

Wired Bridge Node : 유무선 통신을 동시에 지원하는 복합 센서 네트워크 구조 설계

김병철*, 이동규*, 박성호*, 김태현*, 강순주*

*경북대학교 일반대학원 전자전기컴퓨터학과

e-mail : { gos337, edongq, ndr703, namestrike, sjkang }@ee.knu.ac.kr

Wired Bridge Node : Design of Complex Sensor Network Architecture Simultaneously Supporting Wired and Wireless Communication

Byung-Chul Kim*, Dong-Kyu Lee*, Sung-Ho Park*, Tae-Hyon Kim*, Soon-Ju Kang*

*School of Electrical Engineering and Computer Science, Kyung-Pook National University

요 약

본 연구에서는 무선 센서 네트워크에서 공용 주파수 대역 2.4GHz 를 여러 무선 프로토콜이 사 용함으로 발생하는 간섭 및 충돌에 의한 전송 성능 저하 문제를 해결하기 위한 방법으로 무선 센서 네트워크의 일부 센서 노드들을 Wired Bridge Node 로 연결하는 방법을 제안한다. 이를 증명하기 위 해, 무선 통신과 유선 통신을 동시에 지원하는 Wired and Wireless MAC 을 포함하는 센서 노드인 Wired Bridge Node 의 소프트웨어 구조를 제안하고 이 시스템을 검증하였다.

1. 서론

USN 은 현장에 설치된 각종 센서 노드들에서 수집 한 정보를 사용자에게 보내기 위해 구성된 네트워크 를 말하며 WPAN, ad-hoc 네트워크 등의 기술이 발전 함에 따라 무선 센서네트워크 기술이 매우 활성화되 고 있다.

USN 기술을 이용하여 무선 센서네트워크를 구축 하려는 지역에 동일한 주파수 대역을 사용하는 무선 네트워크가 이미 구축되어 운용되고 있는 경우 각 네 트워크에서 발생한 데이터 트래픽이 서로 다른 네트 워크에는 간섭[1]으로 작용하여 통신 장애[2][3]가 발 생하며 그 정도가 심한 경우에는 전파적 차폐 지역이 생겨 하나의 무선 센서네트워크를 서브 네트워크들로 분리하여 구축해야 한다. 또한 냉동 컨테이너나 종자 은행의 유전자 저장소 같이 외부와 물리적으로 차폐 되어 있지만 내부의 무선 센서 노드가 외부의 무선 센서 네트워크와 정보교환을 해야 하는 시스템도 물 리적 차폐 지역을 위한 서브 네트워크를 별도로 구축 해야 한다.

본 논문에서는 USN 에서 전파적 또는 물리적 차폐 로 인한 네트워크 단절 문제를 해결하기 위하여 WBN(Wired Bridge Node)을 제안한다. WBN 은 무선 통 신과 유선 통신을 함께 지원하여 단절된 무선 네트워 크를 유선으로 연결하여 하나의 네트워크로 구성할

수 있다. 그리고 WBN 은 기존의 무선 센서 노드들에 탑재되는 어플리케이션의 수정 없이 동작이 가능하여 호환성 및 확장성을 가진다.

본 논문의 2 장에서는 무선 센서 네트워크의 기본 개념 및 관련 연구에 대하여 알아보고, 3 장에서는 본 논문에서 제안하는 WBN 의 소프트웨어 구조와 특징 에 대하여 살펴본다. 4 장에서는 본 논문에서 제안한 시스템을 검증하고 5 장에서 결론을 맺는다.

