(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 12/26 (2006.01)
H04L 9/32 (2006.01)
H04L 12/24 (2006.01)
H04L 12/22 (2006.01)

(45) 공고일자 2007년03월27일
(11) 등록번호 10-0694248
(24) 등록일자 2007년03월06일

(21) 출원번호 10-2006-0036949
(22) 출원일자 2006년04월25일
심사청구일자 2006년04월25일

(65) 공개번호
(43) 공개일자

(73) 특허권자 충남대학교산학협력단
대전광역시 유성구 궁동 220번지 충남대학교

(72) 발명자 김현수
대전 유성구 전민동 엑스포아파트 403동 902호

국승학
대전 서구 관저동 원앙마을 2단지 212동 1503호

오일노
대전 유성구 구암동 595-13

박영대
대전 대덕구 중리동 173-12

박상춘
대전 대덕구 목상동 상록수아파트 101동 1301호

(74) 대리인 김원준

(56) 선행기술조사문헌
KR1020050031215 A
* 심사관에 의하여 인용된 문헌

심사관 : 김병균

이 발명을 지원한 국가연구개발사업
과제고유번호 B1220-0501-0320
부처명 정보통신부
연구사업명 IT기초기술연구지원사업
연구과제명 보안 솔루션의 보안정책 테스트를 위한 테스트베드 구축방안
주관기관 충남대학교
연구기간 2005년 7월 1일~2007년 6월 30일

전체 청구항 수 : 총 6 항

(54) 네트워크 보안시스템의 보안 정책 테스트 장치 및 방법

(57) 요약

본 발명은 사용자 개입을 최소화하면서 시스템의 보안성을 효과적으로 테스트할 수 있는 네트워크 보안시스템의 보안성 테스트 장치 및 방법에 관한 것이다.

이를 위해, 본 발명에서는 테스트 대상이 되는 시스템의 패킷 필터링 프로그램의 패킷 필터링 규칙을 분석하여 필요한 데이터를 추출하고, 이렇게 추출한 데이터를 이용하여 다양한 조합의 테스트케이스와 테스트오라클을 자동 생성하며, 상기 테스트케이스를 이용하여 본 발명의 테스트베드에서 자동 테스트를 수행하고, 이때 얻어진 패킷의 로그와 테스트오라클을 서로 비교하여 테스트결과를 자동 산출한다.

본 발명에서 제안하는 네트워크 보안시스템의 보안성 테스트 방법 및 장치에 따르면 필터링 규칙의 변경이 발생하여도 변경된 데이터에 맞는 새로운 테스트케이스와 테스트오라클을 자동생성하여 이를 실행결과와 자동으로 비교함으로써, 필터링 결과(보안성)가 옳은지 혹은 틀린 지를 판단할 수 있다.

대표도

도 2

특허청구의 범위

청구항 1.

패킷 필터링 프로그램을 내장한 시스템 보안용의 패킷필터에 접속되는 패킷생성기 및 패킷분석기로 이루어진 보안성 테스트 장치에 있어서,

상기 패킷생성기는

테스트 대상이 되는 패킷 필터링 프로그램의 필터링 규칙을 사용자로부터 입력받아 정확한 규칙인지를 판별하고, 입력된 필터링 규칙이 정확한 규칙이면 해당 규칙을 파싱하여 송신/수신측의 IP주소와 포트 정보 및 프로토콜 정보를 추출하는 **규칙해석모듈**과;

상기 규칙해석모듈에서 추출된 송신/수신측의 IP주소와 포트 정보 및 프로토콜 정보를 바탕으로 테스트케이스를 생성하는 **테스트케이스생성모듈**과;

상기 테스트케이스생성모듈에서 생성된 테스트케이스를 바탕으로 패킷을 자동으로 생성하여 전송하는 **패킷센더**와;

상기 테스트케이스생성모듈에서 생성된 테스트케이스와 상기 패킷센더에서 전송된 패킷의 로그 정보를 이용하여 결과판단을 위한 테스트오라클을 자동으로 생성하는 **테스트오라클생성모듈**과;

전송된 패킷의 수신 여부를 탐지하여 기록하는 **패킷탐지모듈**; 및

테스트 수행에 필요한 정보의 전송 및 동기화를 이루는 **싱크로나이저**;

를 포함하는 것을 특징으로 하는 네트워크 시스템의 보안성 테스트 장치.

청구항 2.

제1항에 있어서,

상기 패킷분석기는

상기 테스트케이스생성모듈에서 생성된 테스트케이스를 바탕으로 패킷을 자동으로 생성하여 전송하는 **패킷센더**와;

전송된 패킷의 수신 여부를 탐지하여 기록하는 **패킷탐지모듈**과;

테스트 수행에 필요한 정보의 전송 및 동기화를 이루는 **싱크로나이저**와

상기 패킷탐지모듈에서 생성된 탐지 패킷 로그와 상기 테스트오라클을 이용하여 보안성 테스트 결과를 자동으로 산출하는 **결과판정모듈**;

을 포함하는 것을 특징으로 하는 네트워크 시스템의 보안성 테스트 장치.

청구항 3.

패킷 필터링 프로그램을 내장한 시스템 보안용의 패킷필터에 패킷생성기와 패킷분석기가 접속되어 시스템의 보안성을 테스트하는 방법에 있어서,

상기 패킷생성기의 규칙해석모듈이 상기 패킷 필터링 프로그램의 필터링 규칙을 파싱하고, 파싱한 필터링 규칙이 기본 정책, 플러딩(Flooding) 정책, 상태기반 정책, 단편화 정책 중 어디에 해당하는 것인지를 판별(115)하여 각각에 맞는 정보를 추출(116) 및 저장하는 **제1 과정**;

상기 제1 과정에서 추출된 정보를 바탕으로 상기 패킷생성기의 테스트케이스생성모듈이 테스트케이스를 생성하는 **제2 과정**;

상기 제2 과정에서 생성된 테스트케이스와 패킷필터의 환경설정정보를 이용하여 패킷을 생성하되 이를 목적지로 보내면서 전송한 패킷에 대한 로그를 남기는 **제3 과정**;

상기 제2 과정에서의 테스트케이스와 제3 과정에서 전송한 패킷의 로그를 이용하여 테스트오라클을 생성하는 **제4 과정**; 및

상기 제4 과정에서 생성된 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 상기 패킷분석기의 결과판정모듈이 비교하여 테스트의 수행결과를 판단하는 **제5 과정**;

을 포함하여 이루어지는 것을 특징으로 하는 네트워크 시스템의 보안성 테스트 방법.

청구항 4.

제3항에 있어서,

상기 제2 과정은,

상기 제1 과정에서 추출된 정보가

기본 정책에 관한 것이면 기본 정책 정보를 읽어들여 해당 필터링 규칙이 표현하고 있는 허가범위를 도출한 후 전체 도메인을 대상으로 동치 영역 분석과 경계값 분석을 통해 테스트케이스를 자동으로 생성하고,

플러딩(Flooding) 정책에 관한 것이면 상기 패킷생성기의 규칙해석모듈에서 추출한 Rate/Burst정보와 단위시간 정보를 읽어들인 후 플러딩 상태를 판단하는 기준을 찾아내어 정상적인 상태(Non-Flooding)와 비정상적인 상태(Flooding)의 테스트케이스를 자동으로 생성하고,

상태기반 정책에 관한 것이면 상기 패킷생성기의 규칙해석모듈로부터 추출한 각 상태별 허가/거부 정보를 읽어들여 정상적인 상태전이와 비정상적인 상태전이 정보를 추출해서 테스트케이스를 자동으로 생성하고,

단편화 정책에 관한 것이면 상기 패킷생성기의 규칙해석모듈에서 추출한 단편화 정보를 읽어들인 후 단편화 패킷의 허가/거부 정보를 추출(124-4)하여 정상적인 상태와 비정상적인 상태의 테스트케이스를 자동으로 생성하는 과정인 것을 특징으로 하는 네트워크 시스템의 보안성 테스트 방법.

청구항 5.

