(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 12/26 (2006.01)
H04L 12/28 (2006.01)
H04L 12/24 (2006.01)

(45) 공고일자 2007년05월09일
(11) 등록번호 10-0716620
(24) 등록일자 2007년05월03일

(21) 출원번호 10-2005-0075223
(22) 출원일자 2005년08월17일
심사청구일자 2005년08월17일

(65) 공개번호 10-2007-0020870
(43) 공개일자 2007년02월22일

(73) 특허권자 고려대학교 산학협력단

(72) 발명자 최현상

이희조

(74) 대리인 유미특허법인

(56) 선행기술조사문헌
KR1020030003981 A
KR1020060013120 A

심사관 : 김병균

전체 청구항 수 : 총 28 항

(54) 평행 좌표계를 이용한 네트워크 감시 장치 및 방법

(57) 요약

네트워크를 감시하거나 분석하는 장치 및 방법이 개시된다.

네트워크 감시 장치는 네트워크 상의 패킷을 수집하고, 수집한 패킷으로부터 공격 패킷을 추출하며, 추출된 패킷을 평행 좌표계에 나타내는 시각화 정보를 생성한다.

이로써, 네트워크 상에 존재하는 공격 패킷을 시각적으로 용이하게 파악할 수 있다.

대표도

도 2

특허청구의 범위

청구항 1.

제1 네트워크를 감시하는 네트워크 감시 장치에 있어서,

상기 제1 네트워크의 패킷을 수집하는 네트워크 패킷 수집부;

상기 패킷에 포함되어 있는 복수의 파라미터를 평행축으로 하는 평행 좌표계에 상기 패킷을 표시하여 상기 제1 네트워크 상에 존재하는 공격의 시각화 패턴이 나타내는 시각화 정보를 생성하는 시각화 정보 생성부를 포함하고,

상기 복수의 파라미터는 패킷의 출발지 주소, 패킷의 목적지 주소, 패킷의 목적지 포트 및 패킷의 길이를 포함하는 네트워크 감시 장치.

청구항 2.

제1항에 있어서,

상기 네트워크 감시 장치는 상기 패킷 중에서 공격 패킷을 추출하는 공격 패킷 추출부를 더 포함하고,

상기 시각화 정보 생성부는 상기 공격 패킷으로 시각화 정보를 생성하는 네트워크 감시 장치.

청구항 3.

제2항에 있어서,

상기 공격 패킷 추출부는,

동일한 값은 1회만 저장되는 하나 이상의 파라미터 저장부;

상기 패킷에 포함된 복수의 파라미터 별로 상기 파라미터의 값이 상기 파라미터 저장부에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 공격 유형 식별자 생성부;

공격 유형 별로 패킷이 저장되는 공격 패킷 저장부;

상기 공격 유형 식별자에 따라 상기 패킷을 상기 공격 패킷 저장부에 저장하는 패킷 저장 제어부;

상기 공격 패킷 저장부에 소정의 개수 이상의 패킷이 저장되는 경우 상기 공격 패킷 저장부에 저장되어 있는 패킷을 상기 시각화 정보 생성부에 제공하는 공격 패킷 제공부를 포함하는 네트워크 감시 장치.

청구항 4.

제3항에 있어서,

상기 파라미터 저장부는 소정의 시간이 경과하면 클리어되는 네트워크 감시 장치.

청구항 5.

제3항에 있어서,

상기 공격 패킷 저장부는 소정의 시간이 경과하면 클리어되는 네트워크 감시 장치.

청구항 6.

제3항에 있어서,

상기 공격 패킷이 존재하면 경고 정보를 생성하는 경고 정보 생성부;

상기 경고 정보를 상기 제1 네트워크를 통해 원격의 장치에 전송하는 네트워크 상태 정보 송신부를 더 포함하는 네트워크 감시 장치.

청구항 7.

제3항에 있어서,

상기 공격 패킷이 존재하면 경고 정보를 생성하는 경고 정보 생성부;

상기 경고 정보를 제2 네트워크를 통해 원격의 장치에 전송하는 네트워크 상태 정보 송신부를 더 포함하는 네트워크 감시 장치.

청구항 8.

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 시각화 정보를 상기 제1 네트워크를 통해 원격의 장치에 전송하는 네트워크 상태 정보 송신부를 더 포함하는 네트워크 감시 장치.

청구항 9.

