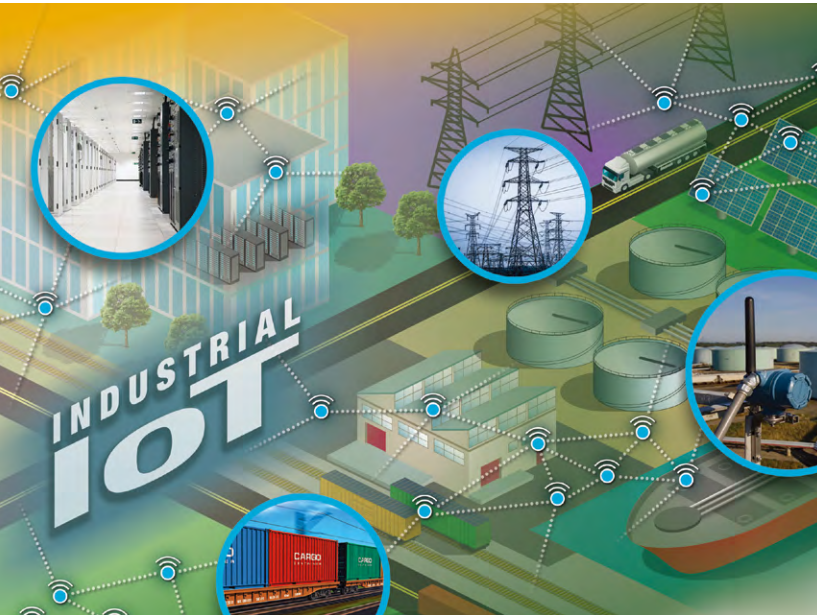


## 산업용 IoT의 무선 센서 네트워킹

산업용 IoT(사물 인터넷)와 여기에 필요로 하는 산업용 센서의 무선 접속과 관련해서 많은 논의들이 이루어지고 있다. 산업용 장비 및 애플리케이션의 네트워킹 요구는 컨슈머 분야와는 또 다른 것으로서 무엇보다도 신뢰성과 보안이 요구된다. 이 글에서는 산업용 무선 센서 네트워크의 고유한 요구사항들을 살펴본다.



글 | \*조이 와이스(Joy Weiss), 사장  
 \*\*로스 유(Ross Yu), 제품 마케팅 매니저  
 더스트 네트워크 제품 그룹(Dust Networks Product Group)  
 리니어 테크놀로지(Linear Technology)

저전력 프로세서, 지능형 무선 네트워크, 저전력 센서 등이 등장하고 빅데이터(Big Data) 분석 기술이 발전함에 따라, 산업용 IoT에 대한 관심이 점차 고조되고 있다. 간단히 말해 이 기술들을 사용할 수 있게 됨에 따라 통신과 전기 인프라를 사용할 수 있는 위치뿐만 아니라 “사물(thing)”의 상태, 위치, 식별 등에 관해서 유용한 정보를 모을 수 있는 곳이면 어느 곳이든(anywhere) 다

양한 유형의 센서들을 설치할 수 있게 됐다. 센서를 사용해서 기계, 펌프, 파이프라인, 열차 같은 “사물”을 측정할 수 있게 한다는 개념은 산업용 분야에서 새로운 것은 아니다. 산업용 분야에서는 정유 플랜트에서부터 제조 라인에 이르기까지 이미 다양한 용도의 센서 및 네트워크들이 널리 사용되고 있다. 전통적으로 이러한 OT(operation technology) 시스템은 별도의 네트워

크로 가동하면서 컨슈머 기술로는 달성할 수 없는 네트워크 신뢰성과 보안성을 유지하도록 했다. 이러한 높은 수준의 신뢰성과 보안성을 요구함으로써 이용할 수 있는 기술들이 중요도 높은 산업용 IoT 애플리케이션에 적합한 것들로만 한정되게 됐다. 특히 이들 센서들을 어떻게 네트워킹 하느냐가 산업용 애플리케이션의 특징인 혹독한 환경에서도 센서들을 안전성, 보안성, 경제성

측면에서 얼마만큼 뛰어나게 구축할 수 있을 것인가를 결정짓는다. 이와 관련해서 이 글에서는 산업용 무선 센서 네트워크(WSN)를 구현하기 위해서 어떤 점들이 요구되는지를 살펴본다.

