2007년도 대한전기학회 하계학술대회 논문집 2007. 7. 18 - 20

이종 제어 네트워크를 위한 암호화 지원 라우터의 설계 및 구현

허종만, 이감록, 권욱현
서울대학교 전기컴퓨터공학부 제어정보시스템연구실

Design and Implementation of Router Supporting Encryption for Heterogeneous Control Network

Jongman Heo, Kamrok Lee, Wook-Hyun Kwon
Control Information Systems Laboratory, School of Electrical Engineering & Computer Science, Seoul National University

Abstract - 본 논문에서는 다양한 이종 기기로 구성된 XCP 제어 네트워크를 위한 라우터를 설계하고 구현하는 방법에 대해 제안한다. XCP 네트워크에서는 통신 보안을 위한 패킷 암호화 방법이 사용되며, 동일 서브넷 내에서는 같은 암호화 키를 사용한 통신을 한다. 제안된 XCP 라우터는 이종의 기기로 구성된 XCP 서브넷 간의 통신을 지원하며, 암호화 기능을 사용하는 서브넷 간의 통신을 위하여 암호화 키를 변환해 주는 기능을 수행한다.

1. 서 론

eXtensive Control Protocol (XCP)은 네트워크 제어를 위해 제안된 새로운 제어 프로토콜이다[1]. XCP는 계층 및 패킷 기반의 규약이며 전력선 외에도 twisted pair, IrDA 및 무선(RF, IEEE 802.15.4) 등의 물리 계층을 지원할 수 있도록 설계되었다. XCP는 미리 정의된 규칙에 따라 한 기기로부터 다른 기기들로 정보를 전달하는 정보 지향 프로토콜이다. XCP는 빌딩/공장 자동화 및 홈 네트워킹, 자동 미터기 검침(AMR), 보안 센서 네트워크 등에 광범위하게 적용 가능한 유연성을 가지고 있다.

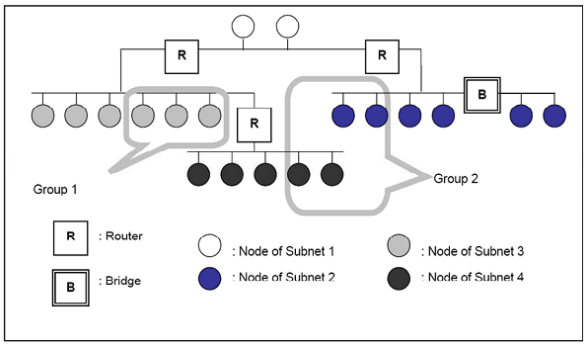
현재 XCP protocol에서는 같은 서브넷 (subnet) 내에서의 통신만이 고려되어 있을 뿐 다른 서브넷 간의 통신은 고려가 되어 있지 않다. 다른 서브넷 간의 통신은 domain broadcast일 경우만 지원을 하고 있다. 하지만 추후에 서브넷 간의 통신이 필요할 것이다. 예를 들어 아파트 관리실에서 긴급 상황이나 전력제한을 하려고 할 때 서브넷 간의 통신이 요구된다. 이에 대비하여 서브넷 간의 통신을 가능하게 하는 라우터의 필요성이 강조된다. 본 논문에서는 이종 기기들로 구성된 XCP 서브넷 간의 통신을 수행하는 XCP 라우터의 설계 및 구현에 대해 설명하고자 한다.

2. XCP 라우터 설계 및 구현

2.1 XCP 개요

XCP는 세션 계층 및 표현 계층을 제외하면 OSI 모델에 부합하도록 정의되었다. XCP는 물리 계층, 데이터 링크 계층, 네트워크 계층, 전송 계층, 응용 계층으로 분류가 가능하다. 물리 계층에서는 전력선, twisted pair, IrDA와 무선(RF, IEEE 802.15.4) 등의 여러 매체를 사용하는 것이 가능하도록 확장성을 제공한다. 데이터 링크 계층에서는 RTS/CTS 기반의 CSMA/CA 방법을 사용하여 충돌 확률을 줄인다. 또한 ARQ (automatic repeat request), CRC 등의 방법이 통신 안정성을 향상시키기 위해 채택되었다. 네트워크 계층에서는 기존의 flooding이나 shortest path 알고리즘을 상황에 따라 동적으로 적용하는 스마트 라우팅 기법을 사용하여 기존 라우팅 방법에 비해 개선된 성능을 제공한다. 전송 계층에서는 주어진 연결에 대해서 요구/응답 패킷을 처리하고 트랜잭션 제어 기능을 수행한다. 마지막 응용 계층에서는 여러 제조사 간의 기기가 상호 운용 가능하도록 네트워크 변수(network variable:NV)라는 개념을 정의하여 네트워크 변수가 갱신됨에 따라서 표준화된 변수의 값이 네트워크를 통해 교환된다. 따라서 기존과 같이 단순한 명령 패킷을 주고받는 것이 아닌, 사전에 연결(NV Binding)된 네트워크 변수 사이에 특정 이벤트가 발생함에 따라 네트워크 통신이 자연스럽게 이루어지게 된다.

