IP 기반의 공정 제어 네트워크에서의 통신 장애 진단

원영준[1], 최미정[1], 김명섭[4], 노홍선[2], 이준협[2], 황화원[3], 홍원기[1]

[1]포항공과대학교 컴퓨터공학과

[2]포스코 전기제어 설비부

[3]포스코 기술연구소

[4]고려대학교 컴퓨터정보학과

[1]{yjwon, mjchoi, jwkhong}@postech.ac.kr, [2]{vishnu4, mujigae}@posco.co.kr,

[3]hwawon@posco.co.kr, [4]tmskim@korea.ac.kr

요 약

IP를 기반으로 하는 공정 제어 네트워크는 공정 프로세스와 제어되는 장비간의 통신을 지원한다. 공정 제어 네트워크에서 발생하는 통신 장애는 정확한 시간 별 이벤트에 영향을 받는 공정 프로세스의 지연을 발생시키기도 하며, 심지어 전체 공정의 중단을 초래하기도 한다. 현재 발생하는 통신장애의 대처는 수동적이며, 단순 반복적인 경험에 치우친 갓대로 장애를 판단하여 처리하고 있다. 이는 장애 발생후의 사후 처리이므로 공정에 차질을 유발하며 경험에 의한 단순 장애 대처 방법은 비효율적일 수 밖에 없다. 따라서 능동적 대처 방안이 필요하다. 본 연구의 목표는 추후 장애 판단 및 처리의 수준을 벗어나 통신 장애 발생 이전에 네트워크 상황의 빠른 판단 요건을 추출하여, 통신 장애를 사전 감지하는 것이다. 이를 위해 실제 공정 제어 네트워크 장애 사례를 수집 및 분류하였다. 또한 장애의 원인과 관련된 네트워크 측정 항목을 제시하고, 항목 별 사전 징후 요건들을 정의한다. 이를 바탕으로 공정 제어 네트워크 진단 시스템을 개발하고자 한다.

1. 개요

공정 제어 네트워크는 제어 기기 또는 제조공정 기기들간의 통신을 제공하는 네트워크이다. 제어 네트워크는 다음과 같이 Building Automation (BA), Factory Automation (FA), 그리고 Process Automation (PA)로 나뉘어 볼 수 있다[1]. 각각의 제어 네트워크는 서로 상이한 목적을 가지고 있으나, mission-critical 한 작업을 위해 안정적 통신을 보장해야 한다는 공통점을 가지고 있다. 그에 따라, 최소한의 통신 지연시간과 기기간 필수 메시지 전송 보장은 제어 네트워크 상에 존재하는 모든 통신 세션의 중요한 품질(QoS)의 관측요소이다. 기존의 제어 네트워크 기술은 (예: FOUNDATION Fieldbus [3], PROFIBUS [4], MODBUS [5], BACnet [6], Lon Works [7] 등) Ethernet 과 IP기반 기술과는 독립적으로 발전되어 왔다. 최근에 들어 이러한 기술들은 상대적으로 저렴한 비용, 높은 확장성, 그리고 용이한 유지/보수의 장점을 가지고 있는 Ethernet 과 IP 기술을 바탕으로 한 발전 방향을 모색하고 있다. 관련 연구에서도 IP 기반의 제어 네트워크 발전에 있어 기술적 이슈들을 명시하고 있다[1]. 위에서 언급된 IP 기반의 장점과 IP 기반으로의 이동에 있어 기술적 부분 문제 해결이 비교적 용이함에 불구하고, 대부분의 제조 공정 환경에서 IP기반의 네트워크 도입 결정을 섣불리 내리지 못하고 있다. 이는 기술적인 이유보다도, 대규모 투자결정을 동반하는 네트워크 도입이 예상되기 때문이다. 기존의 네트워크를 구성하던 하위레벨의 많은 제어 기기 (예: 센서, 모터 등) 들도 모두 IP 화가 이루어져야 하는 문제점을 가지고 있다.

본 연구에서는 포스코의 철강 제조 공정 네트워크를 조사하고, 실제 공정 망에서 발생하는 통신장애 탐지를 위한 시스템에 대한 연구를 목표로 한다. 포스코의 네트워크는 크게 일반 사무 네트워크와 공정 네트워크로 나뉘어 진다. 일반 사무 네트워크는 기존의 IP 기반의 데이터 네트워크와 동일한 반면 공정 네트워크는 IP기반과 비IP기반 제어네트워크 기술이 공존하는 형태로 운용되고 있다[1][2]. 현재 포항지역에만 약 30개 이상의 제조 공정 네트워크를 가지고 있으며,

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA - 2006 - (C1090 - 0603 - 0045))

각각의 공정 과정에 필요에 따라 순차적 또는 병렬적 구조를 가지고 있다.

본 연구를 위하여, 포항지역 공정 중 기존에 크고 작은 네트워크 장애 사례를 겪었거나 또는 불안전한 통신 형태를 띄우고 있는 몇 개 공정을 선택하였다. 선택된 공정 제어 네트워크의 장애 케이스를 선별, 정리하여 네트워크 운용 QA&M 요소를 고려한 원격 네트워크 장애 진단 시스템을 제안하고자 한다. 본 연구에서 제안되는 시스템은 IP 기반의 제어 네트워크에 특화된 시스템이며, 이는 기존의 일반 IP 네트워크의 진단 장비를 대체하는 효과를 가지게 된다.

