사이버테러를 고려한 U-Service 생존성의 정량적 평가 방안

김성기*

요 약

유비쿼터스 서비스(U-service)를 제공하는 시스템은 서비스 생존성이 취약한 환경을 극복해야하는 네트워크 시스템이다. 네트워크 시스템의 생존성은 시스템 구성요소에 장애나 사고, 물리적 공격이 발생하더라도 시스템에 부여된 본연의 서비스를 중단 없이 제공할 수 있는 시스템 능력으로 정의하고 있다. 본 논문에서는 비잔틴 장애를 초래하는 의도적인 사이버테러가 네트워크 시스템에 가해졌을 때의 상황을 고려하여, 사용자 입장에서 서비스 생존성을 정량적으로 평가 할 수 있는 프레임워크를 제시한다. 본 논문에서는 무선 LAN 기반의 Jini 시스템을 생존성 정량화 모델의 예로 삼는다. 그리고 Jini 시스템이 제공하는 U-service의 생존성을 평가하기 위한 연속시간 마코프 모델을 제시하고 이를 토대로 사용자가 서비스에 접근할 수 없는 확률(blocking probability)로서 U-service 생존성을 평가하는 방안을 제시한다.

An Approach to a Quantitative Evaluation of U-Service Survivability Reflecting Cyber-terrorism

Sung-Ki Kim*

ABSTRACT

A system that provides a ubiquitous service is a networked system that has to overcome their circumstances that the service survivability is weak. the survivability of a networked system is defined as an ability of the system that can offer their services without interruption, regardless of whether components comprising the system are under failures, crashes, or physical attacks. This paper presents an approach that end users can obtain a quantitative evaluation of U-service survivability to reflect intended cyber attacks causing the networked system to fall into byzantine failures in addition to the definition of the survivability. In this paper, a Jini system based on wireless local area networks is used as an example for quantitative evaluation of U-service survivability. This paper also presents an continuous time markov chain (CTMC) Model for evaluation of survivability of U-service that a Jini system provides, and an approach to evaluate the survivability of the U-service as a blocking probability that end users can not access U-services.

Key words : survivability, ubiquitous service, byzantine failure, cyber attack, Markov Chain Model

접수일(2011년 12월 09일), 수정일(1차: 2011년 12월 15일), 게재확정일(2011년 12월 22일)

* 선문대학교 IT교육학부

1. 서 론

U-service 환경은 우리일상을 정보통신망으로 연결하여 다양한 서비스를 제공하는 환경이기 때문에 그 서비스의 생존성을 제고하는 것은 중요하다. 그러나 U-service 환경은 연결의 신뢰성이 낮아 네트워크 시스템이 분할(partitioned)되기 쉽고 서비스를 제공하는 시스템 구성요소가 장애나 고장, 사고로 서비스 실패가 발생할 확률이 높다. 게다가 물리적 공격이나 사이버테러를 통한 공격에 서비스 생존성이 쉽게 위협받는다.

생존성에 대한 정의에 대해서 [1]은 생존성을 장애나 사고, 공격이 발생하더라도 자신에게 부여된 본연의 서비스를 지연 없이 제공할 수 있는 시스템 능력으로 정의하고 있다.

[2]에서는 네트워크 시스템의 생존성을 일반화하여 정량화 할 수 있는 프레임워크를 제시하였고, [3]에서는 [2]에서 제안한 프레임워크를 확장하여 무선 ad hoc 네트워크의 정량적인 생존성을 평가할 수 있는 모델을 제시하였다.

Jini(현재는 Apache River로 명명됨)[4]는 장치의 종류, 통신 프로토콜과 같은 하부 이종성을 극복하면서 네트워크상에 편재된(ubiquitous) 장치와 소프트웨어 자원의 공유를 지원하는 Java 기반 미들웨어이다. 이러한 편재된 자원을 이용할 수 있게 해주는 것을 U-Service라 하는데 Jini는 가용한 서비스를 Lookup 서비스를 통해 동적으로 발견하고 클라이언트가 요구하는 서비스를 연결시켜주는 메커니즘을 제공한다. 그러나 Jini 시스템은 임차한 자원에 대한 서비스 실패에 대해서는 결함감내 서비스를 지원하지 않아서 서비스 생존성을 제고시키는 메커니즘이 부족하다.