2. 기본 개념 및 관련 연구

2.1 IEEE 802.15.4 와 ZigBee

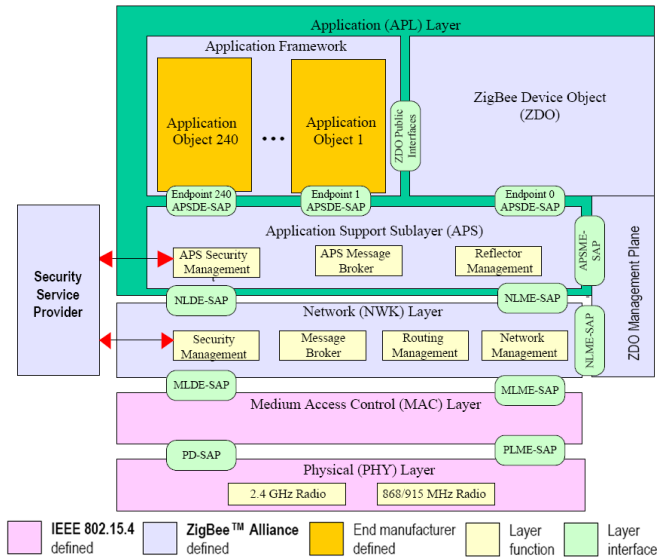
IEEE 802.15.4[4] 프로토콜은 2003 년에 IEEE (Institute of Electrical and Electronics Engineers)에 의해 공인되었으며, 낮은 데이터 전송률과 낮은 소비전력 요구에 중점을 두었기 때문에 802.11 과는 다르게 분 류된다. 실제 전송률은 20~250kbps 정도이며 표 1 과 같이 PHY 계층에서 사용하는 3 가지 무선 주파수에 따라 달라진다. 그리고 노드의 저전력 소모를 줄이기 위한 방법으로 크게 Reduced Function Devices (RFD)와 Full Function Devices (FFD), 두 가지로 노드형태를 구 분하고 있다.

<표 1> 주파수 대역과 전송률

PHY (MHz)	Frequency band (MHz)	Chip rate (kchips/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868	868~868.6	300	BPSK	20	20	Binary
915	902~928	600	BPSK	40	40	Binary
2450	2400~2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

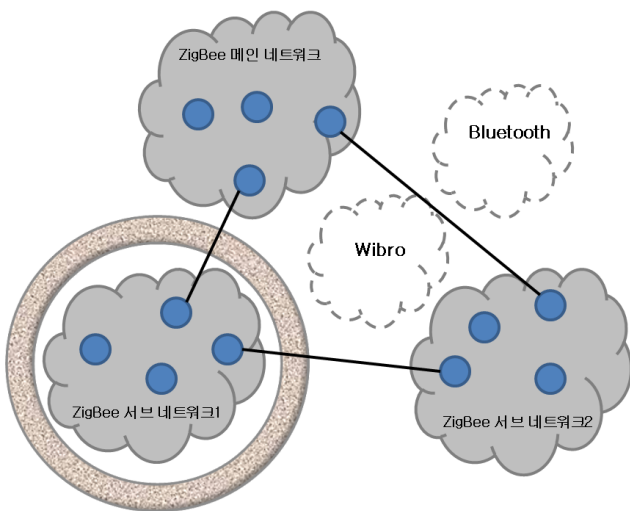
* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2009-C1090-0902-0020)

ZigBee[5]는 2003년 IEEE 802.15.4 작업분과위원회에서 표준화된 PHY/MAC 층을 기반으로 상위 프로토콜을 규격화한 기술이다. ZigBee Alliance는 다양한 칩 제조사와 SI(System Integration) 업체가 저전력 무선 통신의 표준을 정의하기 위해서 상호협동하는 회사들의 연합이며, 데이터 보안에 있어서 서로 다른 네트워크 토폴로지를 어떻게 구성할 것인지 연구하고, 호환성 있는 어플리케이션 프로파일에 대한 명세서를 정의하는데 목적을 둔다. 그림 1은 ZigBee 프로토콜 스택을 나타낸 그림이다.