제3항 또는 제4항 중의 어느 한 항에 있어서,

상기 제4 과정은 읽어들인 정보가

기본 정책에 대한 것이면 테스트케이스의 허가범위에 해당하는 전송 패킷을 분석하여 전송되어야 할 패킷을 추출하는 것으로 테스트오라클을 자동 생성하고,

플러딩(Flooding) 정책에 관한 것이면 플러딩 기준에 해당하는 테스트케이스를 이용해 도착 가능한 전체 패킷 수를 분석하여 테스트오라클을 자동 생성하며,

상태기반 정책에 관한 것이면 정상적인 상태전이를 유도하는 패킷을 분석하여 테스트오라클을 자동 생성하고,

단편화 정책에 대한 것이면 테스트케이스를 이용해 도착 가능한 단편화 패킷을 분석하여 테스트오라클을 자동 생성하는 과정인 것을 특징으로 하는 네트워크 시스템의 보안성 테스트 방법.

청구항 6.

제3항 또는 제4항 중의 어느 한 항에 있어서,

상기 제5 과정은

기본 정책에 관한 것이면 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 비교해 통과 가능한 패킷만을 통과시켰는지 자동으로 판별하고,

플러딩 정책에 관한 것이면 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 비교해 허용되는 패킷 수만큼의 패킷만을 통과시켰는지 자동 판별하며,

상태기반 정책에 관한 것이면 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 비교해 허용 가능한 상태전이가 이루어졌는지 자동으로 판별하고,

단편화 정책에 관한 것이면 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 비교해 허용 가능한 단편화 패킷만을 통과시켰는지 자동으로 판별하는 과정인 것을 특징으로 하는 네트워크 시스템의 보안성 테스트 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 사용자 개입을 최소화하면서 시스템의 보안성을 효과적으로 테스트할 수 있는 네트워크 보안시스템의 보안정책(보안성) 테스트 장치 및 방법에 관한 것으로서, 기술적으로는 패킷 필터링 프로그램 및 이를 이용한 네트워크 보안시스템의 기능 테스팅 분야에 연관되어 있다.

프로그램 테스팅은 코드에 내재하여 있는 오류를 찾아내는 작업이다.

이러한 목적을 위해 수행되는 테스팅 작업은 크게 테스팅의 계획단계, 테스팅의 준비단계, 테스팅의 수행단계, 테스팅의 평가단계와 같은 네 개의 세부적인 과정으로 나누어질 수 있다.

그 중 A) 테스팅의 계획단계는 테스트 활동의 작업범위를 정의하고, 접근법, 자원, 일정들을 파악하는 단계이다. 이 단계에서는 테스트의 요구사항을 수집하고, 테스트를 계획하고, 이를 검토하는 일을 수행한다.

B) 테스팅의 준비단계는 테스트 수행을 위해 테스트케이스를 설계·준비하고, 테스트 환경을 구축하는 과정이다.

C) 테스팅의 수행단계는 테스트케이스를 기반으로 테스트하고자 하는 프로그램을 실행하여 그 실행결과를 기록하는 과정이다.

D) 테스팅의 평가단계는 수행단계에서의 실행결과를 바탕으로 프로그램에 오류가 존재하는지 여부를 판단하는 과정이다.

일반적으로, 테스트케이스는 테스트 절차를 나타내는 테스트스크립트와 상기 테스트스크립트를 수행할 때 필요한 테스트 데이터 및 실행결과의 오류 유무를 판정하기 위한 테스트오라클로 구성된다. 다시 말해, 테스트오라클은 테스트의 실행결과가 오류인지 여부를 파악하기 위해 사용하는 예상결과를 의미한다.

패킷 필터링 테스트는 방화벽이나 라우터의 보안정책 또는 패킷 필터링 규칙을 테스트하기 위한 것이다. 이는 지정된 규칙에 맞게 패킷이 정확하게 필터링 되는지, 즉 패킷필터와 이를 이용한 보안정책에 의하여 시스템이 안전하게 보호될 수 있는지 테스트하기 위한 것이다.

그러나 종래의 많은 연구들은 이러한 패킷 필터링에 관한 연구보다는 침투 테스팅(Penetration Testing)이나 로그 검사(Log Review)나 바이러스 탐지기(Virus Detectors) 등과 같은 세션 레벨 이상의 연구에 편중되어 있는 실정이다.

이 때문에, 라우터나 방화벽 같은 보안시스템의 기본이 되는 패킷 필터링에 관한 테스트 연구들은 간과되어 몇몇 빈약한 기능의 테스트 도구(장치)들이 존재할 뿐이며, 패킷 필터링에 관한 테스트도 대부분 수동으로 이루어지고, 현재 존재하는 테스트 도구 또한 사용자의 많은 개입과 판단을 요구하고 있다.

종래 예

Ftester는 방화벽의 보안정책을 테스트하는데 많이 이용되는 도구(장치)로서 패킷생성기의 역할을 하는 Ftest와, 패킷탐색기의 역할을 하는 Ftested와, 기본환경을 설정하는 'ftest.conf' 파일과, Ftest와 Ftested의 로그를 비교하는데 필요한 스크립트를 담고 있는 Freport로 구성되어 있다. 그러나 상술한 Ftester는 매번 새로운 테스트케이스에 대해 인위적인 설정과 스크립트작성이 필요하고, 분석도구도 종단 간의 로그에 대한 단순비교만을 제공할 뿐이다.

발명이 이루고자 하는 기술적 과제

본 발명은 패킷 필터링 테스트에 관련된 종래의 문제점을 개선하기 위해 안출된 것으로서, 패킷 필터링 규칙의 변경이 발생하여도 변경된 데이터에 맞는 새로운 테스트케이스와 테스트오라클이 자동으로 생성되고 이를 실행결과와 비교함으로써 패킷 필터링 결과가 옳은지 혹은 틀린 지를 자동으로 판단할 수 있도록 한 네트워크 보안시스템의 보안성 테스트 방법 및 장치를 제공하는데 목적이 있다.

또한, 본 발명은 테스트 과정에서의 사용자 개입이 최소화되면서 테스트 과정이 전반적으로 자동화될 수 있는 네트워크 보안시스템의 보안성 테스트 방법 및 장치를 제공하는데 목적이 있다.

발명의 구성

이를 위해 본 발명에서는 보안 정책에 따른 패킷 필터링 프로그램의 패킷 필터링 규칙을 파싱(구문분석)하여 필요한 데이터를 추출한 다음 이를 이용하여 다양한 조합의 테스트케이스와 테스트오라클을 체계적으로 자동 생성하는 방법과, 테스트를 자동으로 수행하는 방법과, 테스트결과를 자동으로 산출하는 방법/장치를 제시한다. 즉, 위에서 기술한 테스트케이스와 테스트오라클의 생성을 자동화하여 사용자 개입을 최소화하면서 효과적인 테스트 수행이 이루어질 수 있게 하는 것을 목표로 한다.

이러한 기술적 과제가 달성될 수 있는 본 발명은 예를 들면 청구항 1 및 2에 개시된 바와 같이 패킷 필터링 프로그램을 내장한 시스템 보안용의 패킷필터에 접속되는 특별한 구성의 패킷생성기 및 패킷분석기로 이루어질 수 있다.

여기서, 상기 패킷생성기는 ⓐ 테스트 대상이 되는 패킷 필터링 프로그램의 필터링 규칙을 사용자로부터 입력받아 정확한 규칙인지를 판별하고 입력된 필터링 규칙이 정확한 규칙이면 해당 규칙을 파싱하여 송신/수신측의 IP주소와 포트 정보 및 프로토콜 정보를 추출하는 **규칙해석모듈**과 ⓑ 상기 규칙해석모듈에서 추출된 송신/수신측의 IP주소와 포트 정보 및 프로토콜 정보를 바탕으로 테스트케이스를 생성하는 **테스트케이스생성모듈**과 ⓒ 상기 테스트케이스생성모듈에서 생성된 테스트케이스를 바탕으로 패킷을 자동으로 생성하여 전송하는 **패킷센더**와 ⓓ 상기 테스트케이스생성모듈에서 생성된 테스트케이스와 상기 패킷센더에서 전송된 패킷의 로그 정보를 이용하여 결과판단을 위한 테스트오라클을 자동으로 생성하는 **테스트오라클생성모듈**과 ⓔ 전송된 패킷의 수신 여부를 탐지하여 기록하는 **패킷탐지모듈** 및 ⓕ 테스트 수행에 필요한 정보의 전송 및 동기화를 이루는 **싱크로나이저**로 구성될 수 있다.