본 논문은 다음과 같은 순서로 구성되어 있다. 2장에서는 공정 제어 네트워크의 개략적인 내용과 연구 동기를 서술하고 있다. 3장에서는 통신 장애 케이스들과 케이스 별로 측정 가능한 요소들을 파악한다. 4장에서는 제어 네트워크 진단 시스템과 장애 요소들의 분석 방법을 제시한다. 마지막으로 결론과 향후 연구에 대하여 서술한다.

2. 공정 제어 네트워크 개요

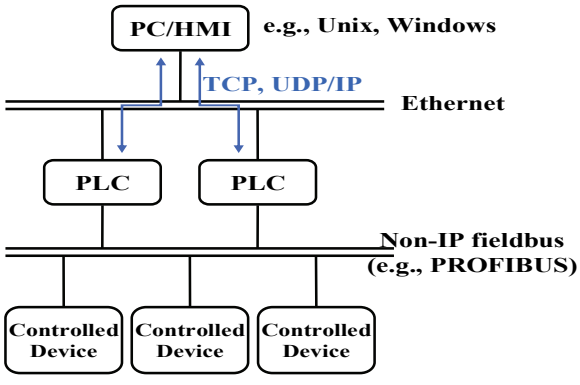
본 장에서는 제어 네트워크를 구성하고 있는 네트워크 요소들과 각각의 역할에 대하여 설명한다. 또한 실제 필드에서의 모니터링 요구사항을 바탕으로 한 연구 동기에 관한 설명을 포함한다.

2.1 제어 네트워크 구성 요소

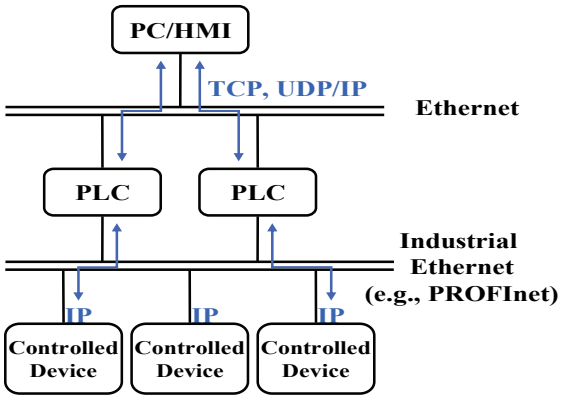
대표적인 공정 제어 네트워크는 그림 1 (a) 와 같은 형태를 가지고 있다. 공정 제어 네트워크 구성요소는 계층 모델을 따르고 있다. 가장 상위 레벨에는 전체 제어를 담당하는 하나 또는 그 이상의 장비로 구성되어 있으며, 전체 제어 장비를 통하여 순차적, 병렬적 공정 구조망을 제어하게 된다. 다음과 같은 네트워크 구성요소를 가지고 있다.

- Programmable Logic Controller (PLC) – 본 요소는 마이크로 프로세서 컴퓨터로 연속성을 보장해야 하는 복잡한 제어 네트워크 환경에 이용된다. Custom-built 제어 소프트웨어가 장착되어 이용되며, 본 연구에서 모니터링 되는 PLC 장비는 Ethernet (RJ-45, 광) 그리고 PROFIBUS (EIA-485)의 두 가지 통신 인터페이스를 장착하고 있다.
- Process Controller/Human Machine Interface (PC/HMI) – 본 요소는 PLC 제조사로부터 제공되는 소프트웨어 및 하드웨어 패키지의 일부이다. PLC에 원격 접근 가능한 UNIX 또는 Windows 플랫폼의 애플리케이션 소프트웨어 패키지로 구성되어 있다. 필요에 따라 Custom-built 된 서버 애플리케이션도 PC에 장착이 가능하며, GUI 환경을 통하여 실시간 공정 모니터링에 이용된다. PLC와의 통신은 TCP/IP 를 기반으로 한다.
- 제어기기(controlled device) – 본 요소는 계층 모델 구조에서 가장 하위 레벨에 위치하는 센서, actuator, 모터등의 장비를 명칭한다. 주로 임베디드된 통신 인터페이스를 장착하고 있으며, PLC로부터 명령 시그널을 PROFITBUS 인터페이스를 통해 수신하여 동작하게 된다
- 라우터/스위치 – 레이어 2, 3 환경의 스위칭 기기들은 위의 세가지 제어 네트워크 구성 요소들간의 통신을 연결, 관장한다. 이는 PC 와 PLC 사이 또는 전 구간 IP 환경일 경우, PLC 와 제어 기기간에도 통신을 관장하는 역할을 한다.

그림 1 (b)는 전 구간이 IP 기반 제어 네트워크로 변환된 환경 구조를 보여주고 있다. PLC 와 제어기기는 Industrial Ethernet과 IP 기반으로 통신이 이루어지게 된다. 이러한 구조를 도입하기 위해서는 수많은 하위 레벨 제어기기들에 할당될 추가 IP주소가 필요하며, 또한 모든 PLC의 재 프로그래밍 작업이 요구된다. 이 작업은 많은 투자비용과 전반적인 네트워크 변경을 요구하게 때문에 대부분의 산업계에서는 전 구간 IP 도입에 있어, 현재 쉽게 결정을 내리지 못하고 있는 실정이다. 본 논문에서는 현재 공정 제어 네트워크가 따르고 있는 구조인 그림 1 (a) 형태 네트워크의 장애 진단을 중점으로 하고 있다.