Jgroup/ARM 프레임워크[5]는 Java 기반 객체 그룹 플랫폼이라는 개념을 도입하여 분산컴퓨팅 환경에서 의존 가능한 Jini 서비스를 구축하는 미들웨어 기술을 제시하였다. 분산된 서비스 복제 객체들이 그룹이 되어 하나의 서비스를 책임지는 생존성 제고를 위한 메커니즘을 제공한다. 그래서 이원화된 미들웨어와 통신 메커니즘을 제공한다. 하나는 클라이언트를 위한 Jini 미들웨어 자체이고 다른 하나는 서비스 복제들이 하나의 개체처럼 동작하도록 지원하는 미들웨어이다. 그러나 Jgroup/ARM 프레임워크는 사이버테러와 같은 보안공격에 대한 고려가 없어, 보안에 취약하다.

[6]의 연구에서는 기존의 Jgroup/ARM 프레임워크에 보안성을 제공하여 침입감내 능력을 제공하기 위한 Jini 시스템 구조를 제시하였다.

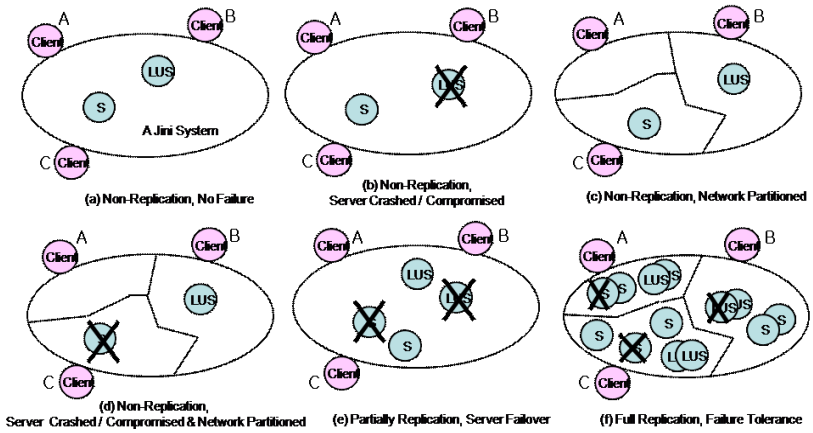
[2]와 [3]의 연구들은 각각 전통적인 전화망이나 무선 ad hoc 망에서 교환기나 라우터가 연결을 보장하지 못하여 네트워크 시스템의 생존성이 달라지는 문제를 정량화하는 방안을 제시하였다. 본 논문에서는 [2]와 [3]의 연구를 확장하여, [6]에서 제시한 시스템에서 의도적인 사이버테러가 발생하는 상황을 고려했을 때, 사용자가 서비스를 이용할 수 없는 확률 측면에서 U-service 서비스 생존성을 정량화 할 수 있는 프레임워크를 제시한다.

2. 시스템 및 서비스 생존성 위협 분석

2.1 Jini 시스템의 서비스 범위

Jini 시스템은 Lookup 서버와 서비스를 구현한 서버, 클라이언트로 구성된다. 서버와 클라이언트는 서비스 발견(discovery) 프로토콜 수행을 통해 유비쿼터스 네트워크 환경에서 Lookup 서버의 존재를 발견한다. 발견 이후에 서버와 클라이언트는 Lookup 서버로부터 Lookup 서비스 이용에 필요한 Lookup 서비스프락시를 다운로드한다. 그 후 서버는 자신의 서비스프락시를 Lookup 서버에 등록하고 클라이언트는 Lookup 서비스프락시를 통해 이용 가능한 서비스 구현들을 발견한다. 이때 원하는 서비스를 선택하면 해당 서버가 제공한 서비스프락시를 Lookup 서버로부터 받게 된다. 클라이언트는 다운로드한 서비스 프락시를 이용해 원격의 서비스 구현을 호출한다. 서비스 호출과 응답은 Java RMI(Remote Method Invocation) 통신을 이용하여 하부 통신 프로토콜에 투명하게 이루어진다.

