클라이언트-서버 모델을 활용한 정보전 시뮬레이션 장치 및 방법

■ 보유기관 한국전자통신연구원

■ 주요 발명자

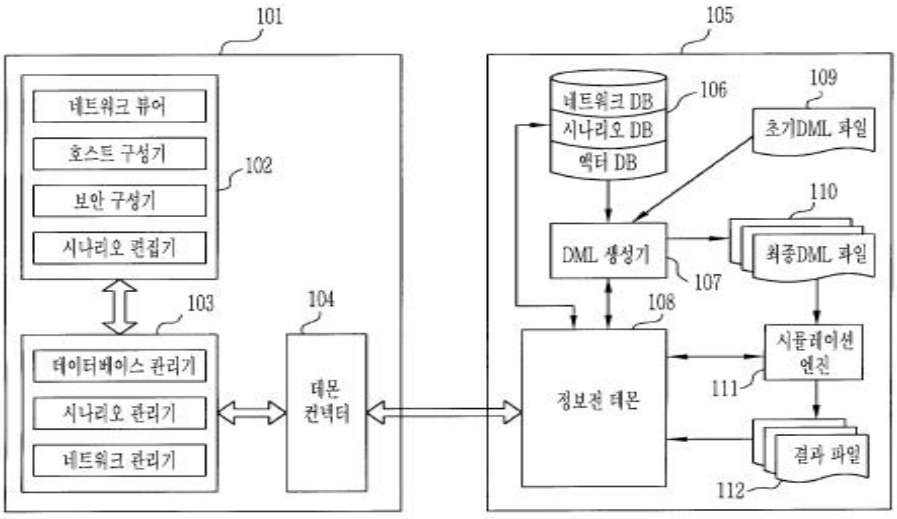
■ 권리사항	
· 출원번호	10-2003-0015361
· 출원일	2003년 3월 12일
· 현재상태	■ 등록 □ 공개(심사중) □ 미공개
■ 기술완성도	□ 기초연구단계 ■ 실험단계 □시작품단계 □ 제품화단계

■ 적용가능분야 및 목표시장 보안 시스템 시장

■ 기술 개요

본 기술은 정보전에 사용되는 여러 가지의 공격 및 방어 기술을 효과적으로 실험할 수 있는 시뮬레이션 장치에 관한 것으로, 클라이언트-서버(client-server) 모델로 구성되어 있음

■ 기술 개념도



[그림] 본 기술에 따른 클라이언트-서버 모델을 활용한 정보전 시뮬레이션 장치의 구성도

■ 기술 내용 및 동향

[상세 기술 내용]

- 본 기술은 사용자에게 인터페이스를 제공하는 클라이언트와, 사용자의 입력을 토대로 네트워크를 구성하고 다양한 시뮬레이션을 실행하여 결과를 출력하는 서버로 구성된 정보전 시뮬레이션 방법 및 장치임

[기술의 특·장점]

- 사용자의 명령에 따라 데이터베이스를 토대로 네트워크를 구성하고 정보전의 공격 및 방어 시나리오를 시뮬레이션하는 시뮬레이션 서버와, 사용자의 명령 및 데이터를 시뮬레이션 서버로 제공하고, 시뮬레이션 서버로부터 전달되는 시뮬레이션 결과를 사용자에게 제공하는 시뮬레이션 스튜디오를 포함하는 것을 특징으로 함
- 정보전 시뮬레이션을 위한 모델링 방법을 개선하여 시뮬레이터의 구현을 통한 정보전 연구 기반의 구축 및 자료 확보할 수 있는 장점이 있음
- 또한 다양한 네트워크 환경과 시나리오를 빠른 시간 내에 구성하여 시뮬레이션할 수 있도록 함으로써 실제로 예상되는 정보전 상황에 대해 효과적으로 대비할 수 있도록 하는 장점이 있음

[기술동향]

