논문 13-38C-12-09 한국통신학회논문지(J-KICS) '13-12 Vol.38C No.12
http://dx.doi.org/10.7840/kics.2013.38C.12.1170

잠수함 전투체계를 위한 이중채널 CAN 버스의 신뢰도 분석

송 무 근◆, 김 은 로*, 이 동 익°

Reliability Analysis of Dual-Channel CAN bus for Submarine Combat System

Moogeun Song◆, Eunro Kim*, Dongik Lee°

요 약

최근 항공기, 잠수함, 로봇 등 고도의 신뢰성이 요구되는 군사무기체계 분야에 상용 필드버스의 적용이 활발히 이루어지고 있다. 잠수함 전투체계 역시 대표적인 군사용 전자 장비로서 다양한 컴퓨터와 센서 및 액추에이터들이 실시간 네트워크로 연결되어 있다. 잠수함의 작전수행능력 및 생존성과 직결되는 전투체계용 네트워크는 매우 높은 수준의 신뢰성을 만족해야 된다. 그 결과 잠수함 전투체계의 구성장비들을 제어하기 위한 필드버스로써 표준 CAN(Controller Area Network)을 기반으로 채널과 제어기를 이중화한 이중채널 CAN 버스가 주로 이용되고 있다. 본 논문에서는 Petri Net을 이용하여 이중채널 CAN 버스의 신뢰도 분석 모델을 제시한다. 기존연구에서는 네트워크를 통한 정보전송 성능 분석에 주안점이 주어졌으나, 본 논문에서는 CAN의 다양한 물리적 고장 유형을 반영하여 GSPN(Generalized Stochastic Petri Nets) 모델을 제안한다. 제안된 모델을 기반으로 고장율과 고장복구율을 변경하면서 각 고장 유형이 이중채널 CAN 버스의 신뢰도에 미치는 영향을 분석한다.

Key Words : GSPN, Dual-CAN, Network, Reliability, Fault Classification

ABSTRACT

Thanks to various benefits, low-cost real-time communication networks so called fieldbus have been widely used in many industrial applications including military systems, such as aircrafts, submarines, and robots. This paper presents a reliability analysis of dual-channel CAN(Controller Area Network) fieldbus which is used for controlling various equipment of submarine combat system. A submarine combat system playing a critical role to the success of missions and survivability consists of various devices including sensors/actuators and computers. Since a communication network for submarine combat system must satisfy an extremely high level of reliability, a dual channel technique is commonly adopted. In this paper, a Petri Net based reliability model for dual-channel CAN is discussed. A reliability model called generalized stochastic Petri Nets (GSPN) is built by utilizing the information on physical faults with CAN. The effectiveness of the proposed model is analyzed in terms of unreliability with respect to failure rate and repair rate.

※ 본 연구는 ㈜삼성탈레스 연구과제(STC-C-10-027) 지원으로 수행되었습니다.
◆ First Author : 경북대학교 IT대학 전자공학부, moogeun.song@gmail.com, 학생회원
° Corresponding Author : 경북대학교 IT대학 전자공학부, dilee@ee.knu.ac.kr, 정회원
* 국방과학연구소 함정전투체계개발단, erkim@add.re.kr
논문번호 : KICS2013-08-355, 접수일자 : 2013년 8월 27일, 심사일자 : 2013년 10월 28일, 최종논문접수일자 : 2013년 12월 6일

Ⅰ. 서 론

필드버스 또는 데이터버스로 불리는 저비용 실시간 통신네트워크는 그 효용성으로 인해 산업계 전반에 널리 사용되고 있다[1-3]. 최근에는 고도의 신뢰성이 요구되는 군사시스템에서도 필드버스가 폭넓게 적용되고 있는데[4], 다양한 무장과 장비들을 제어하는 잠수함 전투체계(submarine combat system)는 대표적인 네트워크 기반 군사시스템이다. 잠수함 전투체계는 20여 개 이상의 다기능 콘솔과 소나 콘솔 등으로 구성되며, 이들은 데이터 네트워크와 제어 네트워크를 통해 서로 연결되어 있다. 데이터 네트워크는 신호처리 및 상황 인지·판단에 필요한 데이터를 전송하기 위한 것으로서 주로 Ethernet 기반의 대용량 네트워크가 사용된다. 반면, 본 논문에서 다루는 제어 네트워크는 각 콘솔의 전원 관리 및 상태 모니터링을 위한 정보와 명령값을 전달하며, CAN[5] 등 실시간 특성이 우수한 필드버스가 주로 사용된다. 전투체계는 잠수함의 작전수행능력 및 생잔성을 결정하는 핵심장비이며, 네트워크의 가용성이 곧 전투체계의 가용성을 좌우하므로, 전투체계에 적용되는 모든 네트워크는 매우 높은 수준의 신뢰도를 만족시킬 필요가 있다. 그러나 앞서 언급한 바와 같이, 최근 개발되는 전투체계는 MIL-STD-1553B 등 신뢰도가 높은 군사용 네트워크가 아니라, Ethernet, CAN 등 상용 네트워크를 주로 활용하며 부족한 신뢰도는 이중화 기법을 통해 개선하고 있다. 네트워크 이중화 기법은 통신제어기, 전송채널 등 네트워크의 주요 요소들을 이중화하여 네트워크의 부분적 고장에 대처할 수 있다. 비교적 적은 추가비용으로 신뢰도를 높일 수 있다는 장점으로 인해 다양한 군사시스템에서 적용되며, 효율적인 이중 네트워크 구현을 위한 연구가 지속적으로 이루어지고 있다[4,6]. 특히 이중화된 네트워크의 신뢰도가 요구수준을 만족하는지 여부를 평가하기 위한 신뢰도 분석 기법에 대한 관심이 매우 높다.