(그림 1) ZigBee 프로토콜 스택

2.2 개발 동기와 요구분석



(그림 2) 서버 네트워크로 분리된 ZigBee 네트워크

USN 기술 중 ZigBee는 IEEE 802.15.4에서 표준화되었으며, 듀얼 물리계층 형태로 주파수 대역은 2.4GHz, 868/915MHz를 사용하고, 데이터 전송 속도는 20~250kbps이다. 가용한 주파수 대역 중 2.4GHz는 공용 주파수 대역으로 Wibro, Bluetooth 등의 다른 무선 네트워크 프로토콜과 함께 쓰인다.[6] 따라서 그

림 2와 같이 ZigBee 프로토콜을 이용하여 무선 센서 네트워크를 구축하려는 지역에 Wibro, Bluetooth 등과 같이 동일한 주파수 대역을 사용하는 무선 네트워크가 이미 구축되어 운용되고 있는 경우 Wibro, Bluetooth 네트워크에서 발생한 데이터 트래픽이 ZigBee 네트워크에는 간섭으로 작용하여 통신 장애가 발생하며 그 정도가 심한 경우에는 전파적 차폐 지역이 생겨 전체 ZigBee 네트워크를 서버 네트워크들로 분리하여 구축해야 한다. 또한 냉동 컨테이너나 종자 은행의 유전자 저장소 같이 외부와 차폐되어 있지만 내부의 무선 센서 노드가 외부의 무선 센서 네트워크와 정보교환을 해야 하는 시스템도 물리적 차폐 지역을 위한 서버 네트워크를 별도로 구축해야 한다. 전체 시스템이 서버 네트워크들로 구축됨에 따라 각 서버 네트워크에서 센서 노드들이 수집한 다양한 정보들을 사용자가 사용하기 위해서는 분리된 네트워크로부터 수집된 정보를 가져오기 위한 시스템을 추가적인 비용을 들여 구축해야 한다.

USN에서 전파적 또는 물리적 차폐로 인한 네트워크 단절 문제를 해결하기 위해서 유선 통신을 이용하여 무선 센서네트워크의 특정 노드들을 연결하는 것을 생각해 볼 수 있다. 그림 2와 같이 메인 네트워크와 서버 네트워크 1, 서버 네트워크 2로 분리된 ZigBee 네트워크를 유선 통신을 이용하여 각 서버 네트워크와 메인 네트워크의 특정 노드를 연결하면 분리된 무선 네트워크를 하나의 무선 네트워크로 만들 수 있다.

분리된 무선 네트워크를 유선으로 연결하여 하나의 무선 네트워크로 구성하기 위해서는 다음 몇 가지 사항이 요구된다. 첫째, 고유 USN 기술에 대한 수정이 없어야 한다. 각 노드마다 분리된 무선 네트워크 간 통신을 위한 프로토콜 스택의 수정이나 부가적인 어플리케이션이 필요하다면 유지관리뿐만 아니라 호환성에도 문제가 발생하기 때문이다. 둘째, 분리된 무선 네트워크에 있는 노드들 간의 통신은 동일 무선 네트워크 내부에서 통신이 이루어지는 것처럼 인식할 수 있어야 한다.

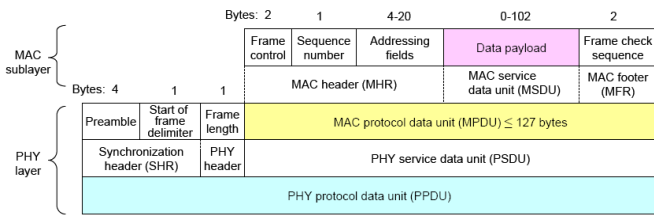
3. Wired Bridge node의 소프트웨어 구조와 특징

본 논문에서는 USN에서 전파적 또는 물리적 차폐로 인한 네트워크 단절 문제를 해결하기 위하여 WBN을 제안한다.