그림 1은 XCP 네트워크의 구조를 보여주고 있다. 각 노드(node)는 XCP 프로토콜이 탑재된 기기 혹은 모뎀을 뜻하며, 서브넷 내에서 유일한 주소를 가지고 구별된다. 서브넷(subnet)은 같은 서브넷 주소와 암호화 키를 가지는 노드의 집합이다. 같은 서브넷 내의 노드들은 라우터 없이 서로 통신이 가능하며 최대 240개의 노드가 단일 서브넷을 구성할 수 있다[2]. 도메인(domain)은 라우터에 의해 연결된 서브넷의 집합으로 정의된다. 도메인 내에서 비슷한 기능을 수행하는 기기들의 논리적 집합은 그룹(group)으로 정의된다. 다른 서브넷 간 통신은 기본적으로 암호화(encryption)에 의해 차단되며, 암호화 방법으로는 128bit stream cipher가 사용된다. 따라서 악의적인 해킹으로부터 통신 보안을 유지할 수 있는 장점이 있다.

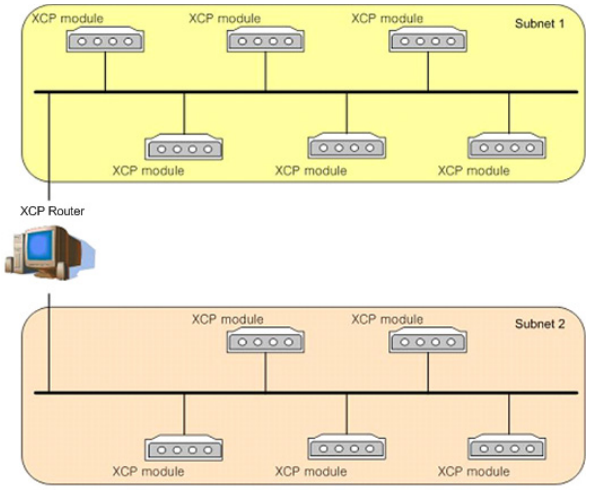


<그림 1> XCP 네트워크 구조

2.2 XCP 라우터의 설계

2.2.1 XCP 네트워크 구조

그림 2는 XCP 라우터를 통해 연결된 서브넷 1과 서브넷 2를 보여주고 있다. XCP 라우터를 통하여 서브넷 1에서 발생된 메시지를 서브넷 2로 전달해 주는 것이 가능하며, 반대의 경우도 가능하다. 각각의 서브넷 내의 XCP 기기들은 전력선, RF, IEEE 802.15.4 등의 다양한 이종 물리 매체를 사용하는 기기가 연결될 수 있다[3].



<그림 2> XCP 네트워크 구성도

2.2.2 XCP 라우터의 목적 및 기능

XCP 라우터는 다음과 같은 3가지 작업을 수행한다.

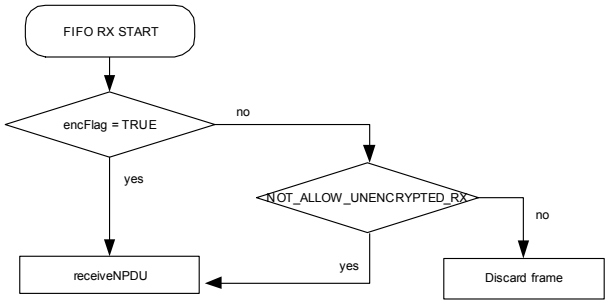
- 목적지 주소가 다른 서브넷인 경우의 패킷 전달
- 각 서브넷 라우팅 테이블 유지 및 갱신

● 암호화 키 변환

XCP 라우터는 이종의 서브넷 간의 통신을 지원해야 하며, 이를 위해 각 서브넷의 라우팅 테이블 정보를 유지하고 있어야 한다. 또한 암호화 기능이 활성화되어 있는 경우 서브넷 간의 통신을 위해 암호화 키를 변환해 주는 기능을 수행해야 한다. XCP 라우터를 사용하지 않는 경우의 서브넷 간 통신은 group multicast와 domain broadcast경우에만 허용이 되어 있다. 하지만 이 경우 암호화 기능이 활성화되어 있다면 아무리 group multicast와 domain broadcast 통신을 한다고 하더라도 패킷을 받는 다른 쪽 서브넷의 노드는 받은 패킷을 해석하지 못할 것이다. 반면 XCP 라우터를 통해 서브넷 간의 통신을 처리할 경우 XCP 라우터가 서브넷 1의 암호화 키를 서브넷 2의 암호화 키로 바꾸어서 전송을 하기 때문에 XCP 라우터를 사용하지 않았을 경우처럼 수신하는 노드가 받은 패킷을 알아보지 못하는 경우를 막고 원활한 통신을 하게 한다.