고전적 신뢰도 분석기법[7-10]은 시스템의 시간 의존적 특성이나 실시간 복구 기능을 고려하지 않으므로 이중화 네트워크의 신뢰도 분석에는 적합하지 않다. 반면 신뢰도 분석 다이어그램이나 고장수목(fault tree) 분석 기법은 구성요소의 고장을 구체적으로 표현할 수 있지만 동시성 및 동기화 기능 등에 있어서 제약이 따른다[11]. 이러한 문제점을 해결하기 위한 대안으로 Petri Net의 일환인 GSPN(Generalized Stochastic Petri Nets) 기법이 사용되고 있다[12]. 특히 참고문헌[4]에서는 GSPN 기법과 시스템 구성요소의 고장복구(repair) 시간을 이용하여 잠수함 전투체계용 이중화 Ethernet의 신뢰도를 정량적으로 분석하였다. 그러나 잠수함의 특성상 장기간 작전수행 중에는 고장복구가 지연될 수 있음을 고려하지 않았으므로 네트워크 신뢰도가 실제보다 높게 평가되는 문제점이 있다.

본 논문에서는 GSPN 기법을 이용하여 잠수함 전투체계의 제어 네트워크로 개발된 이중화 CAN의 신뢰도 분석 모델을 제안한다. 기존연구와 달리, 제안한 모델은 잠수함의 작전수행에 따른 고장수리 지연을 네트워크 신뢰도 분석에 반영하였다. 먼저 CAN의 물리적 고장들에 대해 함내에서 수리 및 복구가 가능한 고장과, 함내 수리가 불가능하여 기지로 귀환 후 복구할 수 있는 고장으로 분류하고, 이를 기반으로 GSPN 모델을 제시한다. 예를 들어, 기지로 귀환하기까지 잔여시간을 d로 가정하고, 함내 복구가 불가능한 임의의 고장 f의 평균수리시간이 h로 주어졌다면, 고장 f의 실제 복구시간은 (h+d)로 변경하여 신뢰도 분석에 적용한다. 이어서, Petri Net 모델을 CTMC(Continuous Time Markov Chain) 모델로 변환하고 이를 바탕으로 신뢰도 함수를 도출한다. 제안된 모델의 효용성을 확인하기 위해서 함내 복구가 불가능한 고장의 고장복구율(repair rate)을 작전수행 기간을 고려하여 변경하면서 이중화 CAN의 신뢰도를 분석하고 그 결과를 기존연구 결과[4]와 비교하여 제시한다.

Ⅱ. 네트워크 고장의 특징을 반영한 GSPN 모델

2.1. 잠수함 전투체계 제어를 위한 CAN 버스

일반적으로 잠수함 전투체계의 제어를 위한 통신네트워크는 다음과 같은 요구사항을 만족할 수 있어야 한다: 짧고 주기적인 메시지 전송에 최적화, 확정적(deterministic) 전송특성, 낮은 지터(jitter), 충분한 전송거리, 높은 수준의 전송 신뢰도 및 전송오류 인식률, 자동고장복구 기능, 메시지 우선순위 할당 기능, 다중마스터 아키텍처 지원 등. 그 밖에 저렴한 비용, 다양한 제품군과 기술지원 가능 여부도 필수적인 요구사항이다. 그러나 이런 특성들을 동시에 만족할 수 있는 군사용 네트워크는 찾아보기 어려운 실정이다[13]. 반면, 1980년대부터 자동차 산업을 중심으로 상기 특성을 만족하는 상용 필드버스에 대한 연구가 진행되었으며 그 대표적인 결

과물이 독일 Bosch사에서 차량제어용으로 개발한 CAN[5] 버스이다. 이후 CAN 버스는 자동차 뿐 아니라 유사한 요구특성을 갖는 제트엔진[13], 풍력발전기[14], 잠수함[15] 등의 제어를 위해 폭넓게 적용되고 있다. 이러한 배경에서 본 연구의 대상인 잠수함 전투체계의 제어를 위해 상용 CAN 버스를 채택하고 있다. 아울러, 잠수함이 운용되는 외부 환경은 매우 열악하지만, 전투체계는 해군 승조원이 상주하는 구역에 설치되므로 일상적인 온도, 진동, 습도 등의 환경조건과 크게 다르지 않다는 점도 상용 CAN 버스의 적용이 가능한 이유이다. 다만 전투체계는 잠수함의 작전 수행 능력과 생잔성에 직접 영향을 미치는 핵심장비이므로 표준 CAN 버스의 이중화를 통해 신뢰도를 개선시켰다. 따라서 본 논문에서는 일반적인 운용환경이라는 가정하에 이중화 CAN의 신뢰도 모델을 제시하고자 한다.

2.2. CAN 버스 고장 분석

일반적으로 CAN을 포함한 네트워크 기반 시스템에서 발생하는 고장은 다음과 같이 세 가지로 분류된다.

- 노드 고장: 모듈단위의 연산장치 또는 송수신 장치에서 발생하는 물리적 고장
- 통신 채널(미디어) 고장: 케이블 절단 또는 합선
- 통신 메시지 오류: 비트 오류, 과도한 전송지연

통신채널 고장은 네트워크의 물리적 결함으로 인해 발생하며 일시적 또는 영구적으로 이상 상태가 지속될 수 있다. 반면, 통신 메시지 오류는 EMI 및 전원의 간섭 등 외란으로 인해 발생하는 일시적 패킷오류 또는 분실이며, 이중화 네트워크의 경우 비교적 쉽게 극복 가능하다. 노드 고장의 경우 CPU, 메모리 등 통신 네트워크와 직접 관련이 없는 연산장치의 결함으로 인해 발생하는 경우가 대부분이다. 따라서 본 논문에서는 그림 1에 나타낸 통신채널의 물리적 결함에 대해서만 고려한다.

