論文95-32B-3-1

결함 허용 Mini-MAP 시스템의 구현 및 성능해석

(Implementation and Performance Analysis of a Fault-tolerant Mini-MAP System)

文 泓 周 *, 朴 洪 聖 **, 權 旭 鉉 *

(Hong-ju Moon, Hong Seong Park, and Wook Hyun Kwon)

요 약

본 논문에서는 고신뢰성의 결함 허용 Mini-MAP 시스템을 제안한다. 결함 허용성을 갖도록 하기 위하여 LLC부계층, MAC부계층, 물리계층을 이중화한 구조를 가지도록 구현한다. 결함의 감지, 고장난 통신망의 교체, 통신망의 유지 및 보수작업은 이중화를 위해 필요한 주요 기능들이며, 이 세가지 기능들은 각각 오동작감시기(ESM: Error Supervisory Machine), 오동작관리기(EMM: Error Management Machine), 통신망관리기(NMM: Network Management Machine)를 구성하여 수행되도록 한다. 결함의 감지에 MAC부계층의 매체 관리기능이 이용되며, 이중화한 두개의 네트웍에서 동시에 데이타를 수신하고 선택된 한개의 네트웍으로 송신하는 구조를 갖도록 구현한다. 제안된 결함 허용 Mini-MAP 시스템의 신뢰도및 평균연속동작시간(MTTF: Mean Time To Failure)을 해석하여, 일반 Mini-MAP 시스템과 비교하여 좋은 성능을 가짐을 보인다.

Abstract

In this paper, a fault-tolerant Mini-MAP system with high reliability is proposed. For fault-tolerance, the LLC sublayer, MAC sublayer, and physical layer of the Mini-MAP system are dualized. The detection of faults, the replacement of the failed network, and the management of the network are three major functions required for the dualization, and they are performed by ESM(Error Supervisory Machine), EMM(Error Management Machine), and NMM(Network Management Machine) of the proposed fault-tolerant Mini-MAP system, respectively. The ring maintenance function of the MAC sublayer is used for the detection of the faults. In the proposed fault-tolerant Mini-MAP system, the data are received from both of the dualized networks and transmitted to the selected one of the two. We analyze the reliability and the MTTF(Mean Time To Failure) of the proposed fault-tolerant Mini-MAP system and show that it has better performance compared to a general Mini-MAP system.

* 正會員, 서울大學校 制御計測工學科
(Dept. of Control and Instrumentation Engr., Seoul National University)
** 正會員, 江原大學校 制御計測工學科
(Dept. of Control and Instrumentation Engr., Kangwon National University)
接受日字 : 1994年 4月 13日

Ⅰ. 서 론

공장 자동화용 표준 통신망으로 발표된 MAP은 전 세계적으로 확산되어 여러 시스템에 적용되고 있으며[1], 국내에서도 활발한 연구가 진행되고 있다[2,3]. MAP은 7개의 계층으로 구성된 Full-MAP과 물리 계층(physical layer), 데이타 링크 계층(data link layer), 응용 계층의 3 계층으로 이루어진 Mini-MAP으로 나누어지며, Mini-MAP은 실시간 특성을 만족시키기 위한 시스템에 주로 사용된다[4]. Mini-MAP의 대표적인 응용 계층 부분은 MMS (Manufacturing Message Specification)이다. 데이타 링크 계층은 다시 MAC 부계층(Medium Access Control sublayer)과 LLC부계층(Logical Link Control sublayer)으로 구분되어진다. MAC 부계층은 IEEE 802.4에 규정된 토큰 전달 방식의 제어와 관리를 수행하며[5,6], LLC부계층은 IEEE 802.2에 규정된대로 데이타를 오류없이 순서대로 시간에 맞춰 전송하는 기능들을 수행한다[7].

시스템의 결함(fault)은 시스템의 하드웨어나 소프트웨어의 어느 한 부분에 이상이 있는 것을 말하며, 결함의 결과로 오동작(error)을 하게 되고, 이로 인하여 시스템이 주어진 기능을 수행하지 못하게 되면 고장(failure)이 발생하게 된다[8]. 결함이 발생하더라도 시스템의 동작에는 지장이 없게 하기 위해서는 결함허용(fault-tolerant) 시스템을 구축해야 한다. 결함허용 시스템의 목적은 신뢰도(reliability), 가용도(availability), 안전도(safety), 수행도(performability), 유지보수도(maintainability), 시험도(testability), 의존도(dependability) 등을 높이기 위한 것이다[8,9]. 이러한 시스템의 응용 예에는 보일러 제어 시스템, 비행기 제어 시스템 등이 있으며, 이들을 살펴보면 시스템에 결함이 발생하여 시스템이 동작하지 않는 경우에는 심각한 상황이 벌어질 수 있다는 것을 알 수 있다. 결함허용성을 갖도록 하기 위해서 잉여성(redundancy)을 넣게 되며, 대상과 방법에 따라 하드웨어 잉여성(hardware redundancy), 정보 잉여성(information redundancy), 시간 잉여성(time redundancy), 소프트웨어 잉여성(software redundancy)으로 나눌 수 있다[8].

Mini-MAP을 실시간성과 고신뢰성을 요구하는 결함허용 시스템에 적용하는 경우에는 당연히 이중화 등의 방법으로 잉여성을 갖도록 하여 Mini-MAP에서 발생할 수 있는 모든 결함들을 인지하여 시스템의 동작이 중지되지 않도록 설계해야 한다. Mini-MAP에서 발생가능한 결함을 계층별로 구분해 보면, 물리계층의 결함으로 케이블의 단락, 임피던스의 변화, 외란의 개입, 모뎀의 고장이 있고, MAC부계층의 고장으로 데이타 전송이나 수신 기능의 마비, 모뎀 접속부의 고장, 논리적 링의 유지 관리 기능의 마비가 있으며, 그 외에 LLC부계층기능의 마비, 응용 계층의 고장, 그리고 각 부분들 사이를 연결하는 접속부의 고장 등이 있다.

고신뢰도를 요구하는 시스템에 적용되는 통신망의 경우 여러 종류의 결함허용 통신망이 개발되어 사용되고 있다[4,10,11]. Mini-MAP 역시 고신뢰성 시스템에 적용되는 경우, 결함허용성을 갖도록 해야 한다. 결함허용 MAP의 연구에는 물리계층이 이중화된 Mini-MAP 시스템인 ADMAP[10]과, 수정된 형태의 Full-MAP 시스템에서 물리계층을 이중화 시킨 MAP Mining[11]이 있다.