Application	
Network Layer	
Wired and Wireless MAC	
Wireless Physical	Wire Physical

(그림 3) Wired and Wireless MAC을 포함하는 Wired Bridge node의 소프트웨어 구조

그림 3 은 WBN 의 소프트웨어 구조를 나타낸다. WBN 은 무선 통신과 유선 통신을 함께 지원하는 Wired and Wireless MAC 을 포함한다. 유선 통신으로 송수신 되는 패킷의 헤더는 그림 4 의 IEEE 802.15.4 의 데이터 프레임 포맷에서 PHY layer 포맷의 Start of frame delimiter 와 Frame length 를 포함하고 패킷의 데이터는 MAC sublayer 포맷을 따르며 무선 통신으로 송수신되는 패킷은 PHY layer 포맷을 따른다. 따라서 Wired and Wireless MAC 은 무선 통신과 유선 통신을 통해 동일한 MAC sublayer 포맷 형식으로 패킷을 처리하며 Network layer 에게 MSDU 를 전달하여 Network 패킷을 처리하게 한다.

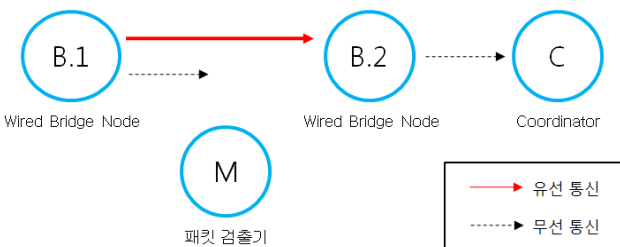


(그림 4) IEEE 802.15.4 의 데이터 프레임 포맷

WBN 이 전파적 또는 물리적 차폐 지역에서 유선 통신으로 연결되어 통신할 경우에는 유선 통신으로 수신된 MAC sublayer 가 Wired and Wireless MAC 에서 처리되어 MSDU 가 Network layer 로 전달된다. Network layer 는 network 패킷의 NWK Dest. Address 를 참조하여 목적지가 자신인 경우 어플리케이션으로 데이터 수신을 알리고 목적지가 다른 센서 노드인 경우 network 패킷을 라우팅시킨다. 따라서 WBN 의 이용에 따른 network 프로토콜 스택의 수정이나 어플리케이션의 수정 없이 기존 시스템과의 호환성을 제공하고 분리된 무선 네트워크에 있는 노드들 간의 통신이 동일 무선 네트워크 내부에서 통신이 이루어지는 것처럼 인식된다.

4. 실험 구성 및 결과

4.1 실험 구성



(그림 5) Wired Bridge node 실험 구성도

실험을 위하여 그림 5 와 같이 3 개의 센서 노드와 무선 센서 네트워크 상의 패킷을 모니터링하기 위해 패킷 검출기를 사용하였다. 무선 센서 네트워크의 프로토콜은 ZigBee 를 사용하였고 TI 사의 Z-Stack 을 이용하여 구현하였다. 3 개의 센서 노드 중 1 개는 코디네이터로 동작하고 나머지 2 개는 WBN 으로 동작하며

두 WBN 사이의 유선연결은 RS232 를 사용하였다. 모든 센서 노드는 TI 사의 CC2430EM 모듈[7]을 사용하였으며 패킷 검출기는 TI 사의 CC2430DB 모듈을 사용하였다. 그리고 패킷 검출기에서 모니터링한 패킷은 TI 사의 소프트웨어인 Packet Sniffer CC2430[8]을 통해 확인하였다.

실험 방법은 코디네이터에 WBN B.2 를 조인시킨 후 WBN B.1 을 WBN B.2 에 조인시킨다. 이후 전파적 또는 물리적 차폐 지역처럼 무선 통신에 장애되는 환경을 만들기 위해 WBN B.1 을 WBN B.2 로부터 더 먼 거리에 위치시켜 WBN B.1 이 패킷을 무선 통신으로는 WBN B.2 에 전송하지 못하지만[9] RS232 를 통해서 전송하게 한다. 패킷 검출기는 WBN B.1 과 WBN B.2 의 중간에 위치시켜 두 WBN 가 무선으로 전송하는 패킷을 모니터링한다. WBN B.1 은 조인 과정을 거친 후 10 초 후에 일정 시간 간격으로 코디네이터를 목적지로 하는 패킷을 발생시킨다.