이에 반해 상기 패킷분석기는 테스트케이스생성모듈에서 생성된 테스트케이스를 바탕으로 패킷을 자동으로 생성하여 전송하는 **패킷센더**와, 전송된 패킷의 수신 여부를 탐지하여 기록하는 **패킷탐지모듈**과, 테스트 수행에 필요한 정보의 전송 및 동기화를 이루는 **싱크로나이저** 및 상기 패킷탐지모듈에서 생성된 탐지 패킷 로그와 테스트오라클을 이용하여 테스트 결과를 자동으로 산출하는 **결과판정모듈**로 구성될 수 있다.

또한, 본 발명이 제안하는 네트워크 보안시스템의 보안성 테스트 방법은 예를 들면 청구항 3에 개시된 바와 같이, 패킷 필터링 프로그램을 내장한 시스템 보안용의 패킷필터에 패킷생성기와 패킷분석기가 접속되어 시스템의 보안성을 테스트하는 방법에 있어서, 상기 패킷생성기의 규칙해석모듈이 상기 패킷 필터링 프로그램의 필터링 규칙을 파싱하고, 파싱한 필터링 규칙이 기본 정책, 플러딩(Flooding) 정책, 상태기반 정책, 단편화 정책 중 어디에 해당하는 것인지를 판별(115)하여 각각에 맞는 정보를 추출(116) 및 저장하는 **제1 과정**; 상기 제1 과정에서 추출된 정보를 바탕으로 상기 패킷생성기의 테스트케이스생성모듈이 테스트케이스를 생성하는 **제2 과정**; 상기 제2 과정에서 생성된 테스트케이스와 패킷필터의 환경설정정보를 이용하여 패킷을 생성하되 이를 목적지로 보내면서 전송한 패킷에 대한 로그를 남기는 **제3 과정**; 상기 제2 과정에서의 테스트케이스와 제3 과정에서 전송한 패킷의 로그를 이용하여 테스트오라클을 생성하는 **제4 과정**; 및 상기 제4 과정에서 생성된 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 상기 패킷분석기의 결과판정모듈이 비교하여 테스트의 수행결과를 판단하는 **제5 과정**으로 이루어질 수 있다.

이하, 첨부도면을 참조하여 본 발명의 일 예에 따른 네트워크 보안시스템의 보안성 테스트 장치 및 방법에 대해 설명하는데, 하기 실시예에서는 입력 값에 대해 도면 부호 I(input)를 병기하였고 출력 값에 대해서는 O(output)를 병기하였다.

또한, 본 명세서에서 사용되는 "네트워크 보안시스템"이라는 용어는 인트라넷이나 인터넷 등의 통신망을 통해 다른 컴퓨터가 접속되는 컴퓨터 시스템인 것으로 정의한다.

또한, 하기 실시예의 보안성(보안 정책) 테스트 장치 및 방법은 다음의 기능을 포함하고 있는 것으로 미리 정의한다.

ⅰ) 필터링 규칙을 분석해 테스트에 필요한 정보를 추출하는 기능.

ⅱ) 필터링 규칙을 분석하여 다양한 조합의 테스트케이스를 생성하는 기능.

ⅲ) 필터링 규칙을 분석해 그에 맞는 테스트오라클을 생성하는 기능.

iv) 테스트케이스를 기반으로 본 발명의 테스트베드에서 테스트하는 기능.

v) 테스트 수행결과와 테스트오라클을 비교하여 필터링 결과가 오류인지 여부를 판단하는 기능. 여기서, 패킷 필터링 프로그램을 통과하기 전·후의 패킷에 대한 로그(log)와 테스트오라클이 비교되어 테스트결과가 자동으로 산출된다.

실시예

첨부된 도 1은 본 발명의 보안성 테스트 장치에 의해 구현된 테스트베드의 구성도이고, 도 2는 본 발명에 따른 보안성 테스트 장치의 구성도이며, 도 3 내지 8은 본 발명의 보안성 테스트 장치를 구성하는 각 모듈에서의 정보처리과정을 나타낸 플로차트이다.

앞에서 언급한 바와 같이, 본 발명의 보안성 테스트 장치 및 방법은 테스트 대상이 되는 시스템의 필터링 규칙을 분석하여 그 규칙에 맞는 테스트케이스를 자동으로 생성해야 하고, 그에 맞는 테스트오라클도 자동으로 생성해야 하며, 테스트 수행결과를 판단함에 있어서도 사용자가 직접 확인/분석/판단하는 것이 아니라 테스트오라클과 테스트 수행결과를 이용하여 자동으로 산출해야 한다.

이를 위해 본 실시예에서는 도 1과 같이 패킷생성기(100), 패킷분석기(200), 패킷필터(300)로 이루어진 테스트베드(전체 시스템)를 제안한다.

상기 패킷생성기(100)는 테스트 대상이 되는 시스템의 패킷 필터링 규칙을 파싱하여 테스트케이스와 테스트오라클을 자동으로 생성하며, 상기 테스트케이스를 이용하여 실제로 전송할 패킷을 생성하여 목적지로 보내는 역할을 한다.

상기 패킷필터(300)는 라우터나 방화벽 같은 패킷 필터링 프로그램을 내장하고 있는 시스템으로서 테스트 대상이 된다.

상기 패킷분석기(200)는 테스트오라클과 패킷분석기에 도착한 패킷의 로그를 서로 비교하여 패킷필터가 제대로 동작하였는지를 판단한다.

또한, 본 발명의 테스트베드(시스템)는 테스트를 위해 2개의 연결을 갖는다.

그 중 ①번 연결(선)은 테스트용 패킷을 전송하는 선으로서 패킷생성기와 패킷분석기가 패킷필터를 통해 서로 패킷을 서로 주고받는다. 반면, ②번 연결은 테스트 수행시 패킷생성기와 패킷분석기 사이에 동기화를 유지할 수 있고, 테스트에 필요한 정보를 주고받기 위한 선이다. ②번 연결을 통해 전달되는 정보는 패킷생성기와 패킷분석기 사이의 로그 정보 및 테스트오라클 정보와 상태기반의 필터링 규칙 테스트를 위한 동기화 정보이다.

도 2는 본 발명의 일 예에 따른 보안성 테스트 장치의 내부 구조를 나타낸 것으로, 도면에서 보듯이 본 실시예의 패킷생성기(100)는 규칙해석모듈(110), 테스트케이스생성모듈(120), 테스트오라클생성모듈(130), 패킷센더(140), 패킷탐지모듈(150), 싱크로나이저(160)로 구성되어 있다. 이에 대해, 본 실시예의 패킷분석기는 패킷센더(210), 패킷탐지모듈(220), 결과판정모듈(230), 싱크로나이저(240)로 구성되어 있다.

한편, 본 실시예에서는 네트워크 보안시스템의 보안을 위해 제공된 패킷필터의 필터링 규칙을 다음과 같이 4가지로 분류하여 테스팅에 적용한다.

■ 기본 정책에 대한 규칙

■ 플러딩(Flooding) 정책에 대한 규칙

■ 상태기반 정책에 대한 규칙

■ 단편화 정책

이하, 본 실시예의 패킷생성기를 구성하는 각 모듈에 관한 설명한다.

A) 규칙해석모듈(110)

테스트 대상이 되는 필터링 규칙을 사용자로부터 입력으로 받아 테스트케이스와 테스트오라클의 자동 생성에 필요한 정보를 추출한다.

도 3은 필터링 규칙으로부터 테스트케이스와 테스트오라클의 자동 생성에 필요한 정보가 어떻게 추출되는지를 나타낸 것으로서, 테스트 대상이 되는 필터링 규칙(I-110)을 사용자가 입력하면, 규칙해석모듈에서 정확한 규칙인지 판별(111)하여 입력된 규칙이 정확한 규칙이면 해당 규칙을 파싱(113)한 후 송신/수신측의 IP주소와 포트 정보 및 프로토콜 정보를 추출(114, O-114)하고, 잘못된 규칙이면 사용자에게 오류를 통지(112)한다.