(a) Typical Control Networks



(b) All IP-based Control Networks

그림 1. 제어 네트워크 구성도

2.2 연구 동기

공정 제어 네트워크상의 통신 장애는 매우 큰 문제를 일으킬 수 있다. 대부분의 제어기기와 네트워크 구성요소들이 동기화된 상태에서 작동하는 환경에서, 단 한번의 통신 장애가 전체 공정의 지연과 최악의 경우 공정 중단과 같은 사태를 일으킬 수 있다. 공정 중단과 같은 상황은 경제적 손실과 직결되어 있으며, 이는 일반적인 IP 데이터 네트워크 (예; 인터넷)와는 달리 장애에 더욱 민감한 IP 네트워크임을 알 수 있다. 예를 들어, 철강 제조망은 각 공정 별 시간의 흐름과 연속적인 제조 흐름이 최종 제품의 도출에 큰 영향을 미치고 있다. 이러한 환경에서 네트워크 관리자의 통신 장애 징후의 사전 탐지 및 장애 발생 이전의 사전 차단 조치는 매우 중요한 요구사항으로 부각되고 있다.

공정 제어 네트워크를 모니터링 구간의 관점에서 보면, PC와 PLC 네트워크, 그리고 PLC와 제어기기간의 네트워크의 두 가지 구간으로 나누어 볼 수 있다. 이 두 구간의 연동이 이루어지고는 있으나, 각각 서로 다른 physical media, 통신 프로토콜로 구성되어 있다. 본 연구에서는 Ethernet 과 IP 기반의 도입이 이루어진 첫 번째 PLC 와 PC 구간의 트래픽에서 탐지 가능한 통신 장애 유형에 주목한다. 기존의 IP 네트워크의 진단을 위한 도구들 (예: Sniffer, Wireshark)은 존재하나, 공정 제어 네트워크 상에서 발생하는 장애 탐지에 이 도구들을 적용하는 것에는 한계를 드러내고 있다.

이는 발생하는 트래픽 유형에 차이가 있어, 일반 IP 네트워크 통신 장애 개념에는 속하지 않는 특화된 장애 유형이 존재 하기 때문이다. 이처럼 특화되고 명확하지 못한 장애 유형 때문에, 네트워크 관리자들은 기존 진단 도구들에 의존한 사전 탐지는 현재까지 거의 불가능하였으며, 실사용자의 통신 장애 신고 접수 후에야 트래픽 수집을 통한 장애 요인 분석을 수행하고 있다. 이는 문제가 되는 시점의 트래픽을 수집할 수 없으므로, 정확한 원인 분석 또한 불가능하게 하는 문제점도 가지고 있다. 그리고 기존의 도구는 on-site 모니터링만이 가능한 구조로 되어 있어, 장애가 발생한 site에 매번 직접 설치해야 하는 번거로움이 따른다. 본 연구에서는 원격 접속과, 다수의 probe를 지원하는 모니터링 구조를 도입하여, 통신 장애의 사전 징후 시점에 발생 가능한 장애의 종류와 원인을 관리자에게 최단시간 내에 통보하는 시스템의 필요성을 검토하였다.

3. 통신 장애 탐지 및 진단

본 장에서는 공정 제어 네트워크의 실제 장애 사례를 나열하였다. 사전에 발생했던 장애 사례의 분석을 통하여, 네트워크 장애별 분류를 실시하였으며, 사전 장애 징후 탐지를 위한 측정요소와 각각의 장애 발생 요건을 제시하였다.

3.1 장애 사례 및 분류

이 장에서 제시되는 통신 장애의 원인은 장애 발생 이후 사후 조치를 행하는 시점에서 해당 장비 로그 분석과 더불어 네트워크 관리자의 직관을 통한 일차적 원인 분석을 바탕으로 작성되었다.