## 무엇보다 중요한 신뢰성과 보안

컨슈머 애플리케이션에서는 대개 가격(비용)이 시스템의 가장 중요한 고려사항인 것에 반해서, 산업용 애플리케이션에서는 신뢰성과 보안성을 가장 중요하게 요구한다. 시장조사 회사인 OnWorld의 전 세계 산업용 WSN 사용자 조사에 따르면, 응답자들은 신뢰성과 보안성을 가장 중요한 문제로 보고 있는 것으로 나타났다<sup>[1]</sup>. 이러한 조사 결과는 놀랄 바가 아닌 것이, 어떤 회사가 제품을 생산할 때의 수익성, 품질, 효율성과 작업자 안전성을 달성하는 것이 이러한 네트워크를 토대로 하기 때문이다. 바로 이 점에서 산업용 무선 센서 네트워크를 위해서는 신뢰성과 보안성이 그처럼 중요하게 요구되는 것이다.

네트워크를 설계할 때 신뢰성을 달성하기 위한 한 가지 원칙은 이중화(redundancy)를 구현하는 것이다. 이중화는 일어날 가능성이 있는 문제에 대해서 페일오버(failover, 고장 시 대체 시스템으로 전환) 메커니즘을 구축함으로써 데이터 소실을 일으키지 않고서 시스템을 복구할 수 있게 하는 것이다. 무선 센서 네트워크 분야에서는 이러한 이중화를 구현하기 위해서 기본적으로 두 가지 방식이 가능하다. 첫째는 공간적 이중화로서, 이것은 모든 무선 노드가 최소한 2개의 다른 노드들과 통신할 수

있게 함으로써 전달 체계를 사용해서 데이터가 둘 중 어느 한 노드로 전달되게 하고 의도하는 최종 목적지에 도착할 수 있게 하는 것이다. 그럼으로써 잘 설계된 메시 네트워크(모든 노드가 2개 혹은 그 이상의 인접 노드들과 통신할 수 있는 네트워크)는 첫 번째 경로를 이용할 수 없게 되었을 때 자동으로 알아서 대안 경로를 데이터를 전송함으로써 점대점(point-to-point) 네트워크에 비해서 더 높은 신뢰성을 달성할 수 있다.

둘째는 이 이중화 외에도 또 다른 층위의 이중화로서 RF 스펙트럼으로 가능한 다중의 채널들을 활용하는 것이다. 이것은 채널 호핑(channel hopping)이라는 개념으로서, 노드 쌍들이 매 전송에 대해서 채널을 변경할 수 있는 것이다. 그럼으로써 계속해서 변화하는 거친 RF 환경을 가진 산업용 애플리케이션에서 어떤 특정 채널이 일시적으로 문제가 생겼을 때 다른 채널을 사용해서 전송을 할 수 있다. IEEE 802.15.4 2.4GHz 표준에서는 호핑에 15개 확산 스펙트럼(spread spectrum, SS) 채널을 사용할 수 있게 함으로써, 호핑을 사용하지 않는(단일 채널) 시스템에 비해서 채널 호핑 시스템은 훨씬 더 높은 탄력성이 가능하다. 이러한 이중적인 공간 및 채널 이중화를 TSCH(Time Slotted Channel Hopping)이라고 한다. 현재 TSCH를 비롯한 다수의 무선 메시 네트워킹 표준이 나와 있다(IEC62591\_WirelessHART, 조만간 발표 예정인 IETF 6TiSCH 표준 등)<sup>[2]</sup>. 이들 메시 네트워킹 표준은 전 세계적으로 이용할 수 있는 비면허 2.4GHz 스펙트럼 대의

무선 대역을 사용하는 것으로서, 리니어 테크놀로지의 Dust Networks® 그룹은 선구적으로 TSCH 프로토콜을 사용해서 자원 사용이 여의치 않은 저전력 장비에 사용할 수 있도록 2002년부터 SmartMesh® 제품을 내놓고 있다.