네트워크상에서 Lookup 서버를 발견할 수 있는 범위는 멀티캐스트 발견(multicast discovery) 메시지를 어디까지 전달할 수 있는가에 달려 있다. 통상적으로 이 메시지의 도달거리는 멀티캐스트 발견 패킷의 TTL 파라미터(최대 15)에 의해 결정된다. 그러나 Jini 시스템을 구성하는 Lookup 서버와 서버, 클라이언트가 이 메시지를 수신할 수 있는 멀티캐스트 그룹에 속해야 하며 라우터의 구성이 이를 지원해야 한다. 따라서 네트워크상에 분산된 Lookup 서버들이 서비스 발견 프로토콜 수행을 통해 상호 발견과



(그림 1) Jini 시스템에서 서비스 이용실패와 감내 시나리오

서비스 연합이 가능하다고 하더라도 Jini 시스템은 관리 가능한 네트워크 경계까지로 그 범위가 국한될 수 밖에 없다.

2.2 Jgroup/ARM 시스템

Jgroup/ARM 시스템의 구조적 특징[5]은 이원화된 미들웨어와 통신 메커니즘을 제공한다는 것이다. 하나는 클라이언트를 위한 Jini 미들웨어 자체이고 다른 하나는 서비스 복제들이 하나의 개체처럼 동작하도록 지원하는 미들웨어이다. 이를 지원하는 핵심 컴포넌트는 Jgroup 데몬(JD)과 GM(Group Manager, 즉, Server-side Proxy)이다. JD 가 신뢰성 있는 그룹멤버십 멀티캐스트 통신을 지원하고 서버의 실패와 네트워크 분할 사실을 실시간으로 탐지하여 관련 이벤트를 GM에게 제공한다. Jgroup/ARM 프레임워크는 네트워크 분할과 서버붕괴와 같은 상황을 대비하기 위한 서비스 개발자에게 복잡한 서비스 중복에 대한 개발 부담을 덜어준다. JD 구현에 대한 인터페이스를 제공하고 그룹 멤버십 관리를 지원하는 GM(즉, Server-side Proxy)이 Jini 서비스 개발자가 본래의 서비스 구현에 집중하도록 다양한 인터페이스를 지원한다.

2.3 서비스 생존성 위협 분석

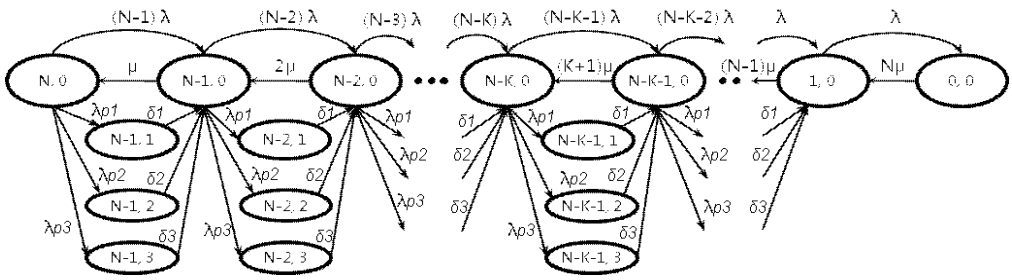
U-Service의 생존성을 위협하는 것은 사용자가 서비스를 이용할 수 없게 만드는 상황이다. 크게 다음 세 가지가 상황이 존재한다.

- 서버의 붕괴(crash)
- 네트워크 분할
- 보안훼손 (compromised results)

서버의 붕괴는 서비스를 호스팅하는 컴퓨팅 노드가 정전이나 물리적 공격에 의한 파괴, 사이버테러에 의한 가용성공격(예, DoS 공격)에 의해서 발생할 수 있다. 네트워크 분할은 전파 신호의 감쇄나 잡음(noise), AP(Access Point)와 라우터, 스위치 같은 네트워크 장치의 정전, 물리적 파괴, 사이버테러에 의해서 네트워크가 분할되었을 때 발생할 수 있다. 보안훼손은 사이버테러에 의해서 서버 및 컴퓨팅 장치에 저장된 데이터의 무결성이 손상된 결과이다. 그로인해 사용자가 정상적인 서비스를 제공할 수 없는 상황에 처하는 경우이다.