이후 파싱한 보안 정책(규칙)이 기본 정책, 플러딩(Flooding) 정책, 상태기반 정책, 단편화 정책 중 어디에 해당하는 것인지를 판별(115)하고 각각에 맞는 정보를 추출(116)하여 저장한다. 여기서, 추출한 정보가 기본 정책(116-1)에 관한 것이면 5-튜플 즉 송신/수신측의 IP주소와 포트 정보 및 프로토콜 정보를 이용하여 허가/거부 정보(O-116-1)를 추출하고, 플러딩(Flooding) 정책(116-2)에 관한 것이면 플러딩(Flooding)을 판별하는 요소인 Rate/Burst 정보와 해당 규칙이 표현하는 단위시간 정보(O-116-2)를 추출하며, 상태기반 정책(116-3)인 경우에는 상태별 허가/거부 정보(O-116-3)를 추출하고, 단편화된 패킷의 처리/수행을 알아보기 위한 단편화 정책(116-4)인 경우에는 패킷을 단편화할 것인지에 대한 정보(O-116-4)를 추출한다.

한편, 다수의 규칙을 대상으로 테스트할 경우(117) 계속해서 다음 규칙에 대해 정보를 추출한다.

B) 테스트케이스생성모듈(120)

규칙해석모듈에서 추출된 정보(O-114, O-116-1~O-116-4)를 바탕으로 테스트케이스를 생성한다. 테스트케이스를 생성할 때에도 기본 정책, 플러딩 정책, 상태기반 정책, 단편화 정책에 따라 테스트케이스를 나누어 생성하는데 이는 시스템의 보안정책을 테스트할 때 정상적인 상태(패킷필터를 통과할 대상)와 비정상적인 상태(패킷필터에서 필터링 할 대상)를 모두 고려하여 테스트하는 것을 반영한다.

참고로, 아래 표는 본 실시예에서 각각의 테스트 대상별로 취한 테스트 정책을 나타낸 것이다.

[표 1]

테스트 대상	정상적 상황	비정상적 상황
기본 정책	주소, 포트, 프로토콜별 허가 패킷 전송 후 정상적으로 전달되었는지 확인	주소, 포트, 프로토콜별 거부 패킷 전송 후 정확히 필터링 되었는지 확인
플러딩 정책	Non-Flooding 패킷 전송 후 모든 패킷이 전달되었는지 확인	Flooding 패킷 전송 후 제어 정책에서 허가하는 수만큼의 패킷이 전달되었는지 확인
상태기반 정책	허가상태 패킷 전송 후 올바른 상태전이가 일어나는지 확인	거부상태 패킷 전송 후 상태 전이가 일어나지 않음을 확인
단편화 정책	허가범위의 단편화 패킷을 전송한 후 올바로 전달되는지 확인	거부범위의 단편화 패킷을 전송 후 필터링 되는지 확인

도 4는 상기 테스트 방법을 반영한 테스트케이스의 생성 과정을 나타낸 것으로, 규칙해석모듈(110)에서 추출된 정보(O-114, O-116-1~O-116-4)를 입력으로 받아들여(121) 어느 정책에 관한 것인지를 판별(122)하고, 각 규칙의 허가/거부 범위를 추출한다.

이에 대해 상술하면, 기본 정책인 경우에는 기본 정책 정보를 읽어(123-1)들여 해당 규칙이 표현하고 있는 허가범위를 도출(124-1)한 다음 전체 도메인을 대상으로 동치 영역 분석과 경계값 분석(125-1)을 통해 테스트케이스를 생성(O-125-1)한다. 예를 들어, IP주소가 192.168.0.1~192.168.0.255인 패킷에 대해 접근을 허가할 경우 해당 IP주소의 범위와 그 범위를 제외한 나머지 범위(해당 범위보다 위 또는 아래 범위)를 갖는 패킷이 테스트케이스가 된다. 이때, 해당 범위에서 추출된 테스트케이스를 이용해서 만들어지는 패킷은 패킷필터를 통과해야 하고, 해당 범위 이외의 범위에서 추출된 테스트케이스를 이용해서 만들어진 패킷은 통과되지 않아야 한다.

플러딩(Flooding) 정책인 경우에는 규칙해석모듈에서 추출한 Rate/Burst 정보와 단위시간 정보(O-116-2)를 읽어(123-2)들인 후 플러딩(Flooding) 상태를 판단하는 기준을 찾아낸다(124-2). 이를 이용해서 정상적인 상태(Non-Flooding)와 비정상적인 상태(Flooding)를 판별하여 테스트케이스를 생성(125-2)한다.

상태기반 정책인 경우에는 규칙해석모듈로부터 추출한 각 상태별 허가/거부 정보(O-116-3)를 읽어(123-3)들여 정상적인 상태전이와 비정상적인 상태전이 정보를 추출(124-3)한다. 이 정보를 이용해서 테스트케이스를 생성(125-3)한다.

단편화 정책인 경우에는 규칙해석모듈에서 추출한 단편화 정보(O-116-4)를 읽어(123-4)들인 후 단편화 패킷의 허가/거부 정보를 추출(124-4)한다. 그리고 그 정보를 이용해 정상적인 상태와 비정상적인 상태에 대한 테스트케이스를 생성(125-4)한다.

C) 테스트오라클생성모듈(130)

테스트오라클생성모듈은 테스트케이스생성모듈(120)에서 생성한 테스트케이스 정보(O-125-1～O-125-4)와 패킷센더(140, 210)에서 생성한 전송 패킷 로그(O-148)를 이용하여 테스트오라클을 생성한다. 이에 따르면, 각각의 테스트케이스에 대해, 전송될 패킷을 추출하여 테스트를 수행한 다음 그 결과를 자동으로 판단할 수 있다.

도 5는 이와 관련된 처리과정을 상세하게 나타낸 것으로 테스트오라클 역시 각각의 테스트 대상에 따라 나뉘어 생성된다.

도면에서 보듯이, 테스트오라클생성모듈은 테스트 대상별로 테스트케이스를 읽어(132-1～132-4)들인 후 이에 해당하는 전송 패킷 로그(O-148)를 읽어(133-1～133-4)들인다.

읽어들인 정보가 기본 정책에 대한 것이면 테스트케이스의 허가범위에 해당하는 전송 패킷을 분석하여 전송되어야 할 패킷을 추출하는 것으로 테스트오라클을 생성(134-1, O-134-1)하고, 플러딩(Flooding) 정책에 관한 것이면 플러딩 기준에 해당하는 테스트케이스를 이용해 도착 가능한 전체 패킷 수를 분석하여 테스트오라클을 생성(134-2, O-134-2)하며, 상태기반 정책에 관한 것이면 정상적인 상태전이를 유도하는 패킷을 분석하여 테스트오라클을 생성(134-3, O-134-3)하고, 단편화 정책에 대한 것이면 테스트케이스를 이용해 도착 가능한 단편화 패킷을 분석하여 테스트오라클을 생성(134-4, O-134-4) 한다.

D) 패킷센더(140)

테스트케이스생성모듈(130)로부터 생성된 테스트케이스(O-125-1～O-125-4)와 네트워크의 환경설정 정보(I-143)를 이용해 패킷을 생성하고, 이를 목적지로 보내며, 보낸 패킷에 대한 로그(148, O-148)를 남긴다.

이와 관련된 처리과정은 도 6과 같다.

도면에서, 패킷센더는 생성된 테스트케이스가 어떤 정책에 대한 규칙인지 판단(141) 한 후 필요한 정보를 읽어(142-1～142-4)들인다.

패킷센더는 보안 정책에 나타난 정보와, 필요할 경우 실제 테스트환경의 네트워크 환경설정 정보를 읽어(143-1～143-4) 실제 패킷을 생성하고 전송(148)한다.

전송될 패킷의 개수(146)는 테스트 횟수를 나타내는 것으로서 사용자의 입력으로 결정되며, 전송되는 패킷은 테스트케이스의 정상적인 상태와 비정상적인 상태를 기반으로 하여 다양한 테스트가 수행될 수 있도록 지원한다.

E) 패킷탐지모듈(150)

패킷생성기(100)로 들어오는 패킷을 탐지(151)하여 로그를 남긴다(154).

패킷탐지모듈에서는 네트워크를 통하여 들어오는 모든 패킷에 대해 테스트와 관련이 있는 패킷인지를 판별(152)한 후 관련이 있는 패킷에 대해서는 로그(O-154)를 남기고, 테스트 종료를 알리는 패킷이 탐지(153)된 때에는 종료한다. 이와 관련된 흐름이 도 7에 나타나 있다.