TSCH는 거친 RF 환경에서도 데이터 신뢰성을 달성하기 위한 필수적인 요소인 한편, 다년간 문제를 일으키지 않으면서 연속적으로 가동할 수 있도록 하기 위해서는 메시 네트워크를 적절히 구축하고 유지관리하는 것 또한 중요하다. 산업용 무선 네트워크는 통상적으로 수년간 지속적으로 작동해야 하며 작동 수명 동안 RF가 심하게 유동적이고 데이터 전송 요구가 계속해서 바뀔 수 있다. 그러므로 결론적으로 유선과 같은 수준의 신뢰성을 달성하기 위해서는 링크 품질을 지속적으로 모니터링 해서 RF 환경에 대한 간섭이나 변화에도 불구하고 스루풋(throughput)을 극대화하도록 네트워크 토폴로지를 역동적으로 최적화할 수 있는 지능적인 네트워크 관리 소프트웨어를 필요로 한다.

보안성은 산업용 무선 센서 네트워크(WSN)의 또 다른 중요한 요구사항이다. WSN에서 보안성을 달성하기 위해서는 다음과 같은 목표를 달성해야 한다:

**기밀성(confidentiality)**—네트워크로 전송되는 데이터를 의도하는 수신자가 아닌 다른 사람이 읽지 못하게 해야 한다.

**무결성(integrity)**—어떤 메시지를 수신했을 때 그 메시지가 내용이 첨가되거나, 삭제되거나, 조작되지 않고 원래 전송된 그대로라는 것을 확인할 수 있어야 한다.

정식성(authenticity)-어떤 출처에서 보낸 메시지라고 했을 때 그 출처가 사실로 맞아야 한다. 시간을 인증 체계의 한 부분으로 사용하면 메시지를 기록했다가 재생하는 방법의 공격을 방지할 수 있다.

이러한 목표들을 달성하기 위해서 WSN으로 도입할 수 있는 주요한 보안 기술들로는 견고한 키 및 키 관리를 사용한 강력한 암호화(AES128 등), 재생(replay) 공격을 방지하기 위한 암호화 급 난수 생성기, 매 메시지에 대한 메시지 무결성 검사(MIC), 특정 장치에 대한 액세스를 명시적으로 허용하거나 거부하기 위한 액세스 제어 리스트(ACL) 등을 들 수 있다. 이러한 첨단 무선 보안 기술들을 오늘날 WSN을 이루고 있는 많은 장치들로 즉시 적용할 수 있는데, 모든 WSN 제품 및 프로토콜들이 이들 모든 조치들을 모두 적용하고 있는 것은 아니다<sup>[3]</sup>. 또 한 가지 유의할 점은, 보안적인 WSN을 보안에 취약한 게이트웨이로 연결하면 또 다른 취약 지점이 될 수 있으므로 시스템 디자인을 설계할 때 단에서 단까지 전체적인 보안성을 고려해야 한다는 것이다.

### 산업용 IoT는 무선 전문가가 설치하지 않는다

많은 업체들이 기존 제품들에 더해서 산업용 IoT 제품 및 서비스를 추가하고 있으며, 이들 업체의 고객들은 기존 장비와 신규 장비가 혼합된 환경으로 이러한 제품들을 설치하고 있다. 그러므로 산업용 WSN으로 지능을 구축함으로써 기존의 필드 작업자들이 산업용

IoT 제품으로 이전하는 작업을 간편하고도 매끄럽게 할 수 있도록 해야 한다. 네트워크가 신속하게 스스로 구성할 수 있게 해서 설치 작업자가 네트워크가 안정적으로 작동하는 것을 확인하고서 현장을 떠날 수 있도록 해야 하며, 접속이 취약하거나 접속이 끊어졌을 때 스스로 조치를 취해서 서비스 중단이 일어나지 않도록 해야 하며, 서비스 중단이 발생했을 때는 자동으로 보고와 진단을 하도록 해야 하며, 설치 후에는 유지보수를 거의 또는 전혀 필요하지 않게 함으로써 비싼 인건비가 들어가는 현장 파견을 피하도록 해야 한다. 또한 많은 애플리케이션에서 성공적인 구현을 달성하기 위한 한 가지 관건은 접근하기 어렵거나 또는 위험한 위치에 설치를 할 수 있느냐 하는 것이다. 이럴 때는 IoT 장비를 배터리로 작동해야 하고 배터리로 작동하면서 수명이 통상적으로 5년 이상 지속돼야 한다.