- Ethernet duplex mismatch [9] – Ethernet 장비간에 자동 구성 (auto-configuration) 이 설정되어 있는 환경에서, 통신 방식 (half 또는 full duplex)의 설정에서 문제가 발생하는 경우이다. 이러한 통신 방식의 불일치는 프레임의 손실 및 충돌 횟수를 증가시키고, 종단간에 급작스런 통신 지연의 현상으로 나타난다. 일반적인 IP데이터 네트워크를 구성하는 레이어 2/3 스위치와 Ethernet 인터페이스간에는 이러한 문제가 거의 발생하지 않고, 발생하여도 고용량의 데이터 전송을 제외하고는 종단에서 쉽게 문제점을 인지하기 힘들다. 그러나 PLC에 장착된 대부분의 임베디드 Ethernet 인터페이스는 상대적으로 불안정하고 업그레이드가 용이하지 못하여 자동 구성이 원활하지 않은 상황이 발생한다. 현재 이러한 문제를 극복하기 위해서는 자동 구성 기능을 사용하지 않고, 메뉴얼하게 각각의 장비간의 구성을 지정하는 것이 유일한 방법이나, 이는 현실적으로 힘든 상황이다.
- PLC 프로그램 장애 – 네트워크 프로그래밍에 대한 깊은 이해가 부족한 시스템 엔지니어들에 의하여 PLC 장비에서 동작하는 프로그램이 디자인, 구현되어 통신 장애를 일으키는 경우이다. 뿐만 아니라 PLC 장비에 porting시 사용되는 네트워크 관련 API 등의 버전별 변화도 기존의 시스템과의 충돌 등의 문제를 일으킨다. 실제로 불필요하거나 용도가 불분명한 패킷의 생성 (예: 비정기적인 keep-alive 패킷의 전송), 비 순차적인 패킷 시퀀스, 그리고 비 정상적인 TCP 윈도우 크기 등이 본 문제점을 반영하고 있다.
- 기기 통신 드라이버 장애 – 서로 다른 메이커의 PLC, 제어 기기등의 통신 인터페이스 드라이버에서 호환성의 문제가 발생한다. 또한 드라이버의 안정성은 연속적인 공정에 중요한 요소이다. 예를 들어, 가용 대역폭을 벗어난 시그널이 장비에 전달되었을 때, 장비의 비정상적 종료를 발생시키기도 한다. 그러나 장비 드라이버의 수정은 불가능한 경우가 대부분이며, 문제 발생시 새로운 장비로의 교체를 최우선으로 하는 미봉책이 많이 쓰인다.
- 링크 장애 – 통신 케이블의 물리적 손상을 가리킨다. 본 문제는 넓은 구간과 상대적으로 불리한 환경에 설치되어 있는 (예: 온도,

습기) 공정 망에서 잦은 빈도를 보이고 있다. 이러한 물리적 손상 자체를 탐지하는 것은 네트워크 패시브 모니터링 기법을 통해서는 무리가 있으며, 몇몇 측정치를 바탕으로 한 종합적인 추측만이 가능하다. 참고 가능한 측정치는 비정상적 크기의 프레임 발생, 프레임 충돌 빈도수 증가, CRC 값의 에러, throughput 값의 급작스런 변화 등을 들 수 있다. 본 장애의 경우 어느 특정한 측정값의 변화 보다는 하나 이상의 복합적인 이상 징후 값을 나타낸다.

- Protocol unawareness – PLC, 제어기기 등에서 알맞은 decoding이 불가능한 프로토콜의 트래픽이 전달될 경우 해당 기기에 장애를 유발한다. 지원되지 않는 프로토콜 트래픽을 사전에 차단하는 것이 권고사항이나, 이를 완벽히 차단하는 것은 힘들다. 실례로 Simple Network Management Protocol (SNMP) 트래픽이 오래된 PLC 장비로 유입된 경우, 해당 장비의 오작동을 초래하였으며, 시스템 재 가동 등의 사후 조치 과정을 통하여 복구하였다.
- 패킷 overflooding – PLC 장비와 제어 기기간에 필요한 최소 대역폭이 비정상 트래픽에 의하여 확보되지 못하여, 공정의 장애를 초래하였다. ARP storm 등이 실례로 잦은 발생 빈도를 보였으며, 취약점이 노출된 OS 시스템의 제어 네트워크 내 설치를 최대한 자제하고 있다.
- Electrical noise – 동축 케이블에 시그널 방해를 일으켜 불안정한 통신 상태를 보이는 것을 가리킨다. 고전력 장비 주변에 설치된 통신 케이블에서 잦은 빈도수를 보이며, 공정 네트워크에서 케이블 및 제어기기 배치시에 주의가 요구된다.
- Power outage – 전력공급 장비에 문제가 발생하는 경우를 가리킨다. 이중화 구조로 대비하고 있으며, 공정 네트워크에서 잦은 빈도수를 보인다.
- Misconfiguration – 트래픽이 최적의 경로로 전달되지 못하고, 잘못된 라우팅 테이블 또는 스위치 구성으로 인하여 불필요한 loop을 거치는 등의 문제를 가리킨다. 일반적으로 종단간의 통신 지연, 메시지 손실 등으로 나타난다. 비정상적인 재전송 패킷양의 증가시 의심해 봐야 하는 장애 형태이다.
- 라우터/스위치 인터페이스 장애 – 인터페이스의 하드웨어 장애로 인한 통신 장애를 가리킨다. 대부분 통신 두절을 동반함으로 종단간에서는 빠른 탐지가 가능하나 패시브 모니터링 기법을 통한 발견에는 어려움이 있다.

위와 같이 실제 공정 망에서 발생되었던 통신 장애 케이스를 바탕으로, 본 논문에서는 표 I 에서와 같이 제어 네트워크 장애의 개념적 분류를 하였다. 제시된 장애의 종류는 IP 기반의 네트워크에서 발생 가능한 장애의 범주 안에 속하지만, 장애로써 인식되는 기준에 민감한 차이를 갖고 있다. IP 단의 연결 에러 (IP connectivity errors) 는 주관적인 판단을 바탕으로 한 통신의 불안정성, 비 정상적으로 낮은 전송률, 네트워크 취약점 공격 등에서 나타날 수 있는 장애 형태 이다. 두 번째 항목은 네트워크 비정상적 설정 (network misconfiguration)에 속하는 언급되었던 바와 같은 패킷의 네트워크 내에서 비효율적인 경로로 전달, 전송 타입의 불 일치 등의 장애 형태를 가리킨다. 세 번째는 모든 하드웨어적 또는 물리적 장애 (physical defects) 이며 위에서 언급되었던 통신 기기자체의 장애, 전력공급의 불안정성 등과, 하드웨어 주소의 충돌 등의 장애로 나뉘어 볼 수 있다. 마지막 항목인 소프트웨어 결점 (software defect)은 네트워크 구성요소의 (예: PLC vs. 일반 컴퓨터) 차이로 인해 나타나는 제어 네트워크에 특화된 장애 유형이다. 기존에 IP 데이터 네트워크 성능 측정 시에 간과하고 주의를 기울이지 않았던 측정항목들을 새롭게 재조명해 볼 필요성을 갖고 있다.