결함 및 사이버테러 발생에 대해 Jgroup/ARM 프레임워크 기반의 Jini 시스템에서 발생할 수 있는 서비스 이용실패와 감내 시나리오는 (그림 1)과 같다.

(그림 1)의 (a)는 서버의 중복을 적용하지 않은 가장 일반적인 Jini 시스템이다. 결함 및 사이버테러가 발생하지 않아 서비스 실패가 없는 경우이다. (b)는 서버가 붕괴되거나 사이버테러에 의해 보안훼손되어 정상적인 서비스를 제공할 수 없는 상황을 의미한다. 만약 Lookup 서버가 붕괴되었다면, 기존에 서버와 연결을 유지하던 사용자는 주어진 임차시간 내에서만 서비스 이용이 가능하다. (c)는 AP 또는 라우터와 같은 네트워크 장치에 결함 및 침입이 발생하여 네트워크가 분할된 경우이다. 서비스 이용자 A는 연결을 잃으며 서비스 재발견의 기회도 잃는다. 서비스 이용자 B는



λ : the failure rate of each replica → 1/λ : avg. failure time
p1 : the probability of failure being node crash or replica crash
p2 : the probability of failure being link failure that occurs connection down
p3 : the probability of failure being compromised server that commits a compromised result

1/δ1 : average switching delay (due to a node or replica crash)
1/δ2 : average switching delay (due to a link failure)
1/δ3 : re-request-reply delay (due to a compromised result)
μ : repair rate for either type of failure → 1/μ : avg. repair time

(그림 2) 서비스 생존성 평가를 위한 연속시간 마코프 체인 모델

서버와의 연결을 잃으면서 연결 불가능한 서비스만 재발견할 뿐이다. 그것도 임차시간이 지나면 Lookup 서버에서 서비스의 존재가 사라진다. 서비스 이용자 C만 주어진 임차시간 동안 서비스 이용이 가능 할 뿐이다. (d)의 상황은 모든 이용자가 서버와의 연결을 잃으며, 서비스 이용자 B만 주어진 임차시간 동안 연결할 수 없는 서비스 발견이 가능하다. (e)의 경우는 서버붕괴 상황은 극복이 가능하지만, 네트워크가 어떻게 분할되는지에 따라서 일부 서비스 이용자는 서비스 이용이 제한된다. (f)는 서비스 수행 태스크가 분산 복제됨에 따라, 서버 붕괴와 네트워크 분할 상황을 극복한다.

3. U-Service 생존성 평가 모델

3.1 연속시간 마코프 체인모델

본 논문에서는 U-service 생존성을 정량적으로 평가하기 위해, r 개의 Jini 서비스 복제가 분산된 시스템에서 사용자에게 제공하는 U-service의 가용도를 구하는 연속시간 마코프 체인 모델을 제안한다. [7]에 따르면 정량적인 생존성 특성은 시스템이 운영되는 환경을 완전히 나타내는 유한상태기계 모형을 구성하고 유한상태기계의 각 상태에 확률밀도 함수를 부여하여 표현한다. 마코프체인은 유한상태기계를 상태변환 확률이 부여된 것으로 보기 때문에 마코프체인 모델을 이용하여 시스템이 정상적으로 동작할 때 정상상태(steady state) 확률을 적용하여 정상상태의 가용도를 구할 수 있다. (그림 2)는 (그림 1)의 (f)와 같은 환경에서 발생할 수 있는 서비스 생존성 위협들에 대해서 시스템이 갖는 정상상태들을 연속시간 마코프 체인 모델로 나타낸 것이다.

(그림 2)의 각 파리미터와 상태의 의미는 다음 <표 1>과 같다.