또한 시스템을 세계 어느 지역이나 설치할 수 있어야 한다. 어떤 회사에서 회사 전체적으로 산업용 IoT를 광범위하게 구축하고자 할 경우에 여러 국가의 표준에 따라서 설치를 해야 할 수 있기 때문이다. 다행히 IEEE 802.15.4e TSCH를 비롯해 이러한 요구를 반영하고 충족하는 국제적 무선 산업 표준들이 있다.

### 어느 곳이든 센서 설치 가능

산업용 IoT 애플리케이션을 위해서는 센서나 제어 위치를 적재적소에 배치해야 한다. 무선 기술은 선 없이 통신을 할 수 있다고 하지만 무선 노드를 구동하기 위해서 전력망으로 연결해야 한다는

지, 아니면 수시간마다 혹은 수개월마다 재충전을 해야 한다면 설치비용이 급격히 올라가고 실용성 또한 떨어질 것이다. 예를 들어, 유선이라면 가동 중인 장비의 상태를 모니터링 하기 위해서 회전하는 장비로 센서를 부착하는 것이 가능하지 않을 것이다. 그런데 가동 중인 장비를 모니터링 해서 얻는 정보를 사용해서 중요도 높은 장비를 예방적으로 유지관리함으로써 높은 손실을 초래하는 예기치 않은 시스템 중단을 피할 수 있다.

그러므로 비용을 절감하면서 유연하게 구축을 할 수 있도록 하기 위해서는 산업용 WSN의 모든 노드가 배터리를 사용해서 최소한 5년 이상 작동할 수 있어야 한다. 산업용 TSCH 기반 WSN의 예로서, 리니어 테크놀로지(Lin Technologies)의 SmartMesh 제품은 정격적으로 50  $\mu$ A 보다 훨씬 미만으로 동작하므로 2개 AA 배터리를 사용해서 다년간 동작할 수 있다. 우수한 하베스트 에너지 소스를 사용할 수 있는 환경이라면 에너지 하베스팅을 사용해서 노드들을 영구적으로 가동할 수도 있다(그림 1).

### 시간의 문제

산업용 모니터링 및 제어 네트워크는 사업적으로 중요한 요소이다. 제품을 생산하기 위한 기본적인 비용에 영향을 미치며 데이터의 적시성(timeliness)을 중요하게 요구한다. 지난 10여 년에 걸쳐서 확정적 TSCH 기반 WSN 시스템은 현장에서 다양한 유형의 모니터링 및 제어 애플리케이션으로 검증되어 왔다. WirelessHART 같은 이러한 시간 슬롯(time-slotted) 시스템은 시간 스

탬프를 사용한 시간 한정적 데이터 전송을 제공한다. 이들 네트워크에서는 데이터를 전송하기 위해서 더 많은 기회를 필요로 하는 노드들에 자동으로 더 많은 시간 슬롯을 부여할 수 있으며, 네트워크 상의 연속적인 경로로 다중의 시간 슬롯을 부여함으로써 네트워크를 점유하면서 낮은 지연시간으로 전송이 이루어지도록 할 수 있다. 이와 같이 데이터 전송을 중재함으로써 전송이 빈번한 조밀한 네트워크를 훨씬 더 잘 구축할 수 있다. TSCH를 기반으로 하지 않은 무선 네트워크는 이러한 시간 스케줄링을 사용하지 않으므로 무선 트래픽이 한꺼번에 몰려들 때 이를 처리하지 못해서 장애가 일어날 수 있다.