표 I. 공정 제어네트워크 장애의 개념적 분류

Types	Details
IP connectivity errors	Unstable transmission, Low throughput, delay, network security threat, IP resource management, and more
Network misconfiguration	Network topology loop, Non-optimal path (redundancy), Duplex mismatch, and more
Physical defects	Hardware malfunction, Link corruption (cable damage), Electrical noise, Power outage, Duplicate hardware addresses, and more
Software defects	PLC programming bugs, Device driver bugs, Protocol unawareness, and more

3.2 장애 초기 증상

공정 제어 네트워크의 안정적 운용을 위하여 사전 장애 징후 탐지는 중요한 역할을 한다. 표 II 는 본 연구에서 제시하는 공정 제어 네트워크에서 발생 가능한 통신 이상 징후를 반영하는 측정 항목(Network Metrics) 과 각 항목별 사전 징후 조건 (Alarm conditions)을 명시하고 있다. IP 네트워크의 모니터링 측면에서 볼 때 특이하거나, 전혀 새로운 측정항목은 제시되지 않았으나, 본 항목들은 기존의 IP 네트워크 측정 툴들에서도 측정가능 했으나, 심도있는 분석을 통한 장애 유형에 도출에는 이용되지 못했던 항목으로 이루어져 있다. 이로 인해 Sniffer 와 같은 네트워크 진단 툴은

제어 네트워크에서는 신뢰 있는 진단 결과를 나타내지 못하고, 정확하지 못한 장애를 report 하는 결과를 낳고 있다. 이는 3.1 장에서 언급되었던 것과 같이, 제어 네트워크 장애 유형의 특수성을 인식하지 못하는 것에서 발생하는 미흡한 점이다. 기존의 측정항목 재발견과 더불어 장애 기준의 수립이 필요하고, 본 표에서 제시된 항목 별로 패시브 모니터링 방법을 이용, 네트워크에서는 직접적 영향을 미치지 않고 측정치를 실시간으로 수집, 장애 예고에 판단 요건으로 사용된다.

표 II. 제어 네트워크에 특화된 측정 항목과 항목별 사전 징후 조건

Index	Network Metrics	Alarm Conditions
1	Collision frames	First appearance, or threshold-based
2	Jumbo (>= 1514 bytes) frames	First appearance
3	Runts (<= 64 bytes) frames	First appearance
4	CRC error frames	First appearance
5	IP/TCP checksum errors	First appearance
6	Fragment packets	Threshold-based
7	Retransmission packets	First appearance, or threshold-based
8	Packet inter-arrival time (ms)	Increase to the previous value
9	Throughput (bps)	Decrease, drop to 0, or pattern analysis over monitoring period
10	Packets per second (or packet burst)	Increase, decrease, drop to 0, or pattern analysis over monitoring period
11	Min/max/diff packet size (bytes)	Change in difference of max and min sizes over monitoring period
12	Min/max/diff TCP window size	Drop to 0, change in difference of max and min sizes over monitoring period
13	Out-of-order sequence packets	First appearance
14	Broadcast packets	Threshold-based
15	Unsupported protocol packets	Threshold-based

본 연구에서 제시하는 측정항목은 플로우 별 측정값을 나타낸다. 플로우란 동일한 소스, 데스티네이션 MAC 주소, IP 주소, 포트 정보, 그리고 프로토콜을 공유하는 연속적 단방향 패킷의 흐름을 가리킨다. 표 II 의 사전 징후 조건의 'First appearance'는 해당 측정값이 증가하였을 때, 측정치의 증가 폭이 단 한번이라도 증가하였다면 통신 장애의 가능성을 높게 보는 측정항목을 나타내고 있다. 그 외 몇몇 사전 징후 조건은 사용자에 의해 네트워크 별로 정의된 threshold를 기반으로 동작하게 된다 ('Threshold-based' 로 표기).

8-12번 측정항목은 IP 데이터 네트워크의 트래픽 유형과는 차별되는 조건을 가지고 있다. 24시간 동일 작업이 반복되는 공정 망의 특성상, PC 와 PLC 사이에는 시간대별 통신 패킷 량 및 패킷 전달 주기의 변화가 거의 없는 트래픽 유형을 띄고 있다. 또한 command & action trigger형식으로 작동하는 기기제어는 매우 작은 통신 대역폭을 가지고 있다. 이러한 측정항목들은 크고 작은 미세한 변화 량의 감지를 통해서 사전 장애 징후를 판단하게 된다. 본 연구에서의 패턴 분석 (pattern analysis) 이란, 패킷의 stream 에서 특정 모니터링 윈도우 사이즈 (패킷 수) w를 지정하여, 다음 시퀀스의 패킷을 w 만큼 shift 시키면서 플로우 별 packets per second (PPS), 패킷 바이트, 그리고 inter-arrival 시간의 평균치, standard deviation값 등을 지속적으로 기록하여 패턴을 표현한다. 각 윈도우 별로 기록된 값들이, 다음 최근 시간 윈도우에서 계산된 값에 대비 difference ratio 가 일정부분 증가/감소 하였다면 사진 징후의 요건으로 본다.