<표 1> 파라미터와 상태의 의미

λ	서비스 연결 실패가 발생할 확률(failure rate)로서 결함 또는 사이버테러가 발생할 확률
$\rho 1$	서비스 연결의 실패가 서버노드 및 서비스 붕괴일 확률
$\rho 2$	서비스 연결의 실패가 통신링크의 단절일 확률, 즉 네트워크 분할에 의한 실패 확률
$\rho 3$	서비스 연결 실패가 보안훼손된 서버에 기인하여 발생했을 확률
$1/\delta 1$	서버노드 및 서비스 붕괴가 발생하여 다른 서비스 복제로 접근하는 데 걸리는 지연
$1/\delta 2$	네트워크 분할로 다른 서비스 복제로 접근하는 데 걸리는 지연
$1/\delta 3$	서버가 보안훼손된 결과로 인해 다른 서비스 복제로 접근하는 데 걸리는 지연
μ	복구율(repair rate)
state(3,0)	총 4개의 복제에서 한 개의 복제에 연결성공, 나머지 3개의 복제에도 아무런 실패(failure) 가 없음
state(3,1)	현재 연결 시도한 복제에서 서버노드 또는 서비스 붕괴가 발생하여 연결실패, 여분의 복제가 3개 존재함
state(3,2)	현재 연결 시도한 복제에 링크단절이 발생하여 연결 실패함, 여분의 연결가능한 복제가 3개 존재함
state(3,3)	현재 연결 시도한 복제가 보안훼손됨, 대체 연결 가능한 복제가 3개 존재함
state(1,0)	현재 연결 시도한 복제에 연결성공, 여분의 복제가 1개 존재함
state(0,0)	현재 연결 시도한 복제에 연결성공, 여분의 복제가 존재하지 않음
state(0,2)	현재 연결 시도한 복제에 링크단절이 발생하여 연결실패, 여분의 복제도 없음

3.2 U-service 생존성 평가

(그림 2)에서 서비스 생존성 위협들에 대해서 시스템이 갖는 각 정상상태들을 $\pi(i,j)$ 라고 가정하고, (그림 2)의 연속시간 마코프 체인을 풀면, 각 정상상태가 발생할 확률은 다음과 같다.

$$\pi(0,0) = \left\{1+\sum_{j=2}^{N}\frac{(N-j)!(j-1)!}{N!}\rho^j(1+\frac{\lambda\rho1}{\mu1}+\frac{\lambda\rho2}{\mu2}+\frac{\lambda\rho3}{\mu3})+\frac{1}{N}\rho^j\right\}^{-1} \quad (1)$$

$$\pi(j,0) = \frac{(N-j)!(j-1)!}{N!}\rho^j\pi(j-1,0) \ (1 \le j \le N) \quad (2)$$

$$\pi(j,1) = \frac{(N-j)!(j-1)!}{N!}\rho^j\frac{\lambda\rho1}{\mu1}\pi(j,0) \ (1 \le j \le N) \quad (3)$$

$$\pi(j,2) = \frac{(N-j)!(j-1)!}{N!}\rho^j\frac{\lambda\rho2}{\mu2}\pi(j,0) \ (1 \le j \le N) \quad (4)$$

$$\pi(j,3) = \frac{(N-j)!(j-1)!}{N!}\rho^j\frac{\lambda\rho3}{\mu3}\pi(j,0) \ (1 \le j \le N) \quad (5)$$

여기서 $\rho = \lambda/\delta$

사용자가 서비스에 접근할 수 없는 확률(blocking probability)로서 U-service의 생존성을 정량적으로 구한다면 이것은 다음과 같이 Jini 시스템을 연결하는 종단간 가용성과 같다.

$$A_{steady-state} = \sum_{j=1}^{N}\pi(j,0) \quad (6)$$

U-service 생존성에 큰 영향을 주는 파라미터는 <표 1>에 나타낸 λ 와 μ 이다. λ는 시스템에 결함 또는 사이버테러가 발생하여 서비스 연결에 실패할 확률이고 μ 는 이에 대한 복구율이다. 두 가지 모두 단위 시간에 대해 서비스 이용이 안 되는 시간과 복구에 소요되는 시간의 비로 구한다.

4. 시뮬레이션 분석

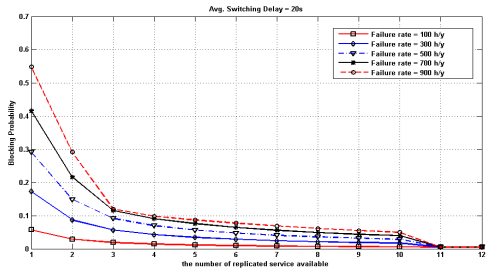
4.1 시뮬레이션 조건

U-service의 생존성을 정량적으로 평가하기 위한 시뮬레이션 조건은 다음 <표 2>와 같다.