본 논문에서는, LLC부계층 이하계층에 대해 대기교체 방법(stand-by sparing)을 적용하여, LLC부계층 이하를 이중화 시킨 결함허용성 Mini-MAP을 제안한다. Mini-MAP을 이중화시킬 경우, 이중화의 범위에 따라 응용계층을 포함한 모든 부분의 이중화, LLC부계층 이하부분의 이중화, MAC부계층 이하부분의 이중화, 물리계층의 이중화로 나눌 수 있다. 상위 계층까지 이중화할수록 적용되는 결함의 범위가 넓어져서 신뢰도가 증가하지만, 구축 비용이 증가하게 된다. 일반적으로 채택되는 방법인 물리 계층만의 이중화의 경우 하드웨어적인 방법에 의해 비교적 간단한 구조로 구현되며 신속한 전환이 가능하지만, MAC부계층및 LLC부계층에 대해서는 결함허용성을 전혀 보장할 수 없는 것은 물론이다. 본 논문에서는, 적당한 비용으로 보다 높은 신뢰성을 얻기 위하여, LLC부계층이하를 이중화한다. 즉, 통신망에서 일반적으로 이중화시키는 물리계층외에 MAC부계층과 LLC부계층을 이중화한다. LLC부계층의 사용자에게는 두개의 통신망이 존재하지만 결함의 유무에 따라 하나가 자동으로 선택되어 사용되도록 구현한다.

이중화를 위해서는 결함의 감지, 결함발견시 이중화된 부분의 전환, 전환후의 처리가 필요하다. 따라서, 본 논문에서 제안된 이중화 Mini-MAP에서의 결함의 감지는 LLC부계층, MAC부계층에서 자신및 아래계층의 동작을 감시하고, 응용계층에서 아래계층의 동작을 감시하는 방식을 사용하며, 동시에 결함 감지 기능을 높이기 위하여 동작감시타이머(watchdog timer)를 사용한다. 물리계층의 이상은 MAC부계층의 접근제어기(Access Control Machine)의 링 유지·관리 기능을 이용하여 감지한다. 이중화된 양쪽의 네트웍에서 수신하고 선택된 한쪽의 네트웍으로 송신하는 구조를 채택하여, 네트웍의 전환은 송신할 네트웍을 전환하는 것

으로 이루어지도록 구현한다. 본 논문에서 구현된 이중화 Mini-MAP은 RedMAP(a REDundant MAP system)이라고 명명되었다. RedMAP은 MMS를 장착한 Mini-MAP에 오동작감시기(ESM: Error Supervisory Machine), 오동작관리기(EMM: Error Management Machine), 통신망관리기(NMM: Network Management Machine)의 세 모듈을 추가하고, MMS와 이중화된 LLC부계층이 양방향 데이타 교환장치(TWDEP: Two-Way Data Exchange Protocol)를 사이에 두고 연결된 구조로 되어 있다. 오동작감시기는 MAC부계층과 LLC부계층및 응용계층에 걸쳐서 존재하여, 오동작을 감시하여 결함을 감지할 경우 오동작관리기에 알려주는 역할을 한다. 오동작관리기는 응용 계층과 같은 레벨에 위치하여, 어느 한 스테이션에서 감지된 이상을 전 통신망에 전달하여 공유시키고, 통신망의 전환과 전환시의 주요작업처리를 담당한다. 통신망관리기는 이상 발생후의 처리와 진단 기능을 포함한다.

RedMAP의 성능향상을 평가하기 위한 지표로는 신뢰도, 평균연속동작시간(MTTF: Mean Time To Failure)[8]를 사용한다. 신뢰도는 시스템이 주어진 실행 환경하에서 일정기간동안 정확히 작업을 수행할 수 있는 확률이다. 즉, 주어진 Mini-MAP 시스템의 신뢰도 $R(t)$는 Mini-MAP 시스템이 동작을 개시한 시간 0부터 시간 t사이에 통신장애가 전혀 일어나지 않고 계속적인 통신이 가능할 확률을 말한다. 평균연속동작시간은 시스템 실패가 발생할 때까지의 예상시간이다. RedMAP의 경우 평균연속동작시간은 이중화된 양쪽의 네트워이 모두 고장난 상태가 되어 통신이 불가능하게 될때까지의 평균 시간을 뜻한다.

2장에서 RedMAP이 갖춰야할 성질과, 이중화와 관련된 MAC부계층의 개략적인 특징에 대해 언급하고, 3장에서 RedMAP의 구현에 대해 설명한 후 4장에서 성능 평가를 한다. 마지막으로 5장에서 결론을 짓는다.

Ⅱ. RedMAP의 개요

RedMAP의 적용 대상 시스템의 예를 들면, 그림 1의 구성도를 갖는 화력 발전소의 분산 제어 시스템[12]과 같다. 대상 시스템은 고신뢰성을 요구하면서, 통신장애 발생순간부터 5초의 복구시간을 허용하는 경우를 대상으로 한다.

결함허용성을 얻기 위해 이중화 방법을 사용한 RedMAP이 갖추어야 할 주요한 성질들은 다음과 같다.

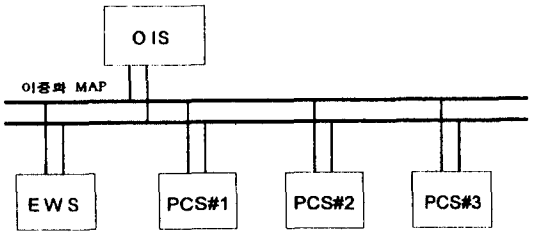
[성질1] 모든 결함을 (정확하고 빠르게) 감지할 수 있어야 한다.

[성질2] 이중화된 부분의 전환이 가능해야 한다.

[성질3] 각 스테이션들의 전환시점의 차이가 동작에 영향을 주지 않아야 한다.

[성질4] 통신망의 이상에 의해 잘못 전송된 정보나 손실된 정보에 대한 적절한 처리가 가능해야한다.

[성질5] 이상 상태 발생으로 이중화된 부분이 전환된 후 이상상태가 발생된 부분의 이상 발생 원인을 찾아내어 가능한 빠른 시간에 복구를 시켜 다시 원래대로 회복시켜 줄 수 있어야 한다.