F) 싱크로나이저(Synchronizer)(160)

②번 연결을 통해 주고받은 패킷에 대한 로그와 테스트오라클을 패킷분석기 쪽으로 보내고, 패킷분석기와의 동기화 정보를 보낸다.

이하에서는 본 실시예의 패킷분석기를 구성하는 각 모듈에 관한 설명한다.

■ 패킷센더(210)

패킷분석기 쪽에서 패킷생성기 쪽으로 보내야 할 패킷을 보낸다.

보낼 패킷에 대한 테스트케이스는 패킷생성기에서 생성하여 ②번 연결을 통해 전달받는다. 보낸 패킷에 대한 정보는 로그를 남기며, 패킷분석기 쪽의 패킷 센더 역시 상술한 패킷생성기 쪽의 패킷센더와 동일한 방법으로 동작한다.

■ 패킷탐지모듈(220)

패킷분석기로 들어오는 패킷을 탐지하여 로그를 남기며, 이 역시도 패킷생성기 쪽의 패킷탐지모듈과 동일한 방법으로 동작한다.

G) 결과판정모듈(230)

테스트오라클(O-134)과 탐지 패킷 로그(O-154)를 분석하여 필터링 결과가 맞는지 판단한다.

이와 관련된 흐름은 도 8에 나타나 있다.

도면에서 보듯이, 테스트오라클(O-134)은 테스트 수행 후 ②번 연결을 통해 패킷생성기로부터 보내진다. 테스트 수행 시에는 패킷탐지모듈(220)의 탐지 패킷 로그(O-154)가 이용되며, 로드된(231, 232) 테스트오라클과 탐지 패킷을 비교(233)하여 테스트 수행결과가 판단(234)된다.

예컨대, 기본 정책에 관한 것이면 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 비교해 통과 가능한 패킷만을 통과시켰는지 자동으로 판별하고, 플러딩 정책에 관한 것이면 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 비교해 허용되는 패킷 수만큼의 패킷만을 통과시켰는지 자동으로 판별하며, 상태기반 정책에 관한 것이면 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 비교해 허용 가능한 상태전이가 이루어졌는지 자동으로 판별하고, 단편화 정책에 관한 것이면 테스트오라클과 상기 패킷분석기에 수신된 패킷의 로그를 비교해 허용 가능한 단편화 패킷만을 통과시켰는지 자동으로 판별하는 것이다. 이때, 테스트 결과에 따라 에러 로그(O-236)와 결과 로그(O-235)를 생성(236, 235)한다.

■ 싱크로나이저(Synchronizer)(240)

패킷생성기로부터 로그 정보와 테스트 오라클을 받고, 패킷분석기 쪽에서 보내야 할 패킷에 대한 정보를 받는다. 또한, 필요하면 패킷생성기와의 동기화 정보를 내보낸다.

이상과 같이 구성되는 본 실시예의 보안성 테스트 장치 및 방법은 다음과 같이 동작한다.

먼저, 패킷생성기(100)에서는 패킷필터(300)의 보안 정책(규칙)을 규칙해석모듈(110)에서 해석하여 필요한 정보를 얻고, 그 정보를 이용하여 테스트케이스생성모듈(120)에서 테스트케이스를 생성하며, 이 테스트케이스에 따라 패킷을 생성한 다음 패킷센더(140)를 통해 패킷분석기(200)에 타겟으로 전송한다. 또한, 계속해서 전송한 패킷을 로그로 남긴다.

이어, 테스트오라클생성모듈(130)은 테스트케이스와 전송된 패킷의 로그(O-148)를 입력으로 하여 테스트오라클(O-134)을 생성하고, 이렇게 하여 생성된 테스트오라클을 싱크로나이저와 도 1의 ②번 연결을 통해 패킷분석기(200)에 보낸다.

이에 따라 패킷분석기의 패킷탐지모듈(220)이 수신 패킷에 대한 로그를 남기게 되며, ②번 연결을 통해 전달된 테스트오라클이 결과판정모듈(230)로 보내져 테스트 결과가 판정된다.

발명의 효과

이상과 같이 본 발명의 일 예에 따른 네트워크 보안시스템의 보안성 테스트 장치 및 방법에 의하면, 테스트의 준비로부터 테스트 결과의 평가에 이르기까지 전 과정이 자동으로 진행됨으로 테스트 과정에서의 사용자 개입을 최소화할 수 있으며, 시스템의 보안 정책에 대한 신뢰성을 향상할 수 있고, 보안성 테스트를 위한 수행시간의 단축을 기대할 수 있다.

도면의 간단한 설명

도 1은 본 발명의 보안성 테스트 장치에 의해 구현된 테스트베드의 구성도.

도 2는 본 발명에 따른 보안성 테스트 장치의 구성도.

도 3은 본 발명의 보안성 테스트 장치를 구성하는 규칙해석모듈에서 테스트의 대상이 되는 네트워크 시스템의 보안규칙(정책)을 분석하여 필요한 정보를 추출하는 과정을 나타낸 플로차트.

도 4는 본 발명의 보안성 테스트 장치를 구성하는 테스트케이스생성모듈에서 테스트케이스를 자동으로 생성하는 과정을 나타낸 플로차트.

도 5는 본 발명의 보안성 테스트 장치를 구성하는 테스트오라클생성모듈에서 테스트오라클을 자동으로 생성하는 과정을 나타낸 플로차트.

도 6은 본 발명의 보안성 테스트 장치를 구성하는 패킷센더에서 테스트케이스를 기반으로 전송할 패킷을 생성하여 전송하는 과정을 나타낸 플로차트.

도 7은 본 발명의 보안성 테스트 장치를 구성하는 패킷탐지모듈에서 전송한 패킷을 탐지하여 기록하는 과정을 나타낸 플로차트.

도 8은 본 발명의 보안성 테스트 장치를 구성하는 결과판정모듈에서 테스트오라클과 전송된 패킷의 로그를 분석해 테스트 결과를 산출하는 과정을 나타낸 플로차트.

[도면 부호의 설명]