본 논문에서 다루는 이중화 CAN 네트워크는 동일한 특성을 갖는 표준 CAN 채널과 통신제어기를 이중으로 적용한 구조이므로, 각 채널에서 발생 가능한 물리적 고장은 그림 1에 제시한 단일 CAN의 경우와 동일하다고 가정할 수 있다[6]. 즉 각 채널의 물리적 고장들은 케이블 단선(A, B), 전원 단락(C, D), 접지 단락(E, F), 신호선간의 단락(G), 종단저항 파괴(H) 등으로 분류되며, 이중화 CAN의 경우 이러한 고장들이 각 채널에서 독립적으로 발생한다. 각 채널에서 발생한 물리적 고장은 해당 네트워크의 장애로 이어진다. 즉 표1에 요약한 것처럼 물리적 고장 발생시 네트워크에 미치는 결과로는 노드 간의 연결이 끊어지는 네트워크 분리, 통신패킷의 분실, 통신채널의 상태가 고정되는 "Stuck-at" 등을 유발한다[4].

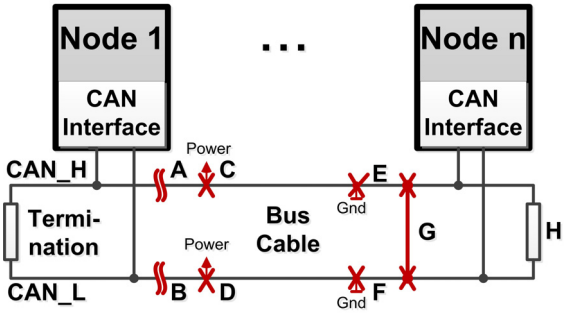

그림 1. CAN 버스(단일 채널)의 물리적 고장
Fig. 1. Physical faults of CAN bus(single channel)

표 1. 표준 CAN 버스의 물리적 고장과 그에 따른 네트워크 이상 상태
Table 1. Physical bus faults and their effects on CAN

fault position	fault mode	fault effect
A, B	cable open	partition, packet loss
C, F	cable short to power or ground	stuck-at-recessive
D, E		stuck-at-dominant
G	cable short each	packet loss
H	termination error	packet loss

한편, 각 고장별 평균수리시간은 일반적으로 상수로 주어지며, 예상치 못한 환경 요인에 의해 발생하는 수리작업의 지연은 평균수리시간 산정시 반영되지 않는다. 그런데, 잠수함의 경우 네트워크 케이블이 설치된 함내 공간 및 접근성 제약 등으로 인해 잠수함이 기지에 정박 중인 상태에서만 수리작업이 가능한 고장에 대한 고려가 필요하다. 예를 들면, 작전 수행 중에 케이블 단선 고장이 발생한 경우, 주어진 평균수리시간 외에도 기지로 귀환할 때까지 수리작업이 지연된 시간도 함께 고려되어야 한다. 따라서 CAN의 물리적 고장을 함내에서 즉시 수리 가능한 고장(f_{ON})과 반드시 기지에 정박 중인 상태에서만 수리 가능한 고장(f_{OFF})으로 세분화할 필요가 있다. 편의상 f_{ON}과 f_{OFF}를 '함내 복구가능 고장'과 '함내 복구불가능 고장'으로 부르기로 한다.

다만, 잠수함의 설계 및 제작이 아직 진행 중인 점을 고려하여 본 논문에서는 각 고장들을 f_{ON}과 f_{OFF}로 확정하지 않은 상태에서 신뢰도 모델을 도출한다.

2.3. 전투체계 네트워크 모델링

신뢰도 분석 다이어그램, 고장수목 분석 기법 등 일반적인 신뢰도 분석 기법들[7-11]은 시간 의존성과 고장복구 기능의 반영이 어렵거나 동기화 기능의 사용에 제약이 따르는 등 이중화 네트워크의 신뢰도 분석에 적용하기에 어려움이 따른다. 반면, Petri Net은 순서도나 블럭다이어그램 같은 도식적 도구로 시각적 의사소통을 가능하게 해줄 뿐 아니라 견고한 이론적 배경을 갖는 모델링 도구이다. 특히 Stochastic Petri Net(SPN)은 CTMC와 동일한 형태임이 증명되어 다양한 시스템의 성능 및 신뢰도 분석에 사용되고 있다[16][17]. 본 논문에서는 SPN에 즉시천이 기능이 추가된 GSPN을 이용하여 전투체계 이중화 CAN 네트워크를 모델링하고 신뢰도 함수를 정의한다.

2.3.1. 전투체계 제어 네트워크의 구성

본 논문에서 다루는 전투체계 제어 네트워크는 분산처리 구조를 이루는 구성장비 간의 실시간성, 생잔성, 가용성 향상을 위해 그림 2와 같이 버스 토폴로지를 갖는 표준 CAN을 이중화한 형태로 구성된다. 일반적으로 이중채널 시스템의 운영은 두 채널을 동일한 형태로 병행 사용하는 hot-standby, 주·부 채널로 기능을 구분하여 병행 사용하는 warm-standby, 그리고 하나의 채널만 사용하다가 고장시 다른 채널로 전환되는 cold-standby 등으로 구분된다[19]. 본 논문에서는 채널의 일부에서 고장이 발생하더라도 채널 전환을 위한 지연이 발생하지 않는 hot-standby 기법을 적용한다.