OIS: Operator Interface Station
EWS: Engineering WorkStation
PCS: Process Control Station

그림 1. 발전소의 분산제어 시스템 구성도
Fig. 1. Structure of the distributed control system for a power plant.

위의 다섯가지 성질들 이외에도 이중화된 두개의 부분은 가능하면 오동작이나 결함에 대해 서로 영향이 없도록 해야 하고, 상위계층에 대한 투명성(transparency)을 갖도록 해야 한다.

MAC부계층은 접속기(interface machine), 접근제어기(access control machine), 수신기(receive machine), 송신기(transmit machine)와 선택적으로 존재하는 재발생반복기(regenerative repeater machine)의 다섯부분으로 이루어진다[5,6]. 이중에서 접근제어기가 버스에 대한 전송권을 관리하는 기능을 갖는다. 접근제어기는 미디어의 사용 권리를 부여하기 위해서, 논리적 링을 구성하고 이 논리적 링의 순서에 따라 토큰을 차례로 전달하여 미디어의 사용권리를 전달하며 이 논리적 링을 유지 보수하는 기능을 갖는다. 고장이나 외란을 고려한 접근제어기의 논리적 링의 유지 보수 기능은 다음과 같다[5,6,13]. 접근제어기는 상태가 PASS_TOKEN상태이고 변수 pass_state가 값 pass_token일때 토큰을 전달한 후 토큰이 제대로 전달 되었는지를 검사하여 다음 스테이션이 링에서 빠져나가거나 고장으로 인해 토큰을 받지 못하는 경우, 접근제어기에서는 token_pass_failed의 천이(transition)가 일어나고 변수 pass_state의 값은 pass_

token에서 repeat_pass_token으로 바뀌어 토큰을 재전송한다. 토큰의 재전송에서도 실패하면 변수 pass_state의 값은 send_who_follows로 바뀌고 논리적 링상에서의 다음 스테이션을 찾기 위해 who_follows 프레임을 전송한다. 그 다음 스테이션도 who_follows 프레임에 대한 응답이 없으면 변수 pass_state의 값은 solicit_any로 바뀌고 링상에 존재하는 모든 스테이션에서 새로운 후속자를 찾는다. 만약 링상의 모든 스테이션들이 전부 사라지거나 자신이 수신 불능 상태에 빠지게 되면 접근제어기의 상태 IDLE에서 bus_idle_timer_expired의 천이가 발생하여 새롭게 링을 구성하려 하거나 새로운 스테이션이 링에 추가되기를 기다린다. MAC부계층의 접속기는 "MA_UNITDATA request", "MA_UNITDATA indication", "MA_UNITDATA confirm"의 세가지 프리미티브(primitive)를 통한 LLC부계층과 MAC부계층사이의 접속을 담당한다. LLC부계층의 전송요구에 대한 결과로 "MA_UNITDATA confirm"이 발생하여 성공 혹은 실패의 여부를 알려준다.

다음장에서는 2장에서 제시한 RedMAP이 갖춰야 할 주요성질들을 만족시키기 위한 각각의 구현 방법을 제시하고, 이들 방법들을 통합하여 구현되는 RedMAP의 구성과 동작에 대해 서술하겠다.

Ⅲ. RedMAP의 구현

이번 장에서는 RedMAP이 갖추어야 할 각 성질을 만족시키기 위한 구현방법을 서술한 후, RedMAP의 구성과 각 구성요소의 동작과 기능을 서술한다.

[성질1]을 만족시키기 위해서는 먼저 이상 상태의 감지가 있어야 한다. 대상이 되는 모든 결함은 그 발생의 결과로 즉시 오동작을 일으킨다고 하면, 오동작의 관찰을 통하여 모든 결함을 감지할 수 있다. 이중화가 LLC부계층을 대상으로하여 이루어지므로 LLC부계층 바로 위의 부분에서 이상현상을 관찰하는 것만으로 결함을 감지하는 역할을 할 수 있겠으나, 결함의 빠른 감지와 잠재적인 결함의 감지를 위하여 MAC부계층의 이상을 LLC부계층이 감시하고, 미디어의 이상이나 통신망상의 다른 스테이션의 MAC부계층에 있는 접근제어기의 이상을 각 스테이션의 접근제어기에서 감시하도록 구현하였다.

그림 1에 보여진 바와 같이 LLC부계층의 사용자는 두개의 통신망에 연결되어 있는 형태가 된다. 이 두개의 통신망을 각각 Nmain, Nsub라고 이름붙인다. 주로 사용하는 통신망이 Nmain, 예비로 대기하는 통신망이 Nsub가 된다. [성질2]와 [성질3]을 만족시키기 위하여, 한쌍으로 되어 있는 통신망은 적절한 방법으로 전환되어야 한다. 두개의 통신망을 전환하며 사용하는 방법은 수신방향과 송신방향에 따라 네가지로 구분할 수 있다. 두개의 통신망을 Nmain, Nsub라고 하고, 두개 중에서 하나를 선택하는 경우, 선택된 통신망을 Nu라고 하고, 다른 하나를 Ns라고 부른다. 예를 들어 Nmain을 Nu로 정하면 Ns는 Nsub가 되고, Nsub는 대기 상태가 됨을 말한다. 이와 같은 기호를 써서 두 개의 통신망의 사용을 다음과 같은 네가지로 구분할 수 있다. 첫째 Nu에만 데이타를 전송하고 Nu로부터오는 데이타만 수신하는 방법, 둘째 Nu, Ns에 데이타를 전송하고 Nu로부터 오는 데이타만 수신하는 방법, 세째 Nu로 데이타를 전송하고 Nu, Ns양쪽으로부터 오는 데이타를 수신하는 방법, 네째 Nu, Ns로 데이타를 전송하고 Nu, Ns로부터 수신하는 방법이 있다. 양쪽으로 데이타를 전송하는 경우 한쪽의 통신망에 이상이 생겨도 데이타의 복구가 가능하겠으나, 양쪽의 LLC부계층이 서로 다른 상태에 있을 수 있으므로 동시에 전송하기 어렵고 각각의 LLC부계층으로부터 오는 데이타를 처리해 주어야 하므로 전송시간과 수신데이타의 처리시간이 길어지고, 수신부의 처리 알고리즘도 매우 복잡해 진다. 한쪽으로만 전송할 때, 상대편 수신측을 생각하면 어차피 한쪽으로만 데이타가 오므로 양쪽으로 수신하는 경우는 한쪽에서만 수신하는 경우와 비교하여 수신방법이나 수신시간에 거의 차이가 없게 된다. 한쪽으로 전송하고 한쪽으로부터 수신하는 경우, 전송측에서 Nu로 데이타를 전송한 후 수신측의 사용자가 이 데이타를 받기전에 Nu와 Ns가 전환되면 데이타는 Ns로 수신되어 수신측의 사용자로 전달되지 않을 수 있지만, 한쪽으로 전송하고 양쪽으로부터 수신하면 송신측의 Nu, Ns에 관계없이 수신측의 사용자는 Nu혹은 Ns로 수신된 데이타를 전달받을 수 있게 된다. 따라서, 본 논문에서는 세번째의 방법을 택하여 Nmain과 Nsub중 하나를 Nu로 정하여 전송하고, Nmain과 Nsub양쪽으로부터 수신하는 방법으로 구현하였다. 이 방식을 사용하면, 전송시 어느 통신망을 Nu로 할 것인가를 정해주는 알고리즘만 있으면, 각각의 스테이션은 다른 스테이션들의 Nu에 관계없이 개별적으로 Nu를 전환하는 것으로 통신망의 전환작업을 마칠 수 있고 [성질3]을 만족시키게 된다. 초기 시점에서는 Nu는 Nmain이 정하고, Nmain에 결함이 생기면 Nsub를 Nu로 바꾸어 통신이 계속되도록 하고, Nmain의 결함이 복구되면 다시 Nu를 Nmain로 정하여 사용한다.

