량화 연구도 꾸준히 진행되어야 한다. 특히 공개키 기반의 암호 메커니즘이나 디지털 서명 등의 경량화 연구가 필요하다.

마지막으로, 상용화되고 있는 프로토콜 스택 예를 들어 IEEE 802.15.4를 채택한 Zigbee에서는 MAC 계층에 인증, 암호화 등의 기본 보안 메커니즘을 채택하고 있지만, CW(Contention Window)값 변조에 따른 공격 및 많은 요청 패킷을 코디네이터 노드에 전송함으로써 슬립거부(Sleep-of-Denial) 공격 등이 수행될 수 있다. 그러므로 표준화되고 있는 프로토콜 스택에 대한 안전성 강화가 추가 적용되어야 한다.

5. 결 론

본 논문에서는 센서 네트워크의 주요 연구 주제들에 대해 최근 진행되었던 안전성 제공 연구의 특징을 설명하고 비교 분석하였다. 또한 분석 결과를 통해 향후 연구 방향에 대해 제안하였다. 이를 통해 센서 네트워크에서의 안전성 제공 및 보안 메커니즘 연구 동향을 이해하고 해당 연구를 도모하며, 그 결과를 통해 센서 네트워크 활용도 및 빠른 적용의 제고를 가능하게 할 것이다.

참고문헌

[1] Lingxuan Hu, David Evans, "Secure Aggregation for Wireless Networks," Applications and the Internet Workshops, Jan. 2003.

[2] Wenliang Du, Jing Deng, Yumghsiang S. Han, Pramod K. Varchney, "Witness-Based Approach for Data Fusion Assurance In Wireless Sensor Networks," GLOBECOM, Dec. 2003.

[3] David Wagner, "Resilient Aggregation in Sensor Networks," 2nd ACM workshop on Security of ad hoc and sensor networks, 2004.

[4] Claude Castelluccia, Einar Mykletun, Gene Tasudik, "Efficient Aggregation of encrypted data in Wireless Sensor Networks," Mobile and Ubiquitous Systems: Networking and Services, Jul. 2005.

[5] Yi Yang, Xinran Wang, Sencun Zhu, Guo hong Cao, "SDAP: A Secure hop-by-Hop Data Aggregation Protocol for Sensor Networks," ACM Trans. Inf. Syst. Secur., vol.11, no.4, 2008.

[6] Levente Buttyan, Peter Schaffer, Istvan Vajada, "RANBAR: RANSAC-Based Resilient Aggregation in Sensor Networks," SASN, Oct. 2006.

[7] Bo Sun, Xing, Jin, Kui Wu, Yang Xiao, "Integration of Secure In-Network Aggregation and System monitoring for Wireless Sensor Networks," IEEE ICC, Jun. 2007.

[8] Donggang Liu and Peng ning, Wenliang Kevin Du, "Attack-Resistant Location Estimation in Sensor Networks," symposium on Information processing in sensor networks, 2005.

[9] Yurong Xu, Yi Ouyang, Zhengyi Le, James Ford, Fillia Makedon, "Analysis of range-free anchor-free localization in a wsn under wormhole attack," 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems, pp.344 - 351, 2007.

[10] Nidal Nasser, Yunfeng Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks," Computer Communications, vol.30, Issue 11-12, pp.2401-2412, Sep. 2007.

[11] Fen-hua Cheng, Jin Zhang, Zheng Ma, "Curve-Based Secure Routing Algorithm for Sensor Network," IIH-MSP, 2006.

[12] Zhen Cao, Jianbin Hu, Zhong Chen, Maoxing Xu, Xia Zhou, "FBSR: feedback-based secure routing protocol for wireless sensor networks," International Journal of Pervasive Computing and Communications, vol.4, pp.61-76, 2008.

[13] Jian Yin, Sanjay Madria, "ESecRout: An Energy Efficient Secure Routing Protocol for Sensor Networks," International Journal of Distributed Sensor Networks, 2007.

[14] J. W. Hui and D. and Culler, "The dynamic behavior of a data dissemination protocol for network programming at scale," International conference on Embedded networked sensor systems, pp.81 - 94, 2004.

[15] P. E. Lanigan, R. Gandhi, and P. Narasimhan, "Sluice: Secure dissemination of code updates in sensor networks," ICDCS, pp.53-63, July 2006.

[16] D. H. Kim, R. Gandhi, and P. Narasimhan, "Exploring Symmetric Cryptography for Secure Network Reprogramming," Wireless Ad hoc and Sensor Networks, pp.17-25, 2007.

[17] S Hyun, P Ning, A Liu, and W Du, "Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks," IPSN, pp.445-456, 2008.

[18] David R. Raymond, Scott F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol.7, no.1, pp.74-81, 2008.

[19] S. Doumit and D.P. Agrawal, "Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor network," MILCOM, vol.22, no.1, pp.609-614, 2003.

[20] P. Techateerawat and A. Jennings, "Adaptive Intrusion Detection in Wireless Sensor Networks," International Conference on Intelligent Pervasive Computing, 2007.

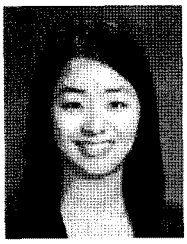
저자약력

김 미 희

1997년 이화여자대학교 전자계산학과(학사)
1999년 이화여자대학교 컴퓨터학과(석사)
1999년~2003년 한국전자통신연구원 연구원
2007년 이화여자대학교 컴퓨터공학과(박사)
2007년~2009년 이화여자대학교 컴퓨터공학과 전임강사
2009년~현재 미국 North Carolina State University Postdoc Researcher
관심분야 : 무선 네트워크(센서네트워크, 유비쿼터스 네트워크, 메쉬네트워크) 보안, 이동 네트워크 보안
이 메 일 : iceblueee@gmail.com

김 지 선

2007년 서울여자대학교 정보보호공학과(학사)
2007년~현재 이화여자대학교 컴퓨터공학과 석사과정
관심분야 : 센서네트워크 보안, 침입 대응 기술, 센서네트워크 리프로그래밍 기술
이 메 일 : 272lovelyjs@ewhain.net



김 아 름

2006년 중앙대학교 정보시스템학과 졸업(학사)
2009년 이화여자대학교 컴퓨터공학과 졸업 (석사)
관심분야 : 센서네트워크 보안, 침입 대응 기술
이 메 일 : reumreum@ewhain.net

채 기 준

1982년 연세대학교 수학과(학사)
1984년 미국Syracuse University 컴퓨터학과(석사)
1990년 미국 North Carolina State University 컴퓨터공학과(박사)
1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수
1992년~현재 이화여자대학교 컴퓨터공학과 교수
관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망/센서네트워크 (보안) 프로토콜 설계 및 성능분석
이 메 일 : kjchae@ewha.ac.kr