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 제1 네트워크를 통해 네트워크 상태 정보 요청을 수신하는 네트워크 상태 정보 요청 수신부; 및

상기 네트워크 상태 정보 요청이 있는 경우 상기 시각화 정보를 상기 제1 네트워크를 통해 원격의 장치에 전송하는 네트워크 상태 정보 송신부를 포함하는 네트워크 감시 장치.

청구항 10.

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 시각화 정보를 제2 네트워크를 통해 원격의 장치에 전송하는 네트워크 상태 정보 송신부를 더 포함하는 네트워크 감시 장치.

청구항 11.

제1항 내지 제7항 중 어느 한 항에 있어서,

제2 네트워크를 통해 네트워크 상태 정보 요청을 수신하는 네트워크 상태 정보 요청 수신부; 및

상기 네트워크 상태 정보 요청이 있는 경우 상기 시각화 정보를 상기 제2 네트워크를 통해 원격의 장치에 전송하는 네트워크 상태 정보 송신부를 포함하는 네트워크 감시 장치.

청구항 12.

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 시각화 정보를 디스플레이 장치에 표시하는 시각화 정보 표시부를 더 포함하는 네트워크 감시 장치.

청구항 13.

제1 네트워크를 감시하는 네트워크 감시 방법에 있어서,

상기 제1 네트워크의 패킷을 수집하는 단계;

상기 패킷에 포함되어 있는 복수의 파라미터를 평행축으로 하는 평행 좌표계에 상기 패킷을 표시하여 상기 제1 네트워크 상에 존재하는 공격의 시각화 패턴이 나타내는 시각화 정보를 생성하는 단계를 포함하고,

상기 복수의 파라미터는 패킷의 출발지 주소, 패킷의 목적지 주소, 패킷의 목적지 포트 및 패킷의 길이를 포함하는 네트워크 감시 방법.

청구항 14.

제13항에 있어서,

상기 네트워크 감시 방법은 상기 패킷 중에서 공격 패킷을 추출하는 단계를 더 포함하고,

상기 시각화 정보를 생성하는 단계는 상기 공격 패킷으로 시각화 정보를 생성하는 네트워크 감시 방법.

청구항 15.

제14항에 있어서,

상기 공격 패킷을 추출하는 단계는,

상기 패킷에 포함된 복수의 파라미터의 값을 동일값이 다시 저장되지 않는 파라미터 저장 수단에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 단계;

상기 공격 유형 식별자에 따라 상기 패킷을 공격 유형 별로 패킷 저장 수단에 저장하는 단계를 포함하는 네트워크 감시 방법.

청구항 16.

제15항에 있어서,

상기 공격 패킷을 추출하는 단계는,

상기 파라미터 저장 수단을 소정의 시간마다 클리어하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 17.

제15항에 있어서,

상기 공격 패킷을 추출하는 단계는,

상기 패킷 저장 수단을 소정의 시간마다 클리어하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 18.

제14항에 있어서,

상기 공격 패킷이 존재하면 경고 정보를 생성하는 단계;

상기 경고 정보를 상기 제1 네트워크를 통해 원격의 장치에 전송하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 19.

제14항에 있어서,

상기 공격 패킷이 존재하면 경고 정보를 생성하는 단계;

상기 경고 정보를 상기 제2 네트워크를 통해 원격의 장치에 전송하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 20.

제13항 내지 제19항 중 어느 한 항에 있어서,

상기 제1 네트워크를 통해 원격의 장치에 상기 시각화 정보를 전송하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 21.

제13항 내지 제19항 중 어느 한 항에 있어서,

상기 네트워크 감시 방법은 상기 제1 네트워크를 통해 네트워크 상태 정보 요청을 수신하는 단계; 및

상기 네트워크 상태 정보 요청이 있는 경우 상기 제1 네트워크를 통해 원격의 장치에 상기 시각화 정보를 전송하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 22.

제13항 내지 제19항 중 어느 한 항에 있어서,

상기 제2 네트워크를 통해 원격의 장치에 상기 시각화 정보를 전송하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 23.

제13항 내지 제19항 중 어느 한 항에 있어서,

상기 네트워크 감시 방법은 상기 제2 네트워크를 통해 네트워크 상태 정보 요청을 수신하는 단계; 및

상기 네트워크 상태 정보 요청이 있는 경우 상기 제2 네트워크를 통해 원격의 장치에 상기 시각화 정보를 전송하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 24.