[성질4]를 만족시키기 위한 방법을 생각해 보면, 데이타를 주고 받는 도중에 결함이 생겨서 데이타가

깨지더라도 LLC윗부분에 존재하는 MMS에서 걸러주게 되므로 잘못된 데이타는 모두 버리게 되고 사용자는 데이타의 손실을 알게 된다. 사용자는 재전송을 통해 손실된 데이타를 복구한다.

[성질5]는 통신망의 전환 후 보고된 이상상태에 대한 정보와 각 스테이션의 각 모듈에 대해 테스트한 결과를 합하여 빠른 시간내에 고장난 부분을 찾아냄으로써 만족시킨다.

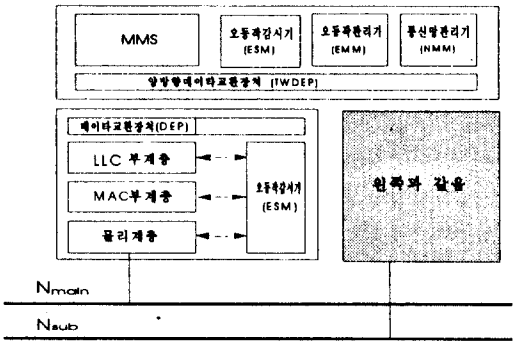


그림 2. RedMAP의 구성도
Fig. 2. Structure of the RedMAP.

이상에서 설명한 방식으로 구현된 RedMAP은 그림 2와 같이 크게 오동작감시기, 오동작관리기, 통신망관리기의 세가지 부분이 원래의 Mini-MAP과 결합되고, 이중화된 LLC부계층과 MMS를 양방향 데이타 교환장치가 연결하는 구조로 이루어진다. 또한, 통신망 상의 어느 한 스테이션은 운영자 스테이션으로 정해져서 고장 발생후의 처리에 대한 책임을 담당하게 된다.

오동작감시기는 MAC부계층과 LLC부계층및 응용계층에 걸쳐서 존재하여 이상상태를 감지하여 오동작관리기에 알려주는 기능을 갖는다. 오동작감시기에서 하는 이상감지는 계층별로 상위 계층이 하위계층을 감시하는 형태로 되어 있어서, 응용계층 레벨에서 LLC부계층을 감시하고, LLC부계층에서 MAC부계층을, MAC부계층에서 물리계층을 감시한다. 응용계층에서 통신이 정상적으로 되고 있는가를 점검하는 것만으로 LLC부계층및 LLC의 아래계층인 MAC부계층, 물리계층의 정상여부가 확인되지만, 결함의 보다 빠른 감지를 위하여 LLC부계층에서 MAC부계층을, MAC부계층에서 물리 계층을 감시한다. 또한, 동작감시타이머(watchdog timer)를 설치하여 이상 감지에 대한 잉여성을 부여한다. 오동작관리기는 응용계층과 같은 계층에 존재하여 통신망의 전환및 전환직후의 처리작업을 담당한다. 오동작관리기는 정상 동작중에 오동작감시기로부터 이상 상태가 보고되면, 먼저 자신의 Nu를 Nsub으로 바꾸고 전환된 Nu(= Nsub)를 통해 이상상태를 방송(broadcast)으로 통신망 전체에 알린다. 통신망관리기는 이상 상태가 발생될 경우 통신망을 분석하여 고장난 부분을 찾아내는 기능과 전체적인 통신망의 관리 기능을 갖고 있어서 이상 상태 발생후의 유지, 보수작업에 사용된다.

MMS는 LLC의 Type 1, Type 3 서비스를 사용하는데, Type 3 서비스의 경우, DL_DATA_ACK_STATUS_indication과 DL_REPLY_STATUS_indication, DL_REPLY_UPDATE_STATUS_indication이 해당되는 요구에 대해 올라오지 않거나 실패를 나타내는 상태값을 갖고 올라오는 경우에 이상상태로 간주한다. Type 1 서비스를 이용하는 경우, MMS에서 확인성 서비스를 사용하면 부정적인 값을 갖는 확인(confirmation)이 발생할 때를 감지하여 이상상태를 알아내고 비확인성 서비스를 사용하면 주기적으로 확인성 서비스형태의 통신망 점검 메세지를 주고받는 방법으로 이상상태를 점검하여야 한다. RedMAP에서는 이상상태의 빠른 감지를 위해 LLC Type 3 서비스를 사용하도록 한다. LLC부계층은 MAC부계층의 MA_UNITDATA_request에 대한 MA_UNITDATA_confirm을 감시하여 실패를 나타내는 상태값을 갖고 올라오는 경우나 MA_UNITDATA_confirm이 올라오지 않는 경우를 보고 MAC부계층 수신부의 이상을 알아낸다.