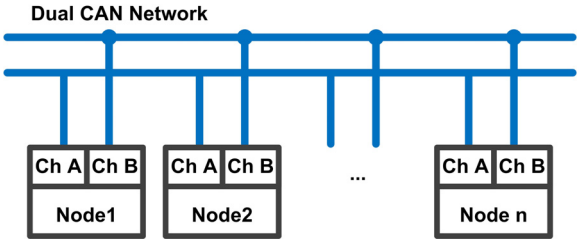

그림 2. 이중화 CAN 기반의 잠수함 전투체계 네트워크
Fig. 2. Dual CAN network for submarine combat system

네트워크의 신뢰도는 성공적인 통신을 위해 노드 사이에 유효한 경로가 존재함을 의미한다. 두 채널의 버스 토폴로지로 구성된 전투체계 네트워크에서 성공적인 통신을 위해서는 최소 한 개의 무결함(즉 유효한 경로) 채널을 필요로 하며, 무결함 채널이 존재하지 않는 경우 네트워크가 다운(down)된 것으로 간주한다. 앞서 제시한 CAN의 물리적 고장들은 독립적인 확률을 가지므로 단독으로 혹은 동시에 발생할 수 있다. 이러한 특성을 적용하면 다음의 조건에서 네트워크 다운이 발생함을 알 수 있다.

$$(f_{OFF,A} \text{ or } f_{ON,A}) \cap (f_{OFF,B} \text{ or } f_{ON,B}) \tag{1}$$

$f_{OFF,A}$, $f_{ON,A}$, $f_{OFF,B}$, $f_{ON,B}$는 순서대로 채널 A의 함내 복구불가능 고장, 채널 A의 함내 복구가능 고장, 채널 B의 함내 복구불가능 고장, 그리고 채널 B의 함내 복구가능 고장을 각각 의미한다. 본 논문에서는 채널의 물리적인 조건이 동일하다고 가정하고, 함내 복구불가능 고장인 $f_{OFF,A}$, $f_{OFF,B}$의 고장율은 λ_{OFF}, 함내 복구가능 고장인 $f_{ON,A}$, $f_{ON,B}$,의 고장율은 λ_{ON}로 표기한다. 함내 복구불가능 고장의 복구율(repair rate) μ_{OFF}은 식(2)와 같이 해당 고장의 평균수리시간 h_{OFF}와 기지로 귀환하기까지 잔여시간 d의 함수로 표현한다.

$$\mu_{OFF} = \frac{1}{(h_{OFF}+d)} \tag{2}$$

함내 복구가능 고장의 복구율 μ_{ON}은 식(2)와 유사하게 해당 고장의 평균수리시간 h_{ON}을 이용하여 다음과 같이 나타내며, 여기서 d=0으로 주어진다.

$$\mu_{ON} = \frac{1}{(h_{ON}+d)} \tag{3}$$

2.3.2. GSPN 모델링

Petri Net은 원으로 표현되는 장소(place)와 막대로 표현되는 천이(transition)로 구성되는 이분(bipartite) 그래프이다. 각 장소는 토큰을 가질 수 있고 토큰의 천이에 의해 다른 장소로 이동한다. GSPN에서 천이는 즉시천이와 시간천이로 구분되며, 즉시천이는 시간천이보다 항상 우선한다. 앞서 제시한 CAN의 물리적 고장 상태를 고려하여 작성된 이중화 CAN 기반 전투체계 네트워크의 GSPN 모델을 그림 3에 나타내었다.

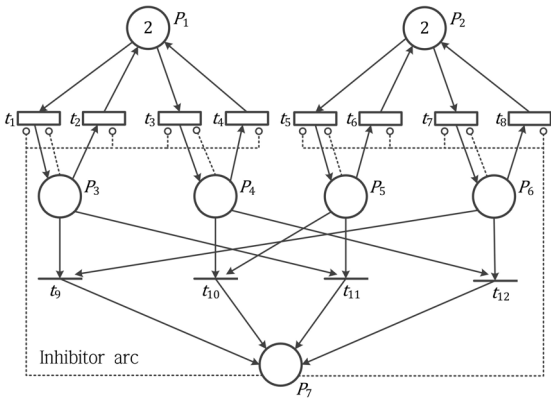

그림 3. 이중화 CAN 네트워크의 GSPN 모델
Fig. 3. GSPN model of dual CAN network

장소 P_1과 P_2는 각각 채널 A와 채널 B의 고장이 없는 상태를 나타낸다. 함내 복구가능 고장의 발생을 시간천이 t_1와 t_5로 표현하였고, 각 채널의 함내 복구가능 고장상태를 P_3와 P_5로 표현하였다. 그리고 함내 복구불가능 고장의 발생을 시간천이 t_3와 t_7로, 각 채널의 함내 복구가능 고장 상태를 P_4와 P_6로 각각 표현하였다. 함내 복구가능 고장 상태에 대한 고장 복구율은 시간천이 t_2과 t_6로 표현하였다. 함내 복구불가능 고장상태에 대한 고장 복구율은 시간천이 t_4과 t_8로 표현하였다. 네트워크의 다운 조건인 식 (1)은 즉시천이 t_9, t_{10}, t_{11}, t_{12} 으로 나타내었으며, 이로 인한 네트워크의 다운은 장소 P_7으로 표현할 수 있다. 화살표 모양의 끝으로 표현된 아크는 상태천이의 방향을 나타내고 토큰의 이동 경로를 표현한다. 원형 모양의 끝으로 표현된 아크는 금지아크를 가리키며, 이는 현재 장소에 토큰이 존재할 경우 해당 천이가 금지됨을 의미한다. 각 채널의 정상상태에서는 영구적 고장과 일시적 고장이 모두 발생할 수 있는데, 이를 표현하기 위해 정상상태에서는 장소 P_1, P_2에 2개의 토큰을 갖는다. 영구적 고장 또는 일시적 고장으로 인한 상태는 오직 하나이므로 각각의 고장상태 장소는 각 고장 상태로 향하는 아크를 가진 천이에 금지 아크를 갖는다. 네트워크의 다운 조건이 충족될 경우 장소 P_7에 토큰이 생성된다. 실제 네트워크 다운이 발생하면 제안된 모델에서는 모든 상태 천이를 멈춘다.