- 컴퓨터 시스템 및 네트워크를 통한 통신의 발달에 따라 전자 메일(e-mail) 첨부 파일을 이용한 해킹 코드의 확산, 컴퓨터 시스템의 취약성을 이용한 공격, 자원의 고갈을 유도하는 서비스 거부 공격(Distributed Denial of Services; DDoS) 등과 같은 컴퓨터 시스템이나 개인 정보의 해킹을 통한 사이버 공격이 점차적으로 증가하고 있음
- 사이버 공격으로부터 시스템을 보호하기 위하여 공격 기법이나 방어 기법을 다양하게 연구하고 공격에 대한 적절한 대책도 발표하고 있으나, 현재로서는 공격과 그에 대한 피해가 확인된 후에야 대책이 수립되는 것이 일반적으로, 일단 대책이 알려지면 동일한 공격 기법을 이용한 공격의 빈도는 적어진다고 알려져 있음

■ 관련 기술

1	출원번호	10-2003-0028185
	발명의 명칭	시스템의 보안성 및 성능 향상을 위한 패치 분배 시스템및 방법
2	출원번호	10-2003-0034010
	발명의 명칭	유해 트래픽 탐지/대응 시스템 및 방법
3	출원번호	10-2003-0067442
	발명의 명칭	네트워크 노드의 보안 엔진 관리 장치 및 방법

■ 시장 동향

- 정보전이란, 적국에 배치된 컴퓨터나 이에 침투시킨 바이러스로 적국의 전산망 등을 공격하는 것을 의미하며, 현대적인 정보전의 개념 및 주요 대상은 적군의 첨단 장비 내부에서 컴퓨터 바이러스나 소프트웨어 해킹을 통한 적 컴퓨터의 기능 마비나 파괴, 정보 획득 등으로 범위가 확대되고 있으며, 논리 폭탄이나 전자기 펄스, 컴퓨터 시스템에 큰 영향을 주는 고출력 전자파 병기 등이 사용됨
- 이러한 정보전은 핵탄두 미사일이나 전투기 등의 가시적인 무기와 병력을 동원하지 않고도 효율적이면서 완전하게 상대방을 제압해버린다는 점에서 미래의 이상적인 전투개념이라고 할 수 있으며, 정보전쟁에서 주요 공격목표가 되는 것은 컴퓨터에 의존하고 있는 방대한 군 조직이나 첨단 정밀무기들임
- 현재도 선진 각국은 비약적으로 발전하고 있는 전자통신기술을 바탕으로 하여 암암리에 발달된 장비를 운용하여 고도의 첩보전과 해커전을 전개함으로써 정보전쟁에서의 우위를 차지하려고 치열한 경쟁을 벌이고 있음
- 정보전 능력은 하드 드라이브를 파괴하고 컴퓨터바이러스를 침투시키는 해킹단계를 훨씬 능가하는데, 최근 미국과 중국 등에서 신설하고 있는 정보전 특수부대와 훈련기관에서는 해커들과 프로그래머들에게 국가 전력 공급 컴퓨터에 침입해서 전력공급을 마비시키거나 상대국에 잘못된 정보를 흘려 적군끼리 싸우게 하고, 미사일의 목표지점을 바꾸게 하는 등의 고도의 훈련을 실시하고 있는 것으로 알려져 있음
- 새로운 전쟁양상의 도래와 함께 앞으로는 전쟁수행의 개념과 수단, 방법 등이 크게 변화될 것으로 특히 과학기술면에서는 장차 인공위성을 포함한 탐지기술과 적외선(IR: Infrared Rays)기술을 이용한 야간 및 악천후 탐지기술이 더욱 발전할 것이며, 현재 항공기에 응용되는 스텔스 기술도 함정 및 지상무기 체계에까지 확대 적용될 것으로 예상됨
- 또한, 고속 정보통신체계의 등장과 함께 C4I(Command & Control, Communication, Computer and Intelligence) 등 전장 감시 및 통제체제가 획기적으로 강화되어 실시간에 적군과 아군의 작전활동을 파악하여 지휘 통제함으로써 광역화되고 분산된 군사력 전개 상황 하에서도 전투력의 통합과 집중의 속도, 즉 작전 템포가 획기적으로 증대될 것으로 기대됨

■ 문의처	
· 소속	기술사업화실
· 담당자	유준상
· 연락처	042-870-4827, yjs39@ensec.re.kr