물리계층의 이상에 대한 감시는 MAC부계층에 있는 접근제어기의 논리적 링 유지 보수 기능을 이용한다. 논리적 링에 이상이 있을 경우 접근제어기의 스테이트 머쉰(state machine)에서 발생할 수 있는 상황을 네가지로 구분하여 상태와 천이의 시퀀스를 나타내면 다음과 같다[5,6,13]. ()로 묶인 것은 MAC부계층의 접근제어기에 있는 변수 pass_state[5,6]의 값, {}로 묶인 것은 접근제어기의 상태, 괄호로 묶이지않은 것은 접근제어기의 천이를 나타낸다.

[경우 1] 토큰을 가진 스테이션 다음의 스테이션이 빠져나갈 경우 토큰을 가진 스테이션에서 발생하는 시퀀스 token_pass_failed -> (repeat_pass_token) -> token_pass_failed -> (who_follows)

[경우 2] 토큰을 가진 스테이션 다음과 그 다음 스테이션이 빠져 나갈 경우 토큰을 가진 스테이션에서 발생하는 시퀀스

token_pass_failed -> (repeat_pass_token)
-> token_pass_failed -> (who_follows)
-> no_response_10 -> (repeat_who_follows)
-> no_response_10 -> (solicit_any)

[경우 3] 토큰을 가진 스테이션 이외의 스테이션이 모두 빠져 나갈 경우 토큰을 가진 스테이션에서 발

생하는 시퀀스

token_pass_failed -> (repeat_pass_token)
-> token_pass_failed -> (who_follows)
-> no_response_10 -> (repeat_who_follows)
-> no_response_10 -> (solicit_any)
-> no_response_10 -> {idle}
-> bus_idle_timer_expired

[경우4] 토큰을 가진 스테이션이 토큰을 넘겨 주지 못하고 빠져 나갈 경우 다른 스테이션에서 발생하는 시퀀스

bus_idle_timer_expired

물리계층에 이상이 생기거나 접근제어기의 토큰 관리 기능에 이상이 생기면 논리적 링이 붕괴하게 되고 접근제어기는 논리적 링 상의 스테이션들이 링에서 빠져 나가는 것으로 감지하게 되고 이상이 생긴 부분따라 위의 [경우1], [경우2], [경우3], [경우4]들이 하나이상의 스테이션에 따라 발생하게 된다. 따라서, 위의 상황들을 감지함으로써 물리계층의 이상이나 다른 스테이션의 접근제어기의 이상을 감지할 수 있다. 전환 알고리즘을 상태도로 나타내면 그림 3과 같다. 앞에서도 설명한 바와 같이 보통때는 Nmain을 Nu로 하고 Nmain에 이상이 있다고 판단되는 경우에만 Nu를 Nsub라 하고 Nmain에 있는 결함이 제거되면 다시 Nu를 Nmain으로 한다. Nmain이나 Nsub의 한쪽에 이상이 있는 상태에서 다시 나머지 한쪽에서 이상이 발생하는 경우는 전환하지 않고, Nmain과 Nsub 모두에 이상이 있는 상태에서 한쪽의 결함 요인이 제거되면 그쪽으로 전환시킨다.

이상에서 설명한 방식과 구조로 구현된 전체적인 이상 감지, 전환, 복구 과정을 살펴보면 다음과 같다.

[단계1] 이상상태의 감지
- 오동작감시기에서 앞에서 설명한 방법으로 Nmain과 Nsub의 이상을 감지하여 오동작관리기에 알린다.
- 다른 스테이션의 오동작관리기의 방송에 의해서도 통신망에 이상이 있는 것을 감지한다.
- Ns에서 이상이 감지되는 경우 [단계3]으로 넘어간다.

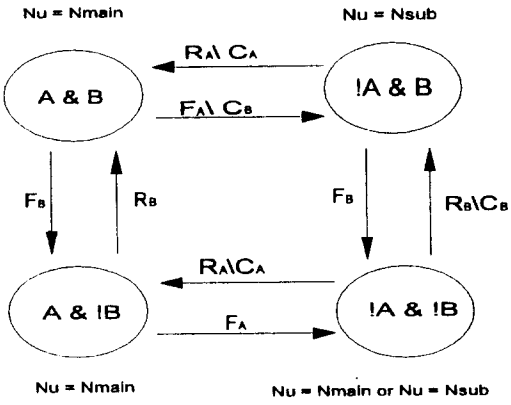
[단계2] 통신망의 전환
- 오동작관리기에서 통신망을 전환한다.

[단계3] 이상상태 정보의 공유
- 자신의 오동작감시기에서 감지한 이상인 경우는 통신망상의 다른 스테이션에 방송을 통해 알린다.

[단계4] 결함에 의해 발생한 오류의 복구
- 사용자는 결함 상태로 인해 분실된 데이타가 있으면, 재전송등의 적절한 처리로 복구한다.

[단계5] 통신망 진단및 고장원인의 제거
- 통신망관리기는 발생한 이상에 대한 정보와 통신망을 진단하여 얻어지는 정보를 종합하여 결함이 생긴 부분을 찾아 결함을 제거한다.

[단계6] 초기상태로 복귀- 통신망관리기는 Ns가 정상인지 확인하고 정상이면 Nmain을 Nu로 하고, 정상이 아닌 경우는 [단계5]를 다시 수행한다.



A : Nmain 정상 A : Nmain 이상
B : Nsub 정상 B : Nsub 이상
F_A : Nmain 고장 F_B : Nsub 고장
R_A : Nmain 수리 R_B : Nsub 수리
C_A : Nmain으로 전환 C_B : Nsub으로 전환
E1\E2 : E1의 결과로 E2가 발생

그림 3. 네트워 전환 알고리즘

A : Normal state of Nmain A : Abnormal state of Nmain
B:Normal state of Nsub B:Abnormal state of Nsub
F_A : Failure of Nmain F_B : Failure of Nsub
R_A : Repair of Nmain R_B : Repair of Nsub
E1\E2 : E2 occurs as the result of E1

Fig. 3. Algorithm of the change of networks.

RedMAP은 일반 Mini-MAP의 동작을 유지하도록 설계되었으므로, 사용자에 대한 투명성을 갖고 있다. 단, 결함 발생순간 통신망의 결함은 복구되지만, 결함에 의해 손실되는 데이타는 복구되지 않으므로, 사용자는 결함발생 순간에 생길 수 있는 데이타의 손실을 없애고자 할 경우에는 데이타의 재전송을 하도록 하여야 한다.

