[5B-35]

# 신뢰성 있는 네트워크 보호 방법 및 특성

정 조희, *남 택용, 한 치문
한국외국어대학교, *한국전자통신연구원
joyjung@hufs.ac.kr, *tynam@etri.re.kr, and cmhan@hufs.ac.kr

# Reliable Network Security Model and Its Characteristics

Johee Jung, Taekyong Nam, and Chimoon Han
HanKuk University of Foreign Studies, ETRI

## 요 약

최근 인터넷 이용자의 급증과 더불어 바이러스, 해킹, 침해 등 보안 사고의 확산으로 신뢰성 있는 네트워크를 구축하고자 하는 연구가 활발히 진행되고 있다. 이러한 연구로는 ITS(Intrusion Tolerance System) 기술, FTN(Fault Tolerance Network) 기술 및 DC(Dynamic Coalitions) 기술에 초점을 맞추고 있다. 본 논문에서는 네트워크 보안 사고에 대해 능동적으로 대처하기 위한 방법으로 국부화(localization) 개념을 적용한 계층적 네트워크 모델을 제시하고, 그 특성을 확인한다. 특히 계층적 네트워크 모델에서는 외부의 공격이나 침입으로 인한 침해지역을 국부화하여 네트워크 생존성을 제공하기 위함이다. 주 내용은 공격, 침입에 의한 네트워크 내의 트래픽을 필터링하고, 감염 정도에 따른 국부화를 수행하여 감염 확산을 방지하고, 우회경로를 제공함으로 감염 피해의 최소화 및 네트워크의 생존성을 제공하는 것이다. 본 논문에서는 국부화 개념을 제공하기 위해 요구되는 네트워크 인프라 보호 모델 및 구성 요건을 제시하고, 본 개념을 확인하기 위해 평가 모델 분석을 통해 본 방식의 타당함을 분명히 한다.

## I. 서론

인터넷을 이용하여 비즈니스를 전개하는 경우, 일시적인 서비스 정지가 기업에 막대한 손해를 초래할 뿐만 아니라 기업 이미지에 치명적인 영향을 준다. 이러한 사이버 공격 유형은 시스템 위주의 공격에서 네트워크 공격으로 변화하고 있다. 특히 최근에는 DDoS 공격이 주를 이루고 있다. 하지만 이러한 공격에 대한 적절한 보안 대책은 아직 미흡한 실정이다.

이에 본 논문은 네트워크 보안에 대한 네트워크 생존성 보장 할 수 있는 방법으로 네트워크 인프라 보호 모델에 대해 개념적 모델과 네트워크 구성 방법을 제시한다. 네트워크 생존성 확보에서는 보안 문제로 네트워크 장애가 발생하는 것을 방지하고, 신뢰성 있는 네트워크를 구축하기 위해, 시스템 설계기술, 운영체제의 전략 전술적 운영 그리고 다양한 정보보호 기술을 이용하여 사전에 침입자가 침입하지 못하도록 방지하는 방법과 침입자를 검출하여 적절히 대응하는 기술 등을 이용하고 있다. 현재까지 연구된 기술로는 ITS 기술, FTN 기술, DC 기술 등이 있다[1,2,3,4].

본 논문에서는 계층적 개념을 적용한 국부화(localization) 개념 도입 및 네트워크 장애 시 우회경로를 설정하여, 네트워크 공격 및 침입에 대한 피해를 최소화하고 감염 확산을 차단하는 방법을 나타낸다. 따라서 본 논문의 구성은 서론에 이어, 2 장에서 신뢰성 있는 네트워크 인프라 보호 모델에 대한 개념과 구성 요건에 대해 설명하고 3 장에서는 본 논문에서 제시한 개념을 확인하기 위해 간단한 평가 모델을 통해 특성을 평가한다. 4 장에서 결론을 맺는다.

## II. 신뢰성 있는 네트워크 인프라 모델

### 2.1 계층적 개념을 도입한 네트워크 인프라 보호 모델

보안 공격에 대해 네트워크의 생존성 보장을 위해 계층적 국부화(localization) 개념 및 우회 경로 설정 방식을 도입한 네트워크 인프라 보호 모델 개념을 제안한다. 본 개념을 적용하기 위해 네트워크를 3 개의 계층 즉 Secure Local Region (SL), Secure Group Local Region (SGL) 그리고 Secure Super Group Local Region (SSGL)으로 나누는 계층적 개념을 제안한다. 이 개념을 그림 1 에 나타냈다.

Secure Local Region (SL) 계층은 한 개 이상의 security router(security gateway)를 포함하는 최소 단위의 국부화 지역을 말한다. 가능한 최소 규모의 지역으로 정의한다. 그리고 각 SL 간에는 적어도 경로가 한 개 이상 존재한다. Secure Group Local Region (SGL) 계층은 두 개 이상의 SL 로 구성되며, SGL 간 또는 SL 간에는 경로가 한 개 이상 존재한다. Secure Super Group Local Region (SSGL) 계층은 두 개 이상의 SGL 로 구성되며, SSGL 간 또는 SL 간에는 경로가 한 개 이상 존재한다.

이상의 계층적 개념을 그림 1 에서 보면, 네트워크 자체는 물리적으로 1 차 평면에 존재하며, 계층화는 국부화 영역을 의미한다. 본 개념에서 SL 지역을 외부 네트워크와 차단시키는 최소 단위의 영역을 말한다. 즉 SL 지역을 국부화시켜 다른 지역으로 바이러스가 전파되는 것을 차단하여 네트워크 생존성을 보장하는 방법으로 신뢰성 있는 네트워크를 구축하는 개념이다. 이때 SL 지역을 국부화 하여도 네트워크 생존성 보장이 불가능한 경우는 SGL 지역을 국부화하여 네트워크 생존성을 제공한다.