단 하나의 특정 측정 항목의 변화치가 장애 사전 징후 요건을 나타내는 경우는 흔치 않다. 하나의 장애 사례가 동시에 여러 측정항목의 변화를 가지고 오게 된다. 예를 들어, 에러 프레임 또는 out-of-order 시퀀스 패킷의 전달은 재전송 프레임의 발생을 가지고 오게 될 것이며, 이는 동시에 세 가지 (에러 프레임, 재 전송 패킷, out-of-order 패킷) 측정항목의 사전 징후 탐지 요건의 충족을 시킴을 알 수 있다.

4. 공정 네트워크를 위한 장애 진단 시스템

본 장에서는 제어 네트워크를 위한 장애 탐지 및 진단 시스템의 설계를 설명한다. 또한 장애 공지와 실제 통신 비정상 원인간의 상관관계 비교의 개념을 제시한다.

4.1 시스템 구조

본 연구에서 제안하는 시스템은 장애의 사전 징후 탐지와 탐지 시스템의 원격 접근성 이렇게 두 가지 기능을 기본으로 설계되었다. 그림 2 (a) 에서는 전체 시스템 디자인을 나타내고 있다. 하나 이상의 모니터링 probe, collector (DB 서버), presenter (웹 인터페이스) 요소들로 구성되어 있다. 그림 2 (b) 의 개념적인 모델과 같이 다수의 세그먼트 모니터링을 위한 분산 구조는 중앙 집중 데이터 표현의 특성을 가지고 있다 [10]. 이는 통합관제의 요건을 충족하기 위한 구조이며, operation cost 가 큰 probe 의 역할을 모니터링 데이터의 수집과 전달 목적에만 국한시키기 위한 방법이다. 모니터링 링크의 데이터 용량에 따라 하나의 시스템에서 세 가지 구성요소의 동시 구현도 가능하며, 이를 통해

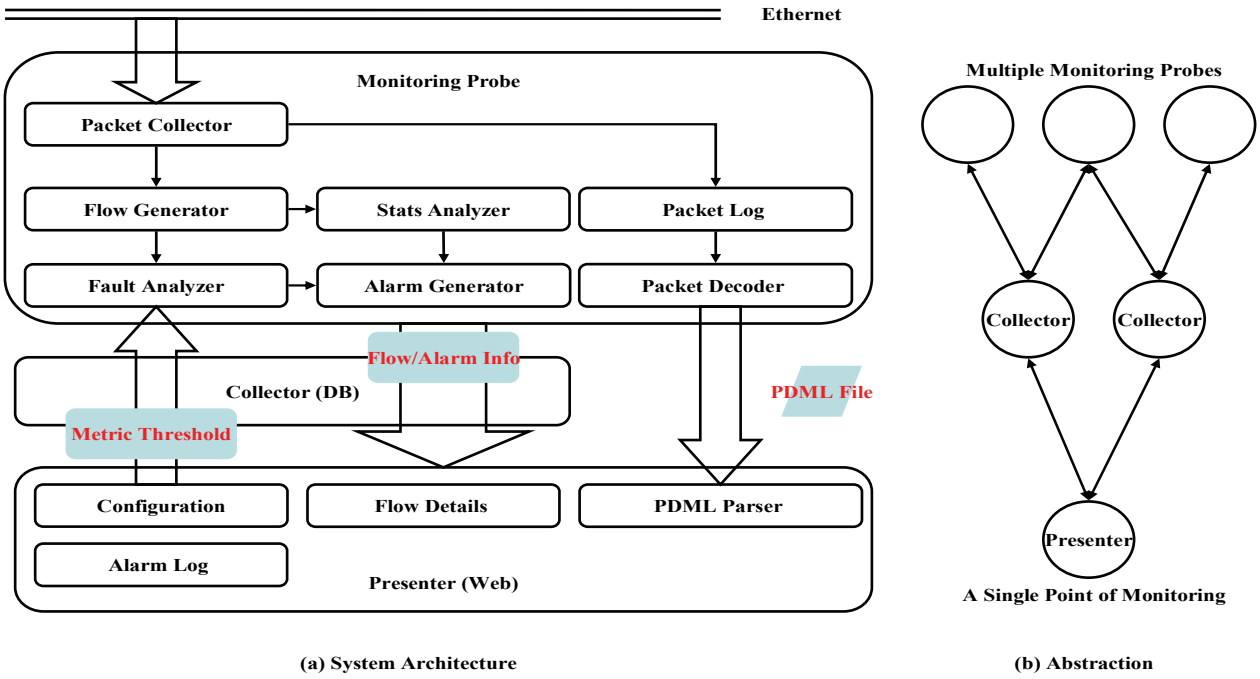


그림 2. 제어 네트워크 진단 시스템

실제 적용 시에 유연성을 보장한다.