100… 패킷생성기 110… 규칙해석모듈

120… 테스트케이스생성모듈 130… 테스트오라클생성모듈

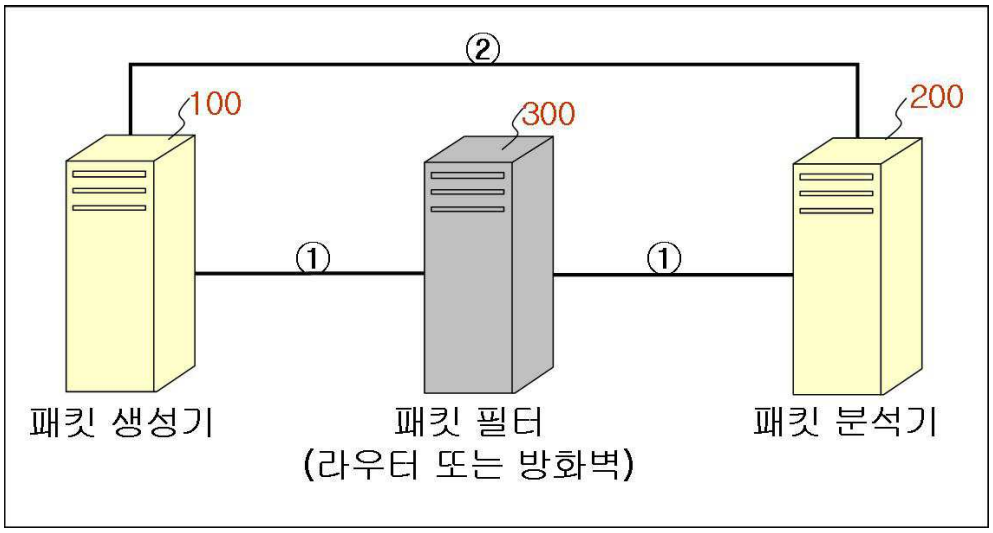
140,210… 패킷센더 150,220… 패킷탐지모듈

160,240… 싱크로나이저 200… 패킷분석기

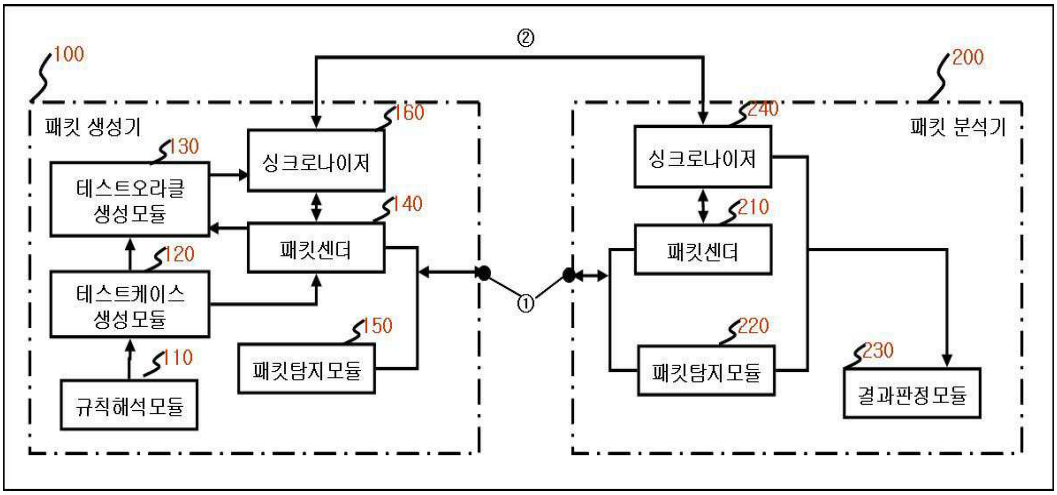
230… 결과판정모듈 300… 패킷필터

도면

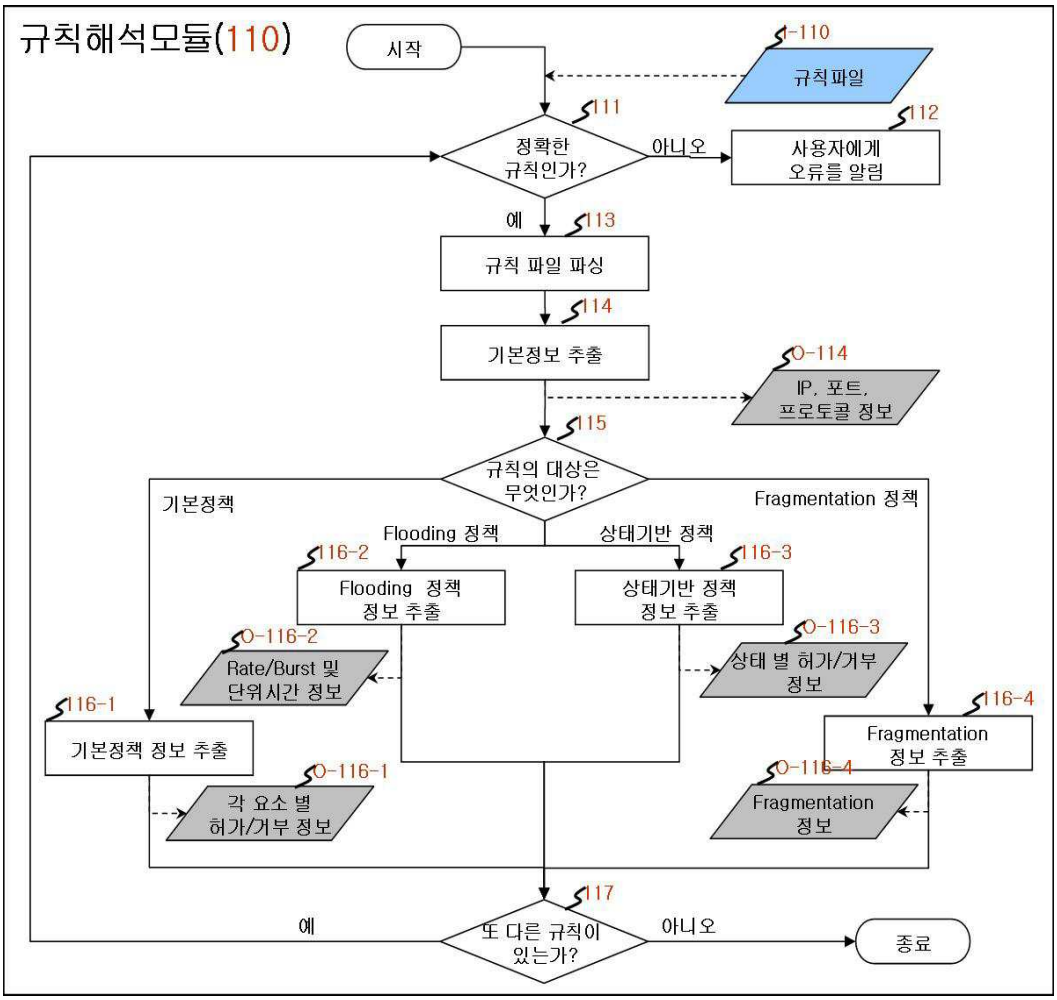
도면1


②
100
300
200
①
①
패킷 생성기
패킷 필터
(라우터 또는 방화벽)
패킷 분석기

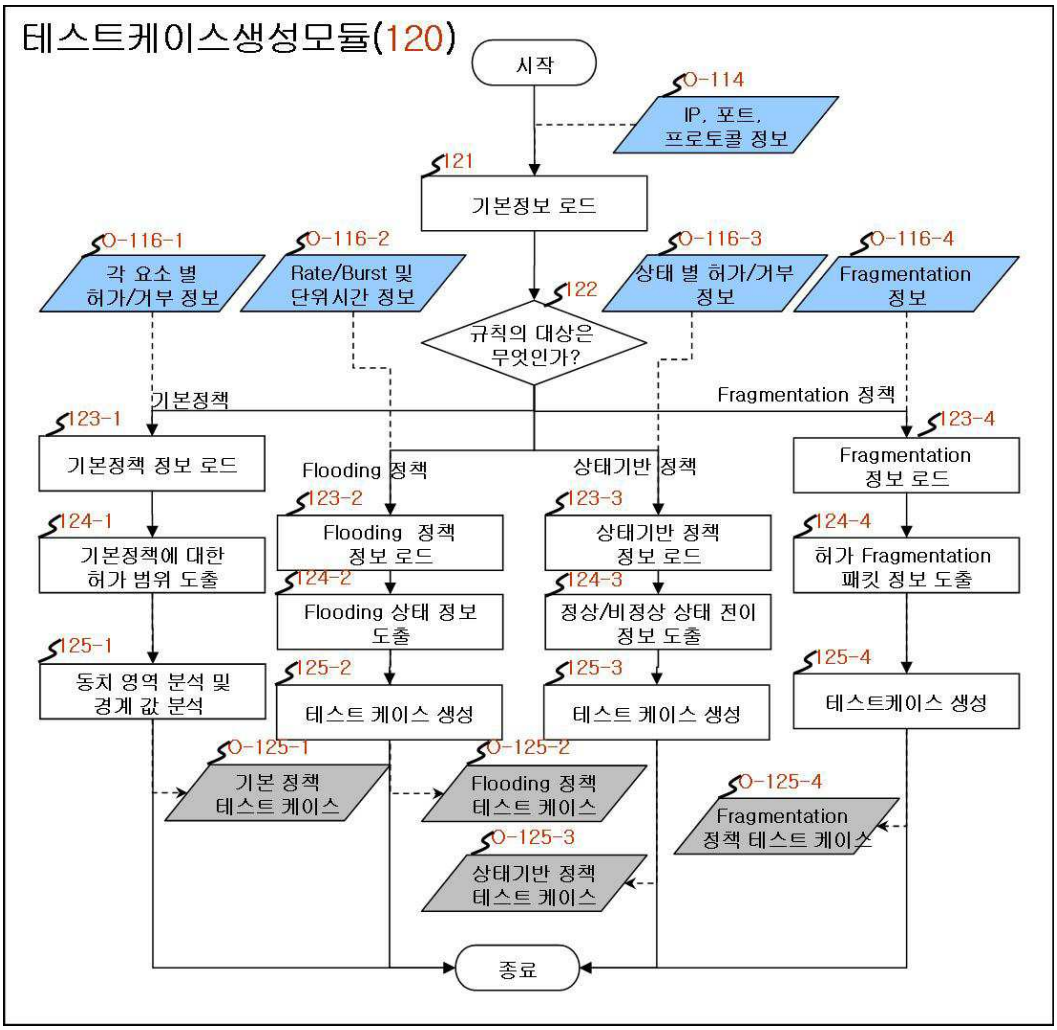
도면2


②
100
200
패킷 생성기
160
싱크로나이저
130
테스트오라클
생성모듈
140
패킷센더
120
테스트케이스
생성모듈
150
패킷탐지모듈
110
규칙해석모듈
①
240
싱크로나이저
패킷 분석기
210
패킷센더
220
패킷탐지모듈
230
결과판정모듈