또한 TSCH 네트워크는 모든 패킷으로 전송된 시간을 지시하는 정확한 시간 스탬프를 포함하며, 또한 필요하면 네트워크 전체적 차원의 시간을 사용해서 WSN 노드 네트워크 전체에 걸쳐서 제어 신호들을 중재할 수 있다. 시간 스탬프 데이터를 사용하면 데이터를 순서 없이 수신하였더라도 애플리케이션이 데이터를 적절히 시퀀싱할 수 있으므로 다중의 센서들로부터 들어오는 정보들을 처리해야 하는 산업용 애플리케이션에서 문제의 원인과 결과를 정확하게 진단하기 위해서 유용할 수 있다.

## 네트워크 동작에 대한 가시성

산업용 네트워크는 몇 년씩 중단 없이 동작해야 하는데, 아무리 네트워크가 견고하게 설계되었다 하더라도 문제는 여전히 일어날 수 있다. 설치 시에는 네트워크 품질이 좋았더라도 작동 수명이 접



[그림 1] 어느 곳이든 센서 설치 가능 -ABB의 이 열 하베스트 무선 온도 센서와 같이 하베스트 에너지를 사용해서 영구적으로 가동되는 저전력 무선 센서 노드를 산업용 환경에서 어느 위치에나 설치하고 추가적인 데이터를 포착할 수 있다.

점 지나면서 다양한 환경적 요인의 영향을 받을 수 있다. 어떠한 산업용 네트워크든 이러한 문제들을 초기에 적절히 식별해낼 수 있어야 하며, 서비스 품질을 달성하기 위해서는 이러한 문제들을 신속하게 진단하고 조치를 취할 수 있어야 한다. 그런데 가시성을 제공하고자 할 때 네트워크 관리의 지표라는 측면에서 모든 무선 센서 네트워크가 동일하게 설계되는 것은 아니다. 그러므로 최소한의 의미에서 산업용 무선 네트워크 관리 시스템은 다음과 같은 측면에 대해서 가시성을 제공해야 할 것이다:

- 무선 링크의 품질, 신호 강도(RSSI)로 측정
- 종단간(end-to-end) 패킷 성공률
- 메시 품질, 신뢰성을 유지하기 위해서 충분한 대안적 경로들을 갖지 못한 노드 하이이라이트로 표시
- 노드 상태와 배터리 수명(해당되는 경우)

뛰어난 산업용 구현이 되기 위해서는 지능적 네트워크가 데이터를 자동으로 다른 대안적 경로로 전송하도록 재지정함으로써 이러한 문제들을 스스로 치유할 수 있어야 하고, 또 한편으로는 성능을 극대화하도록 네트워크 토폴로지를 지속적으로 업그레이드할 수 있어야 할 것이다(그림 2).

## 지능적 사물에 지능적 네트워크

오늘날 “사물들”로 갈수록 더 높은 지능을 집어넣고자 하고 있으며, 산업용 IoT 애플리케이션을 위해서 지능화는 비단 이 지점에서만 필요한 것이 아니다. 산업용 IoT 네트워크는 지능적인 최종 노드를 구현해야 할 뿐만 아니라 지능적인 네트워크 및 보안 관리 기능들을 포함해야 한다. 네트워크를 고도로 구성 가능하게 해서 특정한 애