모니터링 probe는 링크의 트래픽을 수집하며, presenter와 TCP/IP 기반의 통신을 하도록 설계되었다. 패킷 정보는 포트 미러링 또는 passive network tap을 통하여 probe에 전달 되며, Packet collector 모듈에서 시스템에서 확인된 패킷을 수집 Flow generator와 Packet Log 모듈로 전달된다. Fault analyzer 는 3.2 장에서 제시된 측정항목 플로우별로 분석한다. 분석 도중 현재 정의된 장애 사전 징후 조건을 충족시키는 경우, 해당 플로우 정보는 실시간으로 네트워크 관리자에 e-mail 또는 text-message로 전달된다. 주기적인 (예: 20초 주기) 전체 플로우 정보 및 장애 징후 정보는 collector 모듈로 송신되며, collector는 다수의 probe로 수신되는 플로우 정보의 cross-match를 실시하여, 동일 플로우에 대한 aggregation 작업을 실행한다.

Packet log 모듈에서 주기적 (예: 60초 주기)으로 저장되는 바이너리 패킷 형태는 필요한 경우in-depth 한 off-line 분석을 위한 목적이다. 공정 제어 네트워크의 낮은 대역폭은 (예: 공정 가동시 최대 10Mbps 이하) 실시간 full-payload 패킷 저장을 가능하게 하는 probe 시스템에서 허용 가능한 I/O overhead 범위 내에 존재한다. 모니터링 probe와 presenter 사이에 직접적인 통신은 Packet decoder의 결과물 공유를 위하여 이루어진다. 네트워크 관리자로부터 특정 시간대 패킷 데이터에 대한 분석요구가 있을 경우, Packet decoder는 바이너리 형태의 패킷을 Packet Details Markup Language (PDML)[8] 형태로 변형한다. PDML은 XML과 동일한 pre-define된 tag로 패킷 데이터의 레이어 별 정보를 표현하고 있다. Ethereal 과 흡사한 형태의 패킷 디코딩 정보를 원격으로 확인 가능한 환경을 구축한다.

마지막으로 네트워크 관리자는 발생한 사전 징후 현상에 실제 원인에 대한 설명을 추가할 수 있다. 본 연구에서 제시하는 사전 징후는 실제 장애 원인에 대한 제시가 아니며, 경험을 바탕으로 한 원인 분석이 동반되어야 한다. 이러한 로그 기록을 바탕으로 하여, 제시된 측정 항목과 기존에 알려진 장애 요인간의 실질적 mapping이 가능하며, 각 측정항목간 correlation 분석의 바탕을 제공한다.

4.2 장애 요인 분석 방법

그림 3 에서는 장애 요인 파악에 기초가 되는 추론 기법 (Inference engine)과 그를 위한 세 가지 input variable들을 나타내고 있다. 본 연구에서 제시된 측정항목의 모든 배열적 조합에 대하여 상관계수 (correlation coefficient)를 구하여, 연관성이 가장 높은 값을 가진 측정항목의 조합을 표시한다. 이러한 값은 동일한 장애 요인 (troubleshooting cases)의 반복적 계산을 통하여, 특정 조합의 상관계수 지수가 계속 높은 값으로 지속된다면, 다음 시간대에 발생하는 동일한 특정 조합으로 표현되는 사전 징후 발견은, 기존과 동일한 장애 사례로 추측이 가능하다. User intervention 모듈은 위에서 짝 지어진 장애 케이스와 측정항목 별과 상관계수가 네트워크 관리자의 level of confidence 지수를 요구한다. 발생된 사전 징후들에 관하여 false positive/negative 여부를 직관적 관점을 수치 값으로 반영하는 과정이다. 실례로, 사용자의 주관을 바탕으로 한 오디오/비디오의 QoS를

나타내는 Mean Opinion Score (MOS) (reference 추가)와 동일한 개념이다.