<표 2> 시뮬레이션 조건

λ	100, 300, 500, 700, 900 hour/year 씩 가변
$\rho1$	0.25
$\rho2$	0.5
$\rho3$	0.25
δ	20초 (평균 서비스 전환 지연)
μ	1.1416 (평균 복구율)
replica	12개

4.2 시뮬레이션 결과 분석



(그림 4) 시뮬레이션 결과

<표 2>에서 제시한 파라미터 값을 기초하여 U-service 생존성을 평가하면 (그림 4)와 같다. 복제의 수가 많을수록 서비스 생존성이 높아져 사용자가 서비스 접근 할 수 없는 확률이 낮아짐을 확인 할 수 있다. 아울러, 결함 및 사이버테러와 같은 서비스 연결 실패를 초래하는 확률에 따라 서비스 생존성이 어떻게 변화하는지 분석할 수 있다. 본 시뮬레이션 결과는 본 논문의 결과가 복제의 수, 복구시간, 결함 및 사이버테러의 발생 확률값에 따라 서비스 생존성에 어떻게 영향을 주는지 정량적인 분석 도구를 제공할 수 있음을 보여준다.

5. 결 론

유비쿼터스 서비스를 제공하는 시스템은 서비스 생존성이 취약한 환경을 극복해야하는 네트워크 시스템이다. 네트워크 시스템의 생존성은 시스템 구성요소에 장애나 사고, 물리적 공격이 발생하더라도 시스템에 부여된 본연의 서비스를 중단 없이 제공할 수 있는 시스템 능력으로

정의하고 있다.

본 논문에서는 비잔틴 장애를 초래하는 의도적인 사이버테러가 네트워크 시스템에 가해졌을 때의 상황을 고려하여, Jini 시스템이 제공하는 U-service의 생존성을 평가하기 위한 연속시간 마코프 모델을 제시하고 이를 토대로 사용자가 서비스에 접근할 수 없는 확률로서 U-service 생존성을 평가하는 방안을 제시하였다. 본 논문의 연구결과는 U-service 생존성을 정량적으로 분석할 수 있는 도구를 제공함으로써 시스템 설계 단계에서 결함 및 침입을 감내할 수 있는 최소한의 요구사항을 도출하는데 활용될 수 있으리라 기대한다.

참고문헌

[1] R.J.Ellison et.al., ""Survivable Network Systems : An Emerging Discipline", Technical Report CMU/SEI-97-TR013, 1999

[2] Yun Liu et,al., "A General Faramework for Network Survivability Quantification", 12th GI/ITG Conference on Measuring, Modeling and Evaluation of Computer and Communication Systems, MMB & PGTS, 2004

[3] D.-Y. Chen, S. Garg, and K. S. Trivedi. Network survivability performance evaluation: A quantitative approach with applications in wireless ad-hoc networks. MSWiM′ 02, Atlanta, GA, September 2002. ACM

[4] Sun Microsystems, "JiniTM Architecture Specification", Published Specification, http://java.sun.com/products/jini/2.0/doc/specs/html/jini-spec.html, 2003.

[5] Hein Meling, et al., "Jgroup/ARM: a distributed object group platform with autonomous replication managements", Software Practice and Experience, John Wiley & Sons, 2007.

[6] 김성기 외, "유비쿼터스 서비스 생존성 제고를 위한 침입감내 Jini 서비스 구조", 대한전자공학회 제45권 CI편 제 4호, 2008.7.

[7] D. Logothesis, K. S. Trivedi, and A. Puliato,"Markvov regenerative models", In Proc. Intl. Computer Performance and Dependability symp., pages 134-143, Erlangen, Germany, 1995

[저 자 소 개]

김 성 기 (Sung-Ki Kim)

1996년 3월 인천대 전자계산학 학사
1998년 3월 인천대 컴퓨터공학 석사
2006년 2월 인천대 컴퓨터공학 박사
2006년 6월 인천대 초빙교수
2009년~현재 선문대학교 IT교육학부 전임강사

email : skkim@sunmoon.ac.kr