Ⅲ. 네트워크 고장특징을 반영한 신뢰도 모델 설계

3.1. 신뢰도 함수 도출을 위한 모델 변환

각 장소에서의 토큰의 수를 마킹 $m(P_i)$로 표현할 수 있다. 여기서 P_i는 Petri Net 모델의 장소를 의미한다. 각각의 장소에 대한 마킹 정보는 마킹 집합 벡터 $M_i = [m(P_1), m(P_2), ..., m(P_n)]$으로 표현된다. 이때 n은 Petri Net 모델의 장소의 총 수를 의미 한다. 초기상태의 마킹 집합에서 천이에 따라 도달가능한 모든 마킹 집합을 표현한 것이 도달성 트리(Reachability Tree)이다. 도달성 트리를 이용하면 SPN은 CTMC 모델로 변환이 바로 이루어 질 수 있으며, GSPN 모델의 경우에는 즉시천이로 인해 발생하는 마킹의 집합을 제거할 경우 CTMC 모델로 변환이 가능하다. 앞서 도출된 전투체계 네트워크 모델의 도달성 트리와 각 마킹에 대한 정보를 아래에 표2와 표3으로 나타내었다. 마킹 벡터 M_0는 모델에서 각 장소의 초기 토큰의 수를 나타내며, 각 원소들은 순서대로 장소 $P_1, P_2, ..., P_7$의 토큰의 수를 의미한다.

표 2. 이중화 CAN 네트워크 모델의 도달성 트리
Table 2. Reachability tree of dual CAN network

marking of departure	transition of fired	marking of arrival
M_0	t_1, t_3, t_5, t_7	M_1, M_2, M_3, M_4
M_1	t_2, t_3, t_5, t_7	M_0, M_5, M_6, M_7
M_2	t_1, t_4, t_5, t_7	M_5, M_0, M_8, M_9
M_3	t_1, t_3, t_6, t_7	M_6, M_8, M_0, M_{10}
M_4	t_1, t_3, t_5, t_8	M_7, M_9, M_{10}, M_0
M_5	t_2, t_4, t_5, t_7	M_1, M_2, M_{11}, M_{12}
M_6	t_{11}	M_{13}
M_7	t_9	M_{13}
M_8	t_{10}	M_{13}
M_9	t_{12}	M_{13}
M_{10}	t_1, t_3, t_6, t_8	M_{14}, M_{15}, M_4, M_3
M_{11}	t_{10}, t_{11}	M_{16}, M_{17}
M_{12}	t_9, t_{12}	M_{17}, M_{16}
M_{14}	t_9, t_{11}	M_{18}, M_{19}
M_{15}	t_{10}, t_{12}	M_{19}, M_{18}

위의 도달성 트리는 즉시천이가 포함되어 있으므로 엄밀하게 말하면 확장된 도달성 트리(extended reachability tree)이다[16]. 확장된 도달성 트리에는 즉시천이로 인한 숨겨진 마킹(vanishing marking)을 포함한다. 숨겨진 마킹을 제거함으로써 단순한 도달성 트리로 변환이 가능하고 이는 CTMC와 동형을

이루게 된다[16]. 그림 4는 참고문헌[16-18]에 제시된 방법에 의해 숨겨진 마킹을 제거하여 CTMC 모델을 도식화한 것이다.

표 3. 도달성 트리의 마킹 정보
Table 3. Information on marking M_i from reachability tree

marking M_i	
$M_0=[2,2,0,0,0,0,0]$	$M_1=[1,2,1,0,0,0,0]$
$M_2=[1,2,0,1,0,0,0]$	$M_3=[2,1,0,0,1,0,0]$
$M_4=[2,2,0,0,0,1,0]$	$M_5=[0,2,1,1,0,0,0]$
$M_6=[1,1,1,0,1,0,0]$	$M_7=[1,1,1,0,0,1,0]$
$M_8=[1,1,0,1,1,0,0]$	$M_9=[1,1,0,1,0,1,0]$
$M_{10}=[2,0,0,0,1,1,0]$	$M_{11}=[0,1,1,1,1,0,0]$
$M_{12}=[0,1,1,1,0,1,0]$	$M_{13}=[1,1,0,0,0,0,1]$
$M_{14}=[1,0,1,0,1,1,0]$	$M_{15}=[1,0,0,1,1,1,0]$
$M_{16}=[0,1,1,0,0,0,1]$	$M_{17}=[0,1,0,1,0,0,1]$
$M_{18}=[1,0,0,0,1,0,1]$	$M_{19}=[1,0,0,0,0,1,1]$

상태 M_0는 모델의 초기상태를 의미한다. $M_{13}, M_{16}, M_{17}, M_{18}, M_{19}$는 GSPN 모델의 장소 P_7에 토큰이 도달한 상태를 나타낸다. 상태 M_5는 한 쪽 채널에 함내 복구불가능 고장과 함내 복구가능 고장이 동시에 발생한 경우로, 반대 채널에 복구불가능 고장 또는 복구가능 고장이 발생하게 되면 상태 M_{16} 또는 M_{17}로 천이한다. 이때 2가지 즉시천이가 활성화 되며, 동시에 활성화되는 즉시천이들은 어떤 확률로 천이되는데 동시에 활성화되는 즉시천이들의 확률의 합은 1이다. 본 논문에서는 각 채널의 특성을 동일하게 설계하므로 각각의 즉시천이 활성화 확률을 0.5로 가정한다.