Ⅳ. RedMAP의 성능평가

RedMAP의 성능 지표로서 신뢰도, 평균연속동작시간[8]을 사용한다. 완벽한 이상의 감지및 전환을 가정

하며, 이상의 감지및 전환에 의한 시간지연은 무시한다.

분석의 대상이 되는 시스템의 결함발생은 발생률 λ를 갖는 프와송(Poisson)분포[14]이며, 결함수리시간은 평균 $1/\mu$의 지수분포라고 가정한다. 즉, 상수의 결함 발생률 λ를 갖고, 상수의 결함 수리율 μ를 갖는다. 이중화된 두개의 통신망은 서로 결함발생에 대해 독립이고, 같은 특성을 갖는다고 가정한다. 통신망에 결함이 생겼을 때, 수리할 수 있는 자원(resource)은 하나만 있다고 가정한다 즉, 양쪽의 통신망에 모두 결함이 있는 경우, 한 통신망의 결함을 수리한 후 다른 통신망의 고장을 수리한다. 또한, 시스템에 하나의 결함만 있어도 고장을 일으킨다고 가정한다. 성능 평가 모델로는 마코프(Markov) 모델[8,15]을 사용한다.

RedMAP을 마코프 모델로 나타내면 그림 4 (a)와 같이 된다. 상태 0은 두개의 통신망 모두 결함이 없는 경우, 상태 1은 하나의 통신망만 결함이 있는 경우, 상태 2는 두개의 통신망 모두에 결함이 존재하는 경우를 나타낸다. 통신망은 초기상태가 상태 0이라고 가정한다. 이중화되지않은 일반 Mini-MAP은 그림 4 (b)와 같이 모델링되며, 여기서 상태 0은 결함이 없는 경우, 상태 1은 결함이 있는 경우를 나타낸다.

RedMAP의 신뢰도 $R_d(t)$를 구하기 위해 다음과 같이 $\tilde{p}_0(t)$, $\tilde{p}_1(t)$을 정의한다.

$\tilde{p}_0(t)$:= RedMAP이 [0, t]에서 상태 0 또는 상태 1에 있고, t에서 상태 0에 있을 확률

$\tilde{p}_1(t)$:= RedMAP이 [0, t]에서 상태 0 또는 상태 1에 있고, t에서 상태 1에 있을 확률

시간 t에서의 신뢰도 $R_d(t)$는 식 (1)과 같이 $\tilde{p}_0(t)$와 $\tilde{p}_1(t)$의 합이다. 임의의 시점 t와 매우 짧은 시간 Δt후에 대해 생각해 보면 식 (2)와 같은 관계가 성립하고[14,16], 정리하여 극한값을 취하면 식 (3)을 얻을 수 있다. 동작을 시작할 때에는 상태 0에 있게 되므로 초기값은 식 (4)와 같다.

$$R_d(t) = \tilde{p}_1(t) + \tilde{p}_0(t) \tag{1}$$

$$\begin{aligned} \tilde{p}_1(t+\Delta t) &= (1-\lambda\Delta t-\mu\Delta t)\tilde{p}_1(t) + (2\lambda\Delta t)\tilde{p}_0(t) \\ \tilde{p}_0(t+\Delta t) &= (\mu\Delta t)\tilde{p}_1(t) + (1-2\lambda\Delta t)\tilde{p}_0(t) \end{aligned} \tag{2}$$

$$\begin{aligned} \dot{\tilde{p}}_1 &= (-\lambda-\mu)\tilde{p}_1(t) + 2\lambda\tilde{p}_0(t) \\ \dot{\tilde{p}}_0 &= \mu\tilde{p}_1(t) + (-2\lambda)\tilde{p}_0(t) \end{aligned} \tag{3}$$

$$\tilde{p}_1(0) = 0, \quad \tilde{p}_0(0) = 1 \tag{4}$$

식 (1), 식 (3), 식 (4)를 풀면 $R_d(t)$는 다음과 같이 구해진다.

(a) (b)

그림 4. 성능 평가를 위한 MAP의 Markov모델
(a) 이중화된 Mini-MAP
(b) 일반 Mini-MAP

Fig. 4. Markov model of the MAP system for performance analyses.
(a) Dualized Mini-MAP
(b) General Mini-MAP

$$\begin{aligned} R_d(t) &= b_1 e^{-a_1 t} + b_2 e^{-a_2 t}, \\ b_1 &= \frac{1}{2}\frac{(\mu+3\lambda)}{\sqrt{\mu^2+6\mu\lambda+\lambda^2}} + \frac{1}{2}, \\ b_2 &= \frac{-1}{2}\frac{(\mu+3\lambda)}{\sqrt{\mu^2+6\mu\lambda+\lambda^2}} + \frac{1}{2}, \\ a_1 &= \frac{1}{2}(\mu+3\lambda) - \frac{1}{2}\sqrt{\mu^2+6\mu\lambda+\lambda^2}, \\ a_2 &= \frac{1}{2}(\mu+3\lambda) + \frac{1}{2}\sqrt{\mu^2+6\mu\lambda+\lambda^2} \end{aligned} \tag{5}$$

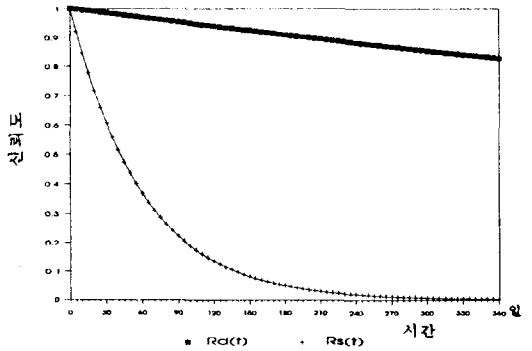
일반 Mini-MAP의 신뢰도 $R_s(t)$는 그림 4 (b)에서 시간 구간 (0,t)동안 계속하여 상태 0에 있을 확률이므로 $R_s(t)=e^{-\lambda t}$로 얻어진다. 고장율 λ가 1번/60일, 수리율 μ가 1번/1일인 경우와 고장율 λ가 1번/120일, 수리율 μ가 2번/1일인 경우에 대하여 $R_d(t)$와 $R_s(t)$를 비교해 보면 그림 5와 같다. 그림에서 알 수 있는 바와 같이 하나의 통신망으로 동작하는 경우 1년 후에는 신뢰도가 거의 0에 가까운 데 반해, 이중화시킨 경우는 신뢰도가 거의 1정도 수준을 계속 유지하는 것을 알 수 있다. 이와 같이 $R_d(t)$는 $R_s(t)$에 비해 매우 큰 값을 갖게 되고, 고장율에 대한 수리율의 비가 클수록 RedMAP의 신뢰도는 더욱 좋아짐을 알 수 있다.