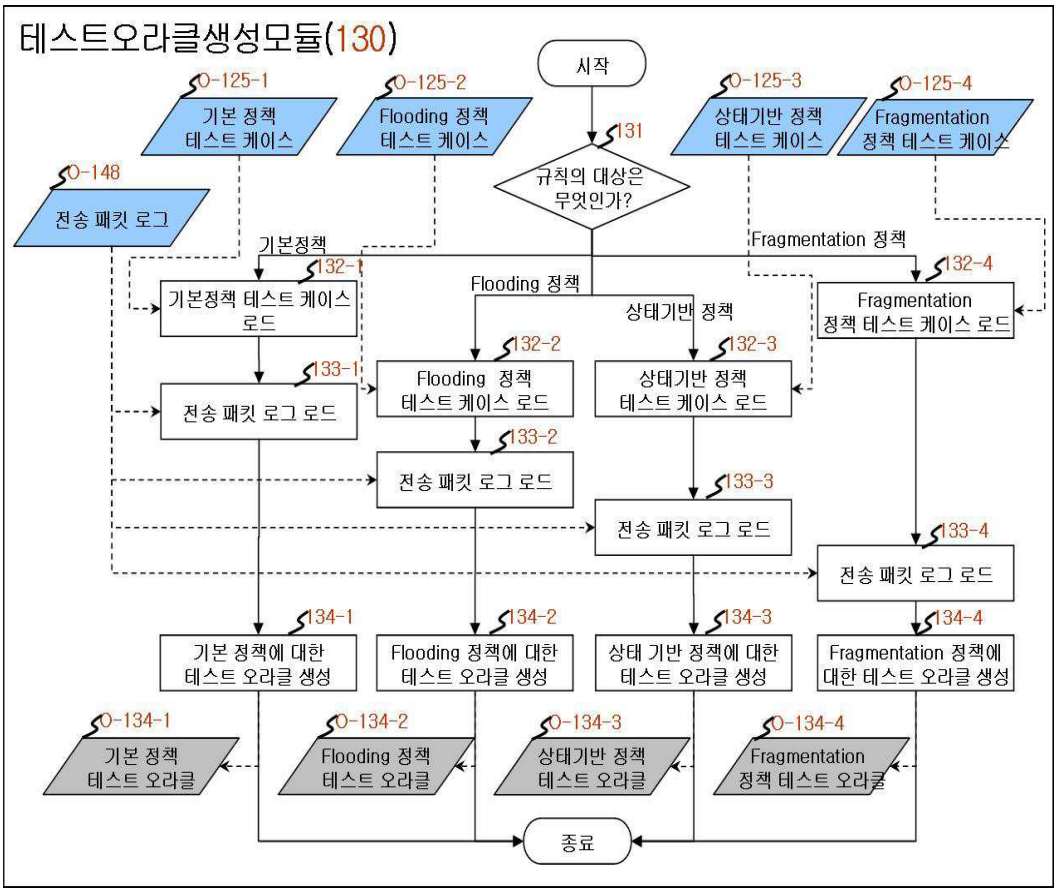
도면3


규칙해석모듈(110)
시작
110
규칙파일
111
정확한 규칙인가?
아니오
112
사용자에게 오류를 알림
예
113
규칙 파일 파싱
114
기본정보 추출
O-114
IP, 포트, 프로토콜 정보
115
규칙의 대상은 무엇인가?
기본정책
Flooding 정책
상태기반 정책
Fragmentation 정책
116-2
Flooding 정책 정보 추출
116-3
상태기반 정책 정보 추출
O-116-2
Rate/Burst 및 단위시간 정보
O-116-3
상태 별 허가/거부 정보
116-1
기본정책 정보 추출
116-4
Fragmentation 정보 추출
O-116-1
각 요소 별 허가/거부 정보
O-116-4
Fragmentation 정보
117
또 다른 규칙이 있는가?
예
아니오
종료

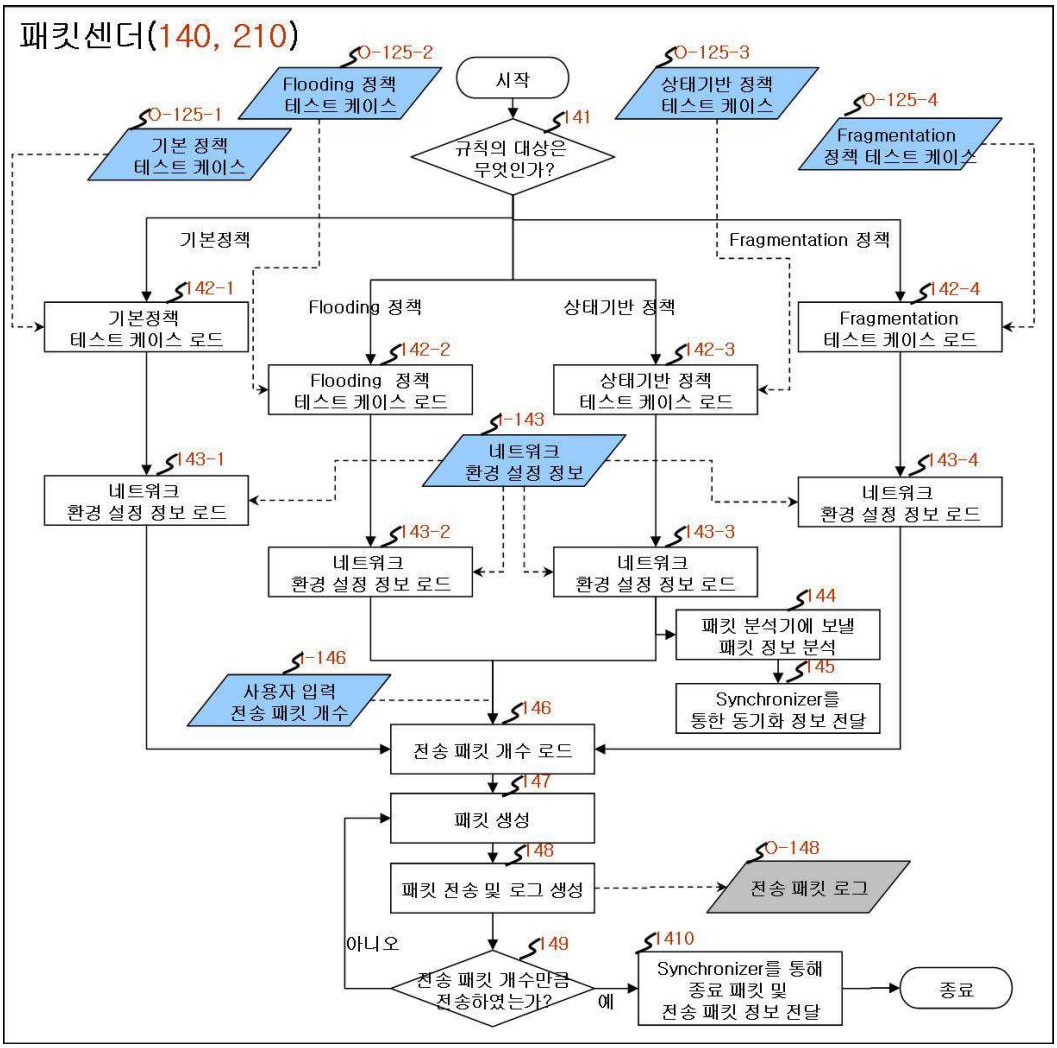
도면4


테스트케이스생성모듈(120)
시작
O-114
IP, 포트,
프로토콜 정보
121
기본정보 로드
O-116-1
각 요소 별
허가/거부 정보
O-116-2
Rate/Burst 및
단위시간 정보
O-116-3
상태 별 허가/거부
정보
O-116-4
Fragmentation
정보
122
규칙의 대상은
무엇인가?
기본정책
Fragmentation 정책
123-1
기본정책 정보 로드
Flooding 정책
상태기반 정책
123-4
Fragmentation
정보 로드
123-2
Flooding 정책
정보 로드
123-3
상태기반 정책
정보 로드
124-1
기본정책에 대한
허가 범위 도출
124-2
Flooding 상태 정보
도출
124-3
정상/비정상 상태 전이
정보 도출
124-4
허가 Fragmentation
패킷 정보 도출
125-1
동치 영역 분석 및
경계 값 분석
125-2
테스트 케이스 생성
125-3
테스트 케이스 생성
125-4
테스트케이스 생성
O-125-1
기본 정책
테스트 케이스
O-125-2
Flooding 정책
테스트 케이스
O-125-4
Fragmentation
정책 테스트 케이스
O-125-3
상태기반 정책
테스트 케이스
종료