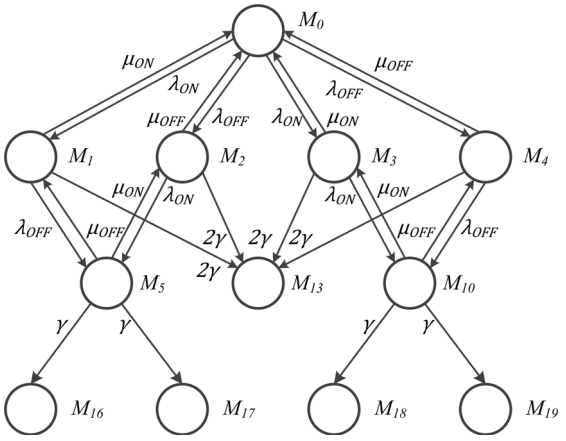

그림 4. 이중화 CAN 네트워크의 CTMC 모델
Fig. 4. CTMC model for dual CAN network

3.2. 신뢰도 함수 도출

이중화 CAN 기반 전투체계 네트워크의 신뢰도 함수는 다음 식으로 표현할 수 있다.

$$R(t)=P(system\,is\,operational\in[0,t]) \quad (4)$$

X를 시스템의 수명시간을 나타내는 랜덤변수로 두고, $F(t)$를 X에 대한 누적 분포함수로 두면 다음과 같다:

$$R(t)=P(X>t)=1-F(t) \quad (5)$$

식 (5)을 보면 $F(t)$는 비신뢰도 함수로 나타나는 것을 알 수 있다.

본 논문에서 도출한 CTMC 모델을 살펴보면 $M_{13}, M_{16}, M_{17}, M_{18}, M_{19}$ 에서 시스템 정지상태가 되는 것을 알 수 있다. 시스템 정지상태를 집합 $\Phi=\{M_{13}, M_{16}, M_{17}, M_{18}, M_{19}\}$ 로 정의할 수 있다. CTMC 모델의 각각의 상태확률은 독립적이므로, 시스템 정지상태의 집합 Φ에 속한 모든 상태의 확률의 합으로 나타낼 수 있다.

$$F(t)=\sum_i P_{\Phi(i)}(t) \quad (6)$$

식(5)과 식(6)에 의해 신뢰도 함수 $R(t)$은 다음 식으로 주어진다.

$$R(t)=1-\sum_i P_{\Phi(i)}(t) \quad (7)$$

시스템의 신뢰도 함수는 전체확률 1에서 시스템의 비신뢰 확률의 차로 구할 수 있고, 시스템의 비신뢰 확률은 시스템 정지상태 확률의 합으로 나타낸다.

시스템 정지상태의 확률 함수는 CTMC 과도상태 해석을 수행하여 얻는다. CTMC에 표현된 각 상태에 대한 과도확률은 극소생설기 행열 Q와 과도확률의 미분방정식으로 표현된다. 즉 상태의 과도확률함수 $P_{\Phi(i)}(t)$는 다음과 같다.

$$\frac{dP_{\Phi(i)}(t)}{dt}=P_{\Phi(i)}(t)\,Q \quad (8)$$

$$P_{\Phi(i)}(0)=\pi_0 \quad (9)$$

위 식에서 Q 와 π_0 는 행렬이며, 다음의 가정으

로 구해질 수 있다.

- 시스템의 초기 상태는 고장이 발생하지 않은 상태이다.
- 함내 복구가능 고장, 함내 복구불가능 고장은 서로 독립적이다.
- 함내 복구가능 고장 및 복구불가능 고장에 대한 고장율과 복구율은 각각 $\lambda_{ON}, \lambda_{OFF}, \mu_{ON}, \mu_{OFF}$이다.

상기 가정으로 인해 극소생성기 행렬 Q와 π_0의 값은 아래와 같이 주어진다.

$$\pi_0 = [1,0,0,0,0,0,0,0,0,0,0,0]$$

$$Q = \begin{bmatrix} \alpha_1 & \lambda_{ON} & \lambda_{OFF} & \lambda_{ON} & \lambda_{OFF} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mu_{ON} & \alpha_2 & 0 & 0 & 0 & \lambda_{OFF} & 2\Upsilon & 0 & 0 & 0 & 0 & 0 \\ \mu_{OFF} & 0 & \alpha_3 & 0 & 0 & \lambda_{ON} & 2\Upsilon & 0 & 0 & 0 & 0 & 0 \\ \mu_{ON} & 0 & 0 & \alpha_4 & 0 & 0 & 2\Upsilon & \lambda_{OFF} & 0 & 0 & 0 & 0 \\ \mu_{OFF} & 0 & 0 & 0 & \alpha_5 & 0 & 2\Upsilon & \lambda_{ON} & 0 & 0 & 0 & 0 \\ 0 & \mu_{OFF} & \mu_{ON} & 0 & 0 & \alpha_6 & 0 & 0 & \Upsilon & \Upsilon & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha_7 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mu_{OFF} & \mu_{ON} & 0 & 0 & \alpha_8 & 0 & 0 & \Upsilon & \Upsilon \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{10} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{11} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{12} \end{bmatrix}$$

숨겨진 마킹을 제거하는 방법[16]에 의해 γ값이 정의되고, 극소생성기 행렬에서 α_i값이 추가 되었다. 각각은 식 (10)와 식 (11)으로 정의 된다.

$$\gamma = \frac{1}{2}(\lambda_{ON} + \lambda_{OFF}) \tag{10}$$

$$\alpha_i = -\sum_j Q_{ij} \tag{11}$$

본 논문에서는 정의된 과도확률을 구하기 위한 방법으로 복잡한 다변수 연립 미분방정식을 풀이 대신, 수치적 해석 방법을 수행하였다.