$R(\infty)=0$인 경우 평균연속동작시간은 신뢰도 $R(t)$를 적분하여 얻어진다[8]. 따라서 RedMAP의 평균연속동작시간 T_{FD}와 일반 Mini-MAP의 평균연속동작시간 T_{FS}는 다음과 같이 얻어진다.

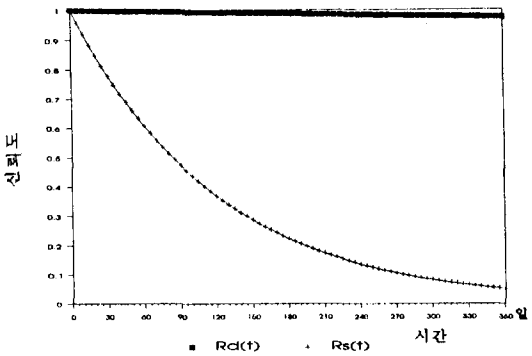
$$\begin{aligned} T_{FD} &= \int_0^\infty R_d(t)\,dt \\ &= \frac{b_1}{a_1} + \frac{b_2}{a_2} \\ &= \frac{(\mu+3\lambda)}{2\lambda^2} \end{aligned} \tag{6}$$

$$T_{FS} = \int_0^\infty R_s(t)\,dt = \frac{1}{\lambda} \quad (7)$$

RedMAP의 평균연속동작시간에 대한 일반 Mini-MAP의 평균연속동작시간의 비 r_{MTTF}는 다음과 같다.



(a)



(b)

그림 5. 일반 MAP과 RedMAP의 신뢰성 비교
(a) λ=1번/60일, λ=1번/1일
(b) λ=1번/120일, λ= 2번/1일

Fig. 5. Comparison of reliabilities between a general MAP and the RedMAP.
(a) λ =1 time/60 days, λ=1 time /1 day
(b) λ=1 time/120 days, λ=2 times /1 day

$$r_{MTTF} = \frac{T_{FD}}{T_{FS}} = \frac{\mu}{2\lambda} + \frac{3}{2} \quad (8)$$

평균연속동작시간의 경우에도 고장율에 대한 수리율의 비가 커짐에 따라 매우 좋은 성능을 낸다. 고장율 λ가 1번/60일, 수리율 μ가 1번/1일인 경우 31.5배, 고장율 λ가 1번/120일, 수리율 μ가 2번/1일인 경우 121.5배로 평균연속동작시간이 좋아진다.

다음으로 물리계층만 이중화된 경우와 LLC 부계층 이하까지, 즉 데이타링크 계층까지 이중화시킨 경우의 성능을 간단하게 비교하겠다. 물리계층의 고장율을 λ_1, 데이타링크의 고장율을 λ_2, 물리계층의 수리율을 μ_1, 데이타링크계층의 수리율을 μ_2라고 하자. 일반적으로 데이타링크계층 이하의 고장율 λ는 $\lambda_1+\lambda_2$으로 놓을 수 있으며, $\mu=\mu_1=\mu_2$ 라고 가정할 수 있다. 이 경우에도 데이타링크계층 이하를 이중화한 경우의 마코프 모델은 그림 4 (a)의 경우와 같다. 물리계층만 이중화시켰을 경우에 대하여 데이타링크계층의 고장을 고려한 네트워의 마코프 모델은 그림 6 (a)와 같다. 통신이 가능하여 시스템이 정상동작할 수 있는 상태와 고장으로 인해 통신이 불가능한 상태의 구분만이 중요하므로 이 마코프 모델을 단순화하여 성능을 알아보자. 그림 6 (a)의 상태 0, 상태 1이 정상동작 상태이고 상태 2, 상태 3, 상태 4가 고장상태이다. 먼저 상태 2와 상태 4를 하나의 상태 5로 합하면 그림 6 (b)와 같이 된다. 상태 0과 상태 1을 합하여 상태 6이라 하고, 상태 3과 상태 5를 합하여 상태 7이라 하면 그림 6 (c)와 같이 된다. 상태 6이 정상동작을 하는 상태이고, 상태 7이 고장난 상태이다. 이때 λ'은 $\lambda_2<\lambda'<\lambda_1+\lambda_2$ 의 범위를 갖는다. $\lambda'=r\lambda$로 쓰면, r은 $\lambda_2/\lambda<r<1$ 의 범위를 갖는다.

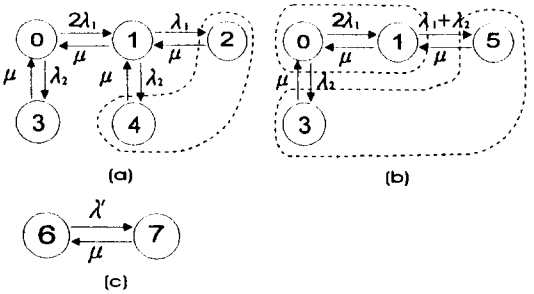


그림 6. 물리계층만을 이중화한 네트워크의 마코프 모델

Fig. 6. Markov model of the network of which physical layer is dualized.

물리계층만을 이중화한 경우의 신뢰도 $R_p(t)$는 $R_s(t)$와 같이 $R_p(t)=e^{-rlt}$이고, 평균연속동작시간 T_{FP}는 $1/r\lambda$이다. 이중화시키지 않은 일반 네트워크과 물리계층만을 이중화시킨 네트워크의 평균연속동작시간의 비 T_{FP}/T_{FS}는 $1/r$이다. λ_1에 비해서 λ_2가 큰 값을 갖음에 따라 r은 1에 가까운 값을 갖게 되고 물리계층만을 이중화하여서는 얻을 수 있는 성능상의 이득이 거의

없음을 알 수 있다. 하지만, λ_1에 비해서 λ_2가 매우 작은 값을 갖는 경우는 물리계층만을 이중화 하여도 데이타링크 이하까지 모두 이중화 하는 경우와 거의 같은 성능상의 이득을 얻을 수 있음을 그림 6 (b)로부터 쉽게 알 수 있다.