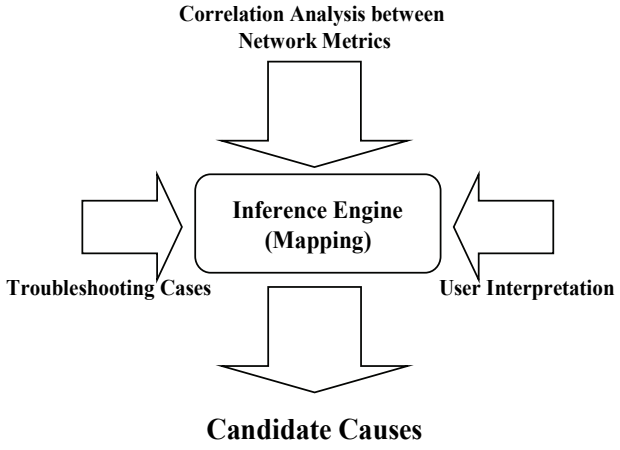


그림 3. 장애 요인 추론을 위한 개념적 구조

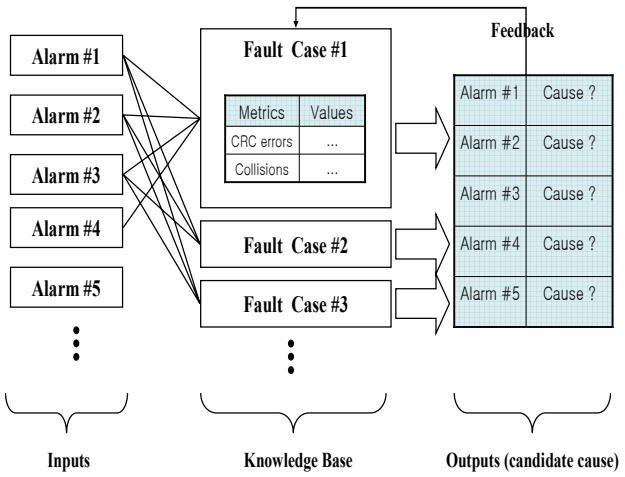


그림 4. 측정 항목과 장애 사례의 mapping 의 예

추론 기법 안에서 발생하는 항목별 mapping의 구체적 기법을 그림 4 에서 보여주고 있다. 각 장애 케이스는 측정가능 하였던 측정항목과 해당 수치로 표현된다. 이러한 장애 별 측정항목을 이용한 표현 방법은 지식 베이스 (knowledge base)의 역할을 수행하게 된다. 새로이 발생하는 사전 징후의 측정 항목과 과거의 장애 케이스를 바탕으로 지식 베이스에 구축되어 있는 장애 별 측정 항목간의 cross-match 를 실시한다. 위의 User intervention 의 과정에서 네트워크 관리자는 cross-match 의 결과 값을 보고 판단하게 된다. 이러 한 구조로 파악된 장애 별 측정항목은 지식베이스에 feedback 의 단계를 거쳐 추가가 이루어 지기도 한다. 이는 트래픽의 변형에 알맞게 대응하기 위한 구조이다. 현재는 충분한 수의 장애 요인의 수집이 필요하기 때문에, 설명된 장애 요인 분석 방법은 off-line 구조에서 이루어지고 있다.

측정치에 의존한 장애 사전 탐지에서는 장애 문제 해결의 답을 주는 것은 아니다. 그러나 최단시간 내에 네트워크 관리자가 주의를 기울어야 할 네트워크 세그먼트, 링크, 또는 특정 제어 기기 (예: IP 주소) 등으로 탐색 범위를 줄여주어, 빠른 장애 인지를 이끌어 내는 것 또한 안정적인 네트워크 운용에 있어 중요하다. 물론 정확하고 빠른 장애 요인의 분석은 사전 징후의 탐지 보다 한 단계 앞선 장애 대응을 가능하게 하며, 이는 fault-handling automation을 위한 중요한 발전 방향과 같이한다.

5. 결론

IP 네트워크가 많은 분야에서 적용되었음에도 불구하고, 장애에 민감한 공정 제어 네트워크에서의 모니터링과 트래픽 분석은 현재까지 연구가 미비하였다. 공정 제어 네트워크는 통신 장애에 더욱 취약하며, 기존 IP 데이터 네트워크에서는 묵과되고 넘어가던 장애가 치명적인 경제적 손실과 직결되어 있다. 빠른 장애 사전 징후의 정의와 탐지는 안정적인 공정 네트워크에 있어서 중대한 사항이다. 본 연구의 contribution 은 다음과 같이 정리해 볼 수 있다.

- 공정 제어 네트워크 장애 케이스의 정리 및 유형별 분류를 통한 참고 자료 수립
- 공정 제어 네트워크의 모니터링에 유용한 네트워크 측정 항목 및 항목별 장애 충족 요건 수립
- 원격 진단 시스템의 설계 및 구성 모듈의 정의

공정 제어 네트워크의 트래픽 특징 분석을 통한 적절한 트래픽 모델 및 장애 발생 유형의 모델 수립 연구를 진행하여, 시스템의 정확성을 평가할 예정이다. 그 밖에도 일반 IP 데이터 네트워크와 제어 네트워크간의 시스템적인 차이점을 정의하고, 비교 검증 연구를 목표로 하고 있다.

참고 문헌

[1] Nobuo Okabe. “Issues of Control Networks When Introducing IP,” Proc. of Symposium on Applications and the Internet Workshops, Vol. 00, pp. 80-83, 2005.

[2] Feng-Li Lian, James R. Moyne, and Dawn M. Tilbury. “Performance Evaluation of control networks: Ethernet, ControlNet, and DeviceNet,” IEEE Control Systems Magazine, 117(6), pp. 641-647, 2001.

[3] Fieldbus Foundation. FF-581-1.3, “FOUNDATION Specification: System Architecture,” 2003.

[4] PROFIBUS International. IEC 61158, “Digital Data communication for Measurement and Control – Fieldbus for Use in Industrial Control Systems,” 1999.

[5] MODBUS.ORG, “Modbus Application Protocol V1.0,” 2002.

[6] ASHRAE. ANSI/ASHRAE Standard 135-1995, “BACnet A Data Communication Protocol for Building Automation and Control Networks,” 1995.

[7] EIA. EIA/CEA-709.1-B, “Control Network Protocol Specification,” 2002.

[8] Packet Details Markup Language Specifications. http://www.nbee.org/Docs/NetPDL/PDML.htm/.

[9] Detecting Duplex Mismatch on Ethernet. http://www.pam2005.org/PDF/34310138.pdf/.

[10] Se-Hee Han, Myung-Sup Kim, Hong-Taek Ju and James W. Hong, "The Architecture of NG-MON: A Passive Network Monitoring System", 13th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management, LNCS 2506, Montreal, Canada, October, 2002, pp. 16-27.