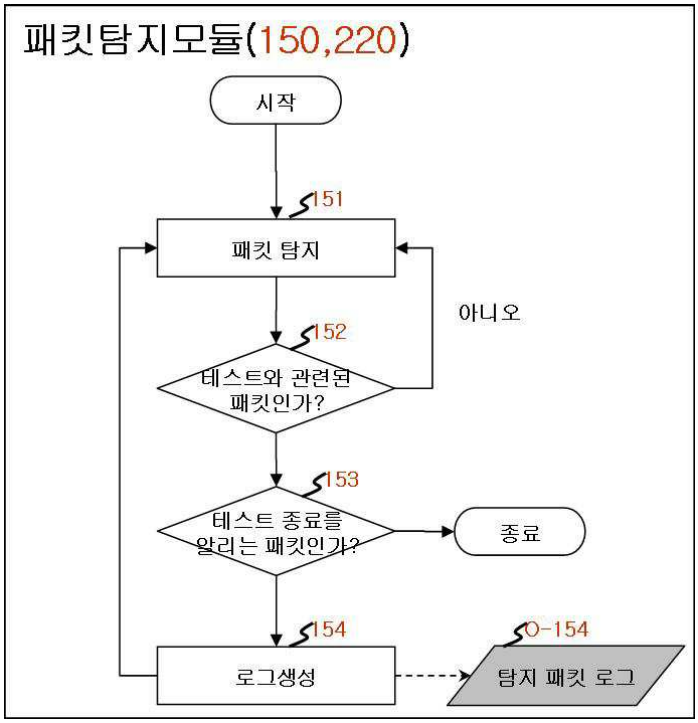
도면5


테스트오라클생성모듈(130)
시작
O-125-1
기본 정책 테스트 케이스
O-125-2
Flooding 정책 테스트 케이스
O-125-3
상태기반 정책 테스트 케이스
O-125-4
Fragmentation 정책 테스트 케이스
131
규칙의 대상은 무엇인가?
O-148
전송 패킷 로그
기본정책
Flooding 정책
상태기반 정책
Fragmentation 정책
132-1
기본정책 테스트 케이스 로드
132-2
Flooding 정책 테스트 케이스 로드
132-3
상태기반 정책 테스트 케이스 로드
132-4
Fragmentation 정책 테스트 케이스 로드
133-1
전송 패킷 로그 로드
133-2
전송 패킷 로그 로드
133-3
전송 패킷 로그 로드
133-4
전송 패킷 로그 로드
134-1
기본 정책에 대한 테스트 오라클 생성
134-2
Flooding 정책에 대한 테스트 오라클 생성
134-3
상태 기반 정책에 대한 테스트 오라클 생성
134-4
Fragmentation 정책에 대한 테스트 오라클 생성
O-134-1
기본 정책 테스트 오라클
O-134-2
Flooding 정책 테스트 오라클
O-134-3
상태기반 정책 테스트 오라클
O-134-4
Fragmentation 정책 테스트 오라클
종료

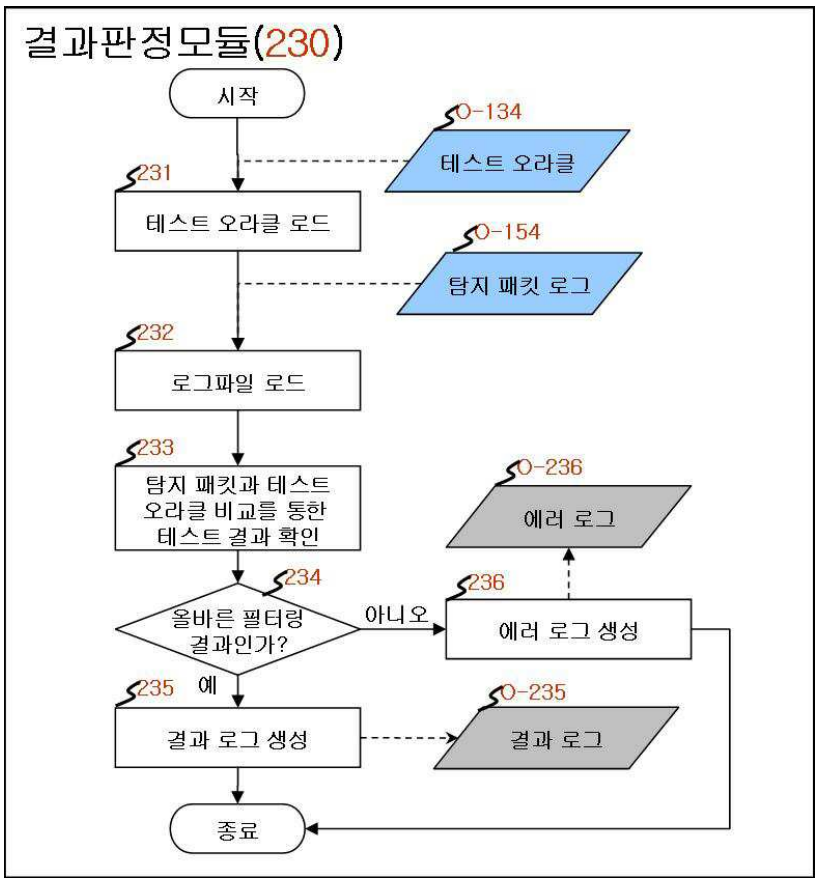
도면6


패킷센더(140, 210)
시작
141
규칙의 대상은 무엇인가?
기본정책
Flooding 정책
상태기반 정책
Fragmentation 정책
O-125-1
기본 정책 테스트 케이스
O-125-2
Flooding 정책 테스트 케이스
O-125-3
상태기반 정책 테스트 케이스
O-125-4
Fragmentation 정책 테스트 케이스
142-1
기본정책 테스트 케이스 로드
142-2
Flooding 정책 테스트 케이스 로드
142-3
상태기반 정책 테스트 케이스 로드
142-4
Fragmentation 테스트 케이스 로드
143
네트워크 환경 설정 정보
143-1
네트워크 환경 설정 정보 로드
143-2
네트워크 환경 설정 정보 로드
143-3
네트워크 환경 설정 정보 로드
143-4
네트워크 환경 설정 정보 로드
144
패킷 분석기에 보낼 패킷 정보 분석
145
Synchronizer를 통한 동기화 정보 전달
146
사용자 입력 전송 패킷 개수
146
전송 패킷 개수 로드
147
패킷 생성
148
패킷 전송 및 로그 생성
O-148
전송 패킷 로그
아니오
149
전송 패킷 개수만큼 전송하였는가?
예
1410
Synchronizer를 통해 종료 패킷 및 전송 패킷 정보 전달
종료

도면7


패킷탐지모듈(150,220)
시작
151
패킷 탐지
152
테스트와 관련된 패킷인가?
아니오
153
테스트 종료를 알리는 패킷인가?
종료
154
로그생성
O-154
탐지 패킷 로그

도면8


결과판정모듈(230)
시작
O-134
테스트 오라클
231
테스트 오라클 로드
O-154
탐지 패킷 로그
232
로그파일 로드
233
탐지 패킷과 테스트
오라클 비교를 통한
테스트 결과 확인
O-236
에러 로그
234
올바른 필터링
결과인가?
아니오
236
에러 로그 생성
예
235
결과 로그 생성
O-235
결과 로그
종료