4.2 실험 결과

ZigBee 네트워크에서 코디네이터의 short address 는 항상 0x0000 으로 초기화되며 WBN B.2 를 켜고 WBN B.2 는 조인 과정을 거쳐 코디네이터로부터 0x0001 을 short address 로 할당 받았다. 그 후 WBN B.1 을 켜서 WBN B.1 이 WBN B.2 에 조인 과정을 거쳐 0x0002 를 short address 로 할당 받았다. 조인 과정이 완료된 WBN B.1 을 그림 5 와 같이 WBN B.1 을 WBN B.2 와 코디네이터로부터 더 먼 거리에 위치시켜 WBN B.1 이 패킷을 무선 통신으로는 WBN B.2 와 코디네이터에 전송하지 못하게 한 후 Packet Sniffer CC2430 을 통해 패킷을 모니터링하였다.

P.nbr.	Time (us)	Length	Frame control field					Sequence number	Dest. PAN	Dest. Address	Source Address																											
RX	+2948	47	Type	Ver	DR	RF	Sec	40	0C	01	00	01	0F	0C	1A	31	32	33	34	35	36																	
	+4797208		DATA	0	0	0	1	37	38	39	30	31	32	33	34	41	43	4B	00	02	06																	
MAC payload																																						
48 00 00 00 02 00 0A 1C 40 0C 01 00 01 0F 0C 1A 31 32 33 34 35 36 37 38 39 30 31 32 33 34 41 43 4B 00 02 06																																						
IWK Frame control field																																						
Type	Version	DR	RF	Sec	IWK Dest. Address	IWK Src. Address	Broadcast Radius	Broadcast Seqnum	IWK payload													LOI	FCS															
DATA	0x2	1	0	0	0x0000	0x0002	0x0A	0x1C	40	0C	01	00	01	0F	0C	1A	31	32	33	34	35	36	37	38	39	30	31	32	33	34	41	43	4B	00	02	06	32	0x
APS Frame control field																																						
Type	Del. side	Ind. on	Sec	ACK	APS Dest. Endpoint	APS Cluster Id	APS Profile Id	APS Src. Endpoint	APS Counter	APS Payload													LOI	FCS														
Data	Broadcast	0	0	1	0x0C	0x0001	0x0F01	0x0C	26	31 32 33 34 35 36 37 38 39 30 31 32 33 34 41 43 4B 00 02 06													32	0x														

(그림 6) Wired Bridge node B.1 의 패킷

P.nbr.	Time (us)	Length	Frame control field					Sequence number	Dest. PAN	Dest. Address	Source Address																											
RX	+5167	47	Type	Ver	DR	RF	Sec	40	0C	01	00	01	0F	0C	1A	31	32	33	34	35	36																	
	+4804264		DATA	0	0	0	1	37	38	39	30	31	32	33	34	41	43	4B	00	02	06																	
MAC payload																																						
48 00 00 00 02 00 09 1C 40 0C 01 00 01 0F 0C 1A 31 32 33 34 35 36 37 38 39 30 31 32 33 34 41 43 4B 00 02 06																																						
IWK Frame control field																																						
Type	Version	DR	RF	Sec	IWK Dest. Address	IWK Src. Address	Broadcast Radius	Broadcast Seqnum	IWK payload													LOI	FCS															
DATA	0x2	1	0	0	0x0000	0x0002	0x09	0x1C	40	0C	01	00	01	0F	0C	1A	31	32	33	34	35	36	37	38	39	30	31	32	33	34	41	43	4B	00	02	06	140	0x
APS Frame control field																																						
Type	Del. side	Ind. on	Sec	ACK	APS Dest. Endpoint	APS Cluster Id	APS Profile Id	APS Src. Endpoint	APS Counter	APS Payload													LOI	FCS														
Data	Broadcast	0	0	1	0x0C	0x0001	0x0F01	0x0C	26	31 32 33 34 35 36 37 38 39 30 31 32 33 34 41 43 4B 00 02 06													140	0x														