V. 결 론

본 논문에서는 Mini-MAP의 LLC부계층, MAC부계층, 물리계층을 이중화하여 결함허용성을 갖는 결함허용성 Mini-MAP을 구현하였다.

본 논문에서 구현된 결함허용성 Mini-MAP인 RedMAP은 일반 Mini-MAP 시스템에 결함을 감지하는 기능을 수행하는 오동작감시기, 결함이 있는 부분을 교체하여 통신망의 이상상태로부터 복구시키는 오동작관리기, 통신망의 점검및 수리를 지원하는 통신망관리기를 결합시켜 구현하였다. 결함의 발견은 동작의 이상을 감시하는 것으로 이루어지는데, 물리계층의 결함은 802.4에 규정되어 있는 논리적 링의 유지 보수 기능을 이용하였다. 이중화된 통신망중 한쪽 통신망으로 전송하고, 양쪽 통신망으로부터 수신하는 구조로 구현되었으며, 통신망의 전환은 전송 통신망의 방향을 바꿈으로써 이루어지고, 전환 기간에 발생될 수 있는 데이타의 손실은 재전송에 의해 복구하였다.

본 논문에서 구현된 결함허용 Mini-MAP 시스템인 RedMAP의 신뢰도 및 평균연속동작시간을 해석하여, 일반 Mini-MAP 시스템과 비교할 때, RedMAP은 신뢰도를 거의 1에 가깝게 계속 유지시킬 수 있고, 평균연속동작시간도 일반 Mini-MAP시스템에 비해 수십~수백배까지 증가시킬 수 있음을 보였다. 따라서, RedMAP은 고신뢰도를 필요로 하는 시스템에 적용될 수 있다. 현재, 서울 당인리 화력발전소 4호기 분산제어시스템[12]에 적용되어 사용중에 있다.

앞으로 남아있는 연구로는 결함 발생시에 발생가능한 데이타의 손실을 줄이는 연구와, 결함 복구후에 결함 원인을 찾아 네트워크를 수리하는 기능에 대한 연구등이 있다.

참 고 문 헌

[1] Michael G. Rodd, Farzin Deravi, *Communication Systems for Indusrial Automation*, Prentice Hall, 1989.

[2] *다수 기업 이종기기간의 접속장치 개발에 관한 연구 최종보고서*, 서울대학교 자동화 시스템 공동 연구소, 1993년 8월

[3] 김 기현, 이 전우, 하 정현, 정 하재, 채 영도, "CIM을 위한 Mini-MAP 네트워크 접속장치의 구현에 관한 연구," *전자공학회논문지, 제 30권 B편 제 10호*, 1993년 10월

[4] Jean-Michel Ayache, Jean-Pierre Courtiat, and Michel Diaz, "REBUS, A Fault-Tolerant Distributed System for Industrial Real-Time Control," *IEEE Trans. on Computers, Vol C-31, No. 7*, July 1982, pp637-647.

[5] *IEEE standards for local area network: Token-passing bus access method and physical layer specifications*, IEEE, Inc., 1985.

[6] *ISO/IEC 8802-4, Information processing systems - Local Area Networks - Part 4 : Token-passing Bus Access Methid and Physical Layer Specification*, IEEE, Inc., 1990.

[7] *IEEE Standards for Local Area Networks: Logical Link Control*, IEEE, Inc., 1985.

[8] Barry W. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems*, Addison-Wesley, 1989.

[9] David A. Rennels, "Fault-Tolerant Computing-Concepts and Examples," *IEEE trans. on Computers, Vol. C-33, No. 12*, Dec. 1984 pp1116-1129.

[10] Yasuhisa Shiobara, Takayuki Matsudaira, Yoshio Sashida and Makoto Chikuma, "Advanced MAP for real-time process control," *Proceedings of IECON*, Cambridge, Messachusetts, Nov. 5-6, 1987, pp883-891.

[11] H. Kleines and K. Zwoll, "MAP Mining-A Communications System for Mining Applications," *EMUG MAP/TOP EVENTS Conference Proceedings, SYSTEC 92*, 1992.

[12] *발전소 보일러의 디지탈 분산 제어 시스템 개발 및 적용(the development and application of digital distributed control system for boiler in the power plant) 기술보고서*, 삼성 데이타 시스템 주식회사,

1991
[13] 문 홍주, "외란이 있는 환경에서의 IEEE 802.4 토큰 전달 방식의 해석," *서울대학교 공학석사 학위본문*, 1993
[14] Athanasios Papoulis, *Probability, Random Variables, and Stochastic Processes*, McGraw Hill, 1984.
[15] Andrew L. Reibman and Malathi Veeraraghavan, "Reliability Modeling: An Overview for System Designers," *IEEE Computer*, April 1991 pp49-57.
[16] Leonard Kleinrock, *Queuing Systems Volume I: Theory*, John Wiley & Sons, Inc., 1975.

저 자 소 개

文 泓 周(正會員)

1968년 5월 22일생. 1991년 서울대 제어계측공학과 졸업(공학사). 1993년 서울대 제어계측공학과 대학원(공학석사). 1993년 ~ 현재 서울대 제어계측공학과 박사과정 재학중. 주관심분야는 이산현상시스템(DES)의 모델링및 해석, 자동화 시스템의 네트워연구, 생산자동화시스템의 구축 등임.

權 旭 鉉(正會員)

1945년 1월 19일생. 1968년 서울대 공대 전기공학과 졸업. 1975년 미국 브라운대 졸업(공학박사). 1976 ~ 77년 미국 아이오아대 객원교수. 현재 서울대 공대 제어계측공학과 교수, 서울대 자동화 시스템 공동연구소 소장, 한국 MAP 사용자 협회 (KMIG) 회장

朴 洪 聖(正會員)

1961년 3월 16일생. 1983년 서울대 제어계측공학과 졸업(공학사). 1986년 서울대 제어계측공학과 대학원(공학석사). 1992년 서울대 제어계측공학과 박사학위 취득. 1983 ~ 90년 삼성전자 연구원. 1992년 ~ 현재 강원대학교 제어계측공학과 조교수