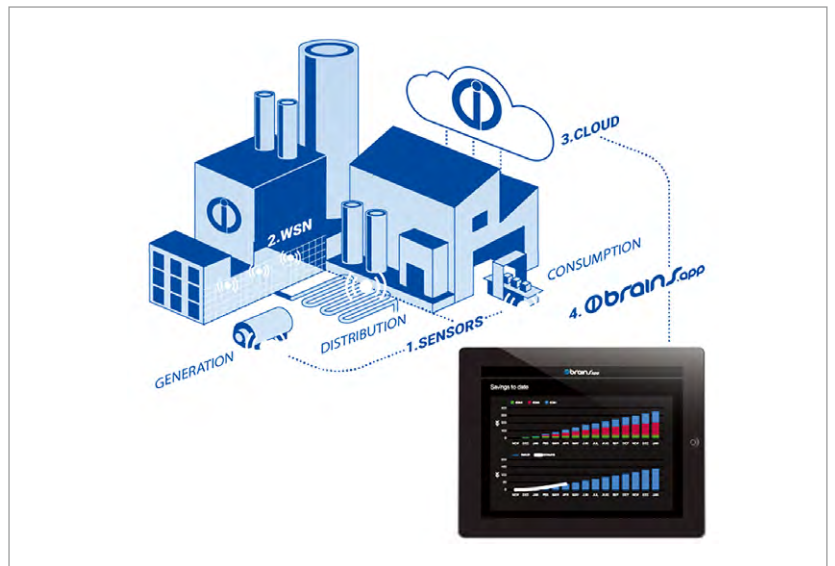
플리케이션 필요에 재빨리 적응할 수 있도록 해야 한다. 또한 배터리 수명을 연장하기 위해서는 전력 소모를 낮춰야 하므로 네트워크의 가용 전력을 스스로 인지하고 네트워크 차원의 전력 소모를 최소화하도록 지능적인 루팅을 할 수 있어야 한다. 또한 네트워크를 RF 환경이 변화하는 것에 자동으로 적응할 수 있도록 해야 하고, 이를 위해서 토폴로지를 동적으로 변경할 수 있게 하면 더욱 더 유리할 것이다. 리니어 테크놀로지의 SmartMesh Network Manager는 네트워크 보안, 관리, 루팅 최적화를 할 수 있을 뿐만 아니라, 필요하다면 사용자가 무선으로(over the air) 노드들을 재프로그래밍할 수 있으므로 향후 요구의 변화에 따라서 편리하게 업그레이드 할 수 있는 수단을 제공한다.

### 맺음말

산업용 분야에서 IoT에 대한 관심이 날로 높아지고 있으며, 투자수익(ROI)을 높이기 위해서 사업적으로 중요한 요소로서 자리잡고 있다. 중요도가 높은 애플리케이션으로서 산업용 무선 센서 네트워크는 지능화, 보안성, 다년간 무선으로 동작할 때의 신뢰성에 대해서 높은 수준의 요건을 충족해야 한다. 기존에 등장해 있거나 혹은 조만간 발표될 예정인 무선 메시 네트워크 표준들을 적용함으로써 이러한 엄격한 요구들을 충족할 수 있다. 이 기술을 사용함으로써 산업용 IoT 시대에 산업용 고객들이 자사의 비즈니스와 서비스를 발전적으로 변화시켜나갈 수 있을 것이다. **ES**



[그림 2] 네트워크 가시성—Emerson Process Management의 SNAP-ON 소프트웨어 유틸리티 같은 네트워크 관리 소프트웨어를 사용해서 무선 네트워크의 건전성에 관한 가시성을 제공할 수 있다.



[그림 3] 변화 가속화—IntelliSense.io의 Brains.App 소프트웨어 같은 소프트웨어 분석을 사용함으로써 산업용 무선 센서 네트워크로부터 얻은 데이터를 활용해서 플랜트 가동을 능률적으로 개선하고 수율을 높이고 안전성을 향상시킬 수 있다.

### 참고자료

1. Industrial Wireless Sensor Networks: Trends and Developments, <https://www.isa.org/standards-publications/isa-publications/intech-magazine/2012/october/web-exclusive-industrial-wireless-sensor-networks/#sthash.c3G9ze5.dpuf>
2. 6TiSCH Wireless Industrial Networks: Determinism Meets IPv6: Maria Rita Palattella<sup>1</sup>, Pascal Thubert<sup>2</sup>, Xavier Vilajosana<sup>3,4</sup>, Thomas Watteyne<sup>4,5</sup>, Qin Wang<sup>4,6</sup>, and Thomas Engel<sup>1</sup> Published in: Communications Magazine, IEEE (Volume:52, Issue: 12)
3. Secure Wireless Sensor Networks Against Attacks, Kristofer Pister and Jonathan Simon, <http://electronidedesign.com/communications/secure-wireless-sensor-networks-against-attacks>