(그림 7) Wired Bridge node B.2 의 패킷

그림 6 과 그림 7 은 Packet Sniffer CC2430 로 수집한 패킷으로써 그림 6 은 WBN B.1 이 발생시킨 패킷이고 그림 7 은 WBN B.2 가 발생시킨 패킷이다. 실제로 그림 6 의 패킷을 WBN B.2 가 무선 통신을 통해 수신하지는 못하였지만 유선 통신인 RS232 를 통해 수신하기 때문에 WBN B.2 에서 WBN B.1 로부터 수신한 패킷을 그림 7 과 같이 코디네이터로 라우팅하였다. 따라서 코디네이터는 그림 7 의 NWK Src. Address 필드 값 0x0002 를 참조하여 데이터의 진원지가 WBN B.1

임을 알 수 있었고 NWK payload 도 WBN 의 사용에 따른 변동없이 전송을 완료할 수 있었다.

5. 결론

본 논문에서는 USN 에서 전파적 또는 물리적 차폐로 인한 네트워크 단절 문제를 해결하기 위한 방법으로 유선 통신을 제안했다. WBN 는 Wired and Wireless MAC 을 포함하고 있어서 무선 통신과 유선 통신을 함께 지원하며 USN 프로토콜의 수정없이 분리된 네트워크 간의 통신을 제공하고 유선 통신에 대한 확장성을 제공한다. 최근 USN 프로토콜을 이용한 화재 및 방범 시스템, 위치인식 서비스 등과 같은 무선 센서네트워크 구축 사례가 많아지고 있는데 본 논문의 내용이 이들 산업 현장의 전파 장애 문제를 해결하는데 효과적으로 사용될 것을 기대한다.

향후 WBN 를 여러 네트워크 토폴로지와 라우팅 알고리즘에 대한 적용 가능성을 검토하고 그 성능을 평가할 예정이다.

참고문헌

- [1] Jo Woon Chong; Ho Young Hwang; Chang Yong Jung; Dan Keun Sung, "Analysis of Throughput and Energy Consumption in a ZigBee Network Under the Presence of Bluetooth Interference," *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, vol., no., pp.4749-4753, 26-30 Nov. 2007
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4411811&isnumber=4410910>
- [2] J. Zheng and M. J. Lee, "Will IEEE 802.15.4 make ubiquitous networking a reality?: A discussion on a potential low power, low bit rate standard," *IEEE Communication Mag.*, vol. 42, no. 6, pp. 140-146, June 2004.
- [3] J. S. Lee, "Performance evaluation of IEEE 802.14.3 for low-rate wireless personal area network," *IEEE Trans. Consumer Electron.*, vol. 52, no.3, Aug. 2006.
- [4] IEEE Standard for Information Technology Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4-2003.
- [5] ZigBee Alliance, ZigBee Specification Document 053474r13, Dec, 2006
- [6] Sikora, A.; Groza, V.F., "Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band," *Instrumentation and Measurement Technology Conference, 2005. IMTC 2005. Proceedings of the IEEE*, vol.3, no., pp.1786-1791, 16-19 May 2005
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1604479&isnumber=33712>
- [7] Chipcon, CC2430 Zigbee development kit – User Manual
- [8] Chipcon, General Packet Sniffer CC2430 IEEE 802.15.4 and ZigBee – User Manual
- [9] G. Ferrari, P. Medagliani, S. Di Piazza, and M. Martalò, "Wireless Sensor Networks: Performance Analysis in Indoor Scenarios," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, Article ID 81864, 14 pages, 2007. doi:10.1155/2007/81864