2.3 XCP 라우터의 구현

XCP 라우터의 내부 스케줄러는 다른 일반 XCP 기기와 비슷하다. 하지만 XCP 라우터의 기능상 자체 송신 패킷이 없기 때문에 상위 계층으로부터의 패킷 여부를 검사하는 UART Rx FIFO 처리 부분은 불필요하다. 따라서 이에 관련된 함수를 호출하는 부분이 생략이 되어 있다. 그 외의 부분은 일반 노드와 거의 동일하다.



<그림 3> FIFO RX 함수 동작 순서도

그림 3은 패킷 수신시에 호출되는 FIFO RX 함수의 과정을 간략화한 것이다. 만약 패킷의 네트워크 헤더 중 암호화 옵션 플래그가 true이면 receiveNPDU 함수를 호출하여 받은 패킷을 검토하지만 그렇지 않으면 받은 패킷을 무시해 버린다. 만약 암호화 옵션 플래그가 false이더라도 NOT_ALLOW_UNENCRYPTED_RX 기능을 지원한다면 마찬가지로 receiveNPDU 함수를 호출하여 받은 패킷을 검토한다.

암호화 옵션 검사를 거친 후, 실제 receiveNPDU 함수에서는 addressRecognition() 함수를 통해 해당 패킷이 어떤 목적지 서브넷을 가지고 있는지 판별한다. XCP 라우터는 연결된 모든 서브넷 간의 통신을 처리할 수 있어야 하므로, 각 서브넷의 암호화 키를 가지고 있어야 한다. 이는 XCP 라우터 설정 프로그램을 통해 설정 가능하다. 패킷의 목적지 서브넷을 판별한 후, XCP 패킷의 통신 종류에 따라 패킷을 적절하게 처리한다. 라우팅 테이블 갱신 패킷을 수신한 경우에는 XCP 라우터가 가지고 있는 해당 서브넷의 라우팅 테이블을 갱신하게 되며, 일반 패킷의 경우에는 목적 주소의 서브넷에 따라 패킷을 적절히 전달하게 된다.

XCP 라우터가 받은 메시지를 다른 subnet의 노드로 보내는 Transform_Subnet()라는 함수의 경우 패킷 종류가 unicast이거나 multicast response인 경우는 다음과 같이 처리한다. 스마트 라우팅 전송 방법을 사용한다면 findNextPath() 함수의 응답 주소 값으로 subnet broadcast를 하거나 path info를 삭제를 하거나 next node의 주소로 패킷을 보내도록 목적지 주소를 세팅한다. 동일한 패킷 종류에 대해 flooding 전송 방법을 사용한다면 목적지 주소를 서브넷 broadcast 주소로 설정한다. 마지막으로 경로 재설정 flooding 전송 방법을 사용하는 패킷이라면 해당 경로 정보를 삭제를 한다. Transform_Subnet() 함수에서 패킷 종류가 unicast나 multicast response가 아닌 경우에는 목적지 주소를 서브넷 broadcast 주소로 세팅을 한다. 위와 같은 과정을 거쳐 수정된 패킷을 목적지 서브넷으로 전송할 수 있다.

일반 데이터 패킷이 아닌 라우팅 테이블 갱신 패킷을 수신하게 된다면 XCP 라우터는 해당 서브넷에 대한 라우팅 테이블 갱신을 하여야 한다. 이는 다른 서브넷의 노드를 목적지 주소로 가진 패킷이 도착하는 경우, 유효한 경로를 찾기 위한 라우팅 테이블을 유지하고 있어야 하기 때문이다. 라우팅 테이블 갱신 방법은 기존의 XCP 노드 각각이 수행하는 방법과 유사하다. 다만 XCP 라우터는 서브넷 간의 통신을 지원하여야 하기 때문에 연결된 서브넷 전체의 라우팅 테이블을 유지하고 있다는 점이 다르다.

3. 결 론

XCP는 여러 산업분야에서 광범위하게 사용가능한 네트워크 제어 시스템을 위하여 제안된 통신 프로토콜이다. 빌딩/공장/홈/센서 네트워크 등에 적용가능하며 다양한 유무선 기기로 구성된 이종 제어 네트워크를 지원할 수 있다. 본 논문에서는 XCP 제어 네트워크를 위한 라우터를 설계하고 구현하는 방법에 대해 제안하였다. 제안된 XCP 라우터를 사용하면 보다 큰 규모의 제어 네트워크를 구성하는 일이 가능하며, 다양한 응용 분야에 적용 가능한 장점이 있다.

[참 고 문 헌]

[1] J. M. Heo, H. K. Kang, W. Y. Kim, and W. H. Kwon, “Design and implementation of XCP network system,” in *Proceedings of the International Conference on Control Automation and Systems, ICCAS 2005*, pp. 1581-1585, June 2005

[2] H. K. Kang, Kamrok Lee, Jong-Man Heo, Wook-Hyun Kwon, Hong-Seong Park, and Beon-Jin Chung, “Adaptive Channel State Routing Algorithm for Power line communication”, *IEEE ISPLC 2006*, pp. 166-171, Mar. 2006.

[3] J. Y. Ha et al, ″Design and Implementation of Convergence sub-layer for a Heterogeneous Home Network,″ *IEEE ISPLC 2007,* pp. 252 - 256, Mar. 2007