Ⅳ. 네트워크 신뢰도 모델의 이론적 분석

본 논문에서는 두 개의 채널에서 함내 복구가능 고장 또는 함내 복구불가능 고장이 동시에 발생하지 않을 확률을 신뢰도로 정의하였다. 본 장에서는 앞서 제시한 신뢰도 함수 식 (7)를 이용해 네트워크에서 각 채널의 고장에 따른 시스템의 신뢰도를 산출한다. 우선 본 논문에서 제안한 네트워크 신뢰도 모델을 검증하기 위해, 기존의 신뢰도 모델[4]과 신뢰도 분석 결과를 비교한다. 기존의 신뢰도 모델의 경우, 함내 복구불가능 고장을 고려하지 않았기 때문에, λ, μ를 λ_{ON}, μ_{ON}에 각각 대응시킬 수 있으며, μ_{OFF}은 잠수함의 기지귀환 지연시간을 0으로 가정하여 μ_{ON}과 같은 값으로 설정하였다. 제안된 방법과 기존 방법의 비교를 위해 함내 복구불가능 고장의 복구율 λ_{OFF}을 0에서 증가시키며 분석하였다.

시뮬레이션에 사용되는 λ_{ON}, μ_{ON}의 값은 참고문헌[4]에서 사용된 파라미터를 참고하였다. 값을 고정시킨 파라미터 $\lambda_{ON}, \mu_{ON}, \mu_{OFF}$은 각각 1.0e-4, 1.0e-2, 1.0e-2으로 설정하였다. 그림 5를 보면 λ_{OFF} 값이 0일 때, 기존의 신뢰도 모델과 제안된 신뢰도 모델의 결과가 일치함을 볼 수 있다. 또한 λ_{OFF} 즉 함내 복구불가능 고장의 발생이 증가함에 따라 기존의 신뢰도 모델의 결과 보다 보수적인 결과를 나타내었다. 따라서 제안한 신뢰도 모델은 기존의 신뢰도 모델을 포함하는 확장된 신뢰도 분석 모델임을 확인할 수 있다.

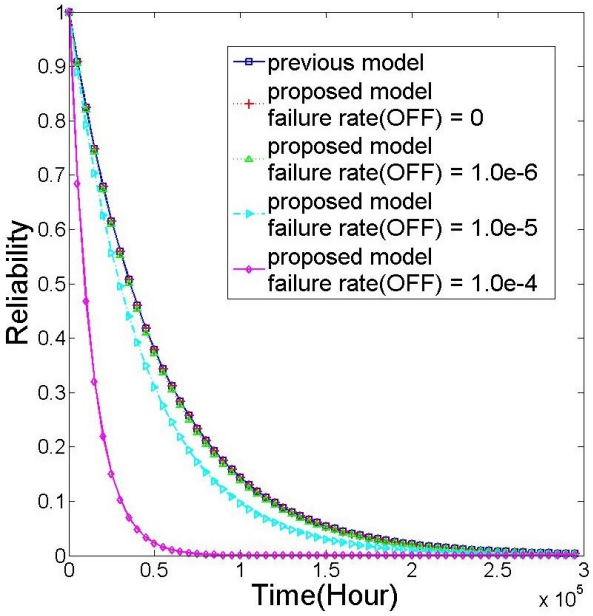

그림 5. 고장율 증가에 따른 신뢰도 비교
Fig. 5. Reliability according to failure rate

작전수행 후 기지귀환까지 잔여시간에 따른 신뢰도 분석을 위해, $\lambda_{ON}, \lambda_{OFF}, \mu_{ON}$의 값을 고정 시킨 채 μ_{OFF}값만 변화시킨다. μ_{ON}과 μ_{OFF}은 식(2)와 식(3)으로 표현되는데, 이 때 각 고장 종류에 대한 평균수리시간 h_{ON}, h_{OFF}의 값을 같다고 가정하고, 작전수행 후 귀환 잔여시간 d는 최소 1일에서 최대 15일로 설정하였다. 이때 설정된 $\lambda_{ON}, \lambda_{OFF}, \mu_{ON}$의 값은 각각 1.0e-4, 1.0e-4, 1.0e-1 이다. 그림 6에서, 작전수행 후 귀환 잔여시간이 길어질수록 신뢰도 값이 현저히 빠르게 감소함을 확인할 수 있다. 따라

서 작전수행 기간이 긴 잠수함 등의 군사시스템은 짧은 작전수행 기간을 갖는 근해용 선박에 비해 높은 수준의 네트워크 신뢰도가 요구됨을 알 수 있다.

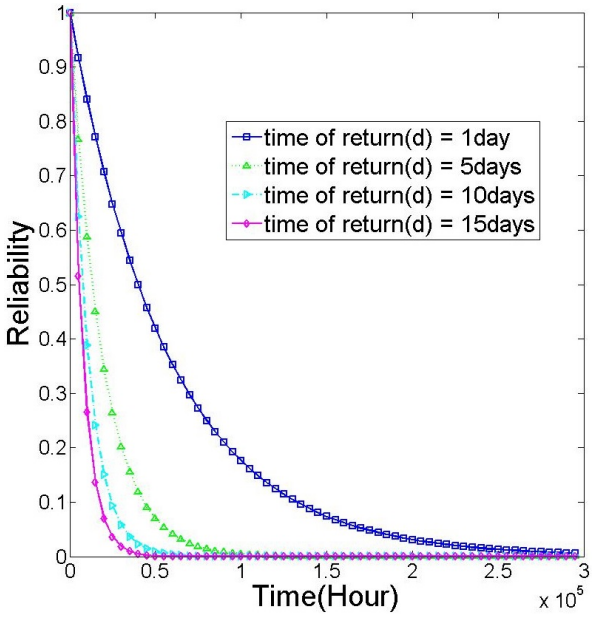

그림 6. 기지 복귀 잔여시간 증가에 따른 신뢰도
Fig. 6. Reliability according to time-of-return

V. 결 론

본 논문에서는 잠수함의 작전수행 기간을 고려하여 이중화 CAN 기반 전투체계 제어 네트워크의 신뢰도를 분석할 수 있는 GSPN 모델을 제안하였다. 제안한 모델에서는, 이중화 CAN에서 발생 가능한 고장을 함내에서 즉시 수리 가능한 고장과, 기지에 정박한 상태에서만 수리할 수 있는 고장으로 세분화하여 고장율과 복구율을 반영하였다. 모든 고장을 즉시 수리 가능한 것으로 가정하였던 기존 방법과 본 논문의 신뢰도 모델을 비교한 결과, 잠수함의 작전수행 기간에 따라 더 높은 수준의 네트워크 신뢰도가 요구됨을 알 수 있었으며, 아울러 제안된 모델은 기존 모델을 포함하는 확장된 모델로 볼 수 있음을 확인하였다. 향후 연구주제로써 이중화 네트워크의 운영방식과 채널의 고장검출 및 자동복구 알고리즘 특성에 따른 네트워크 신뢰도 분석을 수행할 예정이다.

References

[1] H. T. Dorissen and K. Durkopp, "Mechatronics and drive-by-wire systems: advanced non-contacting position sensors," *Control Engineering Practice*, vol.11, no.2, pp.191-197, Feb. 2003.

[2] S. M. Kim, P. H. Anh, J. M. Lee, "Fault Tolerant Ethernet Techniques of High-tech Weapon Systems," *Information and Communications Magezine*, vol. 26, no. 3, pp. 69-75, Feb. 2009.

[3] T. Hiaroka, S. Eto, O. Nishihara, H. Kumamoto, "Fault tolerant design for x-by-wire vehicle," *SICE 2004 Annual Conference*, pp.1940-1945, Aug. 2004.

[4] H. S. Kim, "Study on the reliability analysis for fault-tolerant dual ethernet," *Journal of the KIMST*, vol.10, no.2, pp.107-114, Jun. 2007.

[5] ISO 11898, Road vehicles - interchange of digital information - Controller Area Network(CAN) for high-speed communication, *International Standards Organisation(ISO)*, Nov, 1993.

[6] J. Rufino, *Technical Report CSTC Technical Report RT-98-02*, Instituto Superior Tecnico NavIST Group, 1998.

[7] Sheldon B. Akers, "Binary decision diagram," *IEEE Trans. Computers*, vol.100, no.6, pp.509-516, Jun. 1978.

[8] S. Rai, K. K. Aggarwal, "An efficient methods for reliability evaluation of a general networks," *IEEE Trans. Reliability*, vol.27, no.3, pp.206-211, Aug. 1978.

[9] J. A. Abraham, "An improved algorithm for network reliability," *IEEE Trans. Reliability*, vol.28, no.1, pp58-61, Apr. 1979.

[10] S. Hariri, C. S. Raghavendra, "SYREL : A symbolic reliability algorithm based on path and cutset methods," *IEEE Trans. Reliability*, vol.35, no.10, pp.1224-1232, Oct. 1987.

[11] Malhotra, M. and Ciardo, G. and Trivedi, K. S., "Dependability modeling using Petri-nets," *IEEE Trans. Reliability*, vol.44, no.3, pp.428-440, Sep. 1995.

[12] A. Ajmone-Marsan, G. Balbo, "A class of generalized stochastic Petri nets for the performance evaluation multiprocessor

systems," *ACM Trans. Comp. Systems*, vol.2, no.2, pp.93-122, May. 1984.

[13] H.A.Thompson, et al., "A CAN based safety critical distributed aeroengine control systems architecture demonstrator," *Microprocessors and Microsystems*, vol.23, pp.345-355, Nov. 1999.

[14] M.A.Parker, Li Ran, S.J.Finney, "Distributed Control of a Fault-Tolerant Modular Multilevel Inverter for Direct-Drive Wind Turbine Grid Interfacing," *IEEE Trans. Industrial Electronics*, vol.60, no.2, pp.509-522, Feb. 2013.

[15] J. Blandin, P.Leon "Network architectures for underwater systems: two applications of the CAN bus," *Proc. OCEANS'98*, pp.503-507, Oct. 1998.

[16] G. Ciardo, *Analysis of large stochastic Petri net models*, PhD thesis, Duke University, 1989.

[17] G. Chiola, *GreatSPN users' manual technical report*, Dipartimento di Informatica, Universita degli studi di torino, 1987.

[18] M. A. Marsan, G. Balbo, G. Ciardo, and G. Conte, *Modelling techniques and tools for performance analysis*, Elsevier Science Publishers, pp.155-170, 1985.

[19] I.Koren, C.M.Krishna, *Fault-Tolerant Systems*, Elsevier Science Publishers, 2007.

송 무 근 (Moogeun Song)

2008년 2월 경북대학교 전자 전기컴퓨터학부 졸업

2010년 2월 경북대학교 전자전기컴퓨터학부 석사

2010년 3월~현재 경북대학교 전자공학부 박사과정

<관심분야> 고신뢰성 임베디드 시스템, 필드버스 네트워크, 신뢰도 분석

김 은 로 (Eunro Kim)

1992년~현재 국방과학 연구소 함정전투체계 개발단 책임연구원

<관심분야> 소프트웨어 프로세서 개선 및 신뢰성

이 동 익 (Dongik Lee)

1987년 8월 경북대학교 전자공학과 졸업

1990년 2월 경북대학교 전자공학과 석사

1990년 3월~1997년 8월 국방과학연구소 연구원

1997년 9월~2002년 4월 영국 셰필드대학교 자동제어시스템공학과 박사

2002년 1월~2005년 3월 영국 DRTS Ltd 공동설립 및 CTO

2005년~현재 경북대학교 전자공학부 부교수

<관심분야> 고장대처 제어, 시스템 안전, 고장진단, 산업용 네트워크, 풍력 발전기, 지능형 자동차