제13항 내지 제19항 중 어느 한 항에 있어서,

상기 시각화 정보를 디스플레이 장치에 표시하는 단계를 더 포함하는 네트워크 감시 방법.

청구항 25.

제1 네트워크를 분석하는 네트워크 분석 장치에 있어서,

상기 제1 네트워크로부터 패킷을 수집하는 네트워크 패킷 수집부;

동일한 값은 1회만 저장되는 하나 이상의 파라미터 저장부;

상기 패킷에 포함된 복수의 파라미터에 해당하는 값이 상기 파라미터 저장부에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 공격 유형 식별자 생성부를 포함하는 네트워크 분석 장치.

청구항 26.

제25항에 있어서,

공격 유형 별로 패킷이 저장되는 공격 패킷 저장부;

상기 공격 유형 식별자에 따라 상기 패킷을 상기 공격 패킷 저장부에 저장하는 패킷 저장 제어부를 더 포함하는 네트워크 분석 장치.

청구항 27.

제1 네트워크 상의 패킷의 공격 유형을 식별하는 패킷 공격 유형 식별 방법 에 있어서,

상기 제1 네트워크로부터 패킷을 수집하는 단계;

상기 패킷에 포함된 복수의 파라미터에 해당하는 값을 동일한 값은 1회만 저장되는 파라미터 저장 수단에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 단계를 포함하는 패킷 공격 유형 식별 방법.

청구항 28.

제1 네트워크 상의 패킷을 공격 유형 별로 분류하는 패킷 분류 방법에 있어서,

상기 제1 네트워크로부터 패킷을 수집하는 단계;

상기 패킷에 포함된 복수의 파라미터에 해당하는 값을 동일한 값은 1회만 저장되는 파라미터 저장 수단에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 단계;

상기 공격 유형 식별자에 따라 상기 패킷을 공격 유형 별로 패킷 저장 수단에 저장하는 단계를 포함하는 패킷 분류 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크 감시 장치 및 방법에 관한 것이다.

특히 본 발명은 네트워크의 상태를 시각적으로 파악할 수 있도록 하는 감시 장치 및 감시 방법에 관한 것이다.

인터넷의 발달과 급격한 사용자의 증가로 인해 오늘날의 네트워크는 복잡하고 다양한 종류의 트래픽들로 포화 상태에 이르고 있다. 이러한 방대한 트래픽 정보 중에서 악성 트래픽 정보를 빠르게 감지하는 것은 그 정보의 방대함 때문에 쉽지 않다.

악성 트래픽의 종류에는 스캔 공격(Scan Attack), 도스 공격(Denial of Service, 서비스 거부 공격), 인터넷 웜 등이 있다.

스캔 공격은 시스템, 네트워크 등의 허점을 파악하기 위한 공격으로 해킹을 위한 전 단계의 공격이다. 스캔 공격에는 포트 스캔 공격(Port Scan Attack), 호스트 스캔 공격(Host Scan Attack), 분산 호스트 스캔 공격(Distributed Host Scan) 등이 있다. 포트 스캔 공격은 한 호스트의 열린 포트를 검색하기 위한 공격이고 호스트 스캔 공격은 공격 가능한 호스트를 검색하기 위한 공격이다. 분산 호스트 스캔 공격은 공격 가능한 호스트를 검색하되 출발지를 바꾸어 가면서 수행하는 공격이다.

도스 공격은 시스템 또는 네트워크의 리소스를 독점하여 다른 사용자들이 해당 시스템 또는 네트워크의 서비스를 정상적으로 사용하는 것을 방해하는 공격이다. 보통 도스 공격은 서버나 네트워크에 불필요한 정보를 쏟아 부어 과부하 상태를 일으켜 다른 정당한 사용자들의 접근을 금지 시키는 방법을 취한다. 서비스 거부 공격의 예로 출발지 속임 도스 공격, 다중 포트 도스 공격, 네트워크 대향 도스 공격 등이 있다. 출발지 속임 도스 공격은 출발지 주소를 다양하게 바꾸어 한 서버에 과다 정보를 제공하여 서버를 다운 시키거나 이용 불능 상태로 만드는 공격으로 출발지를 속임으로써 공격 주체 및 공격의 존재를 파악하기 힘들게 한다. 다중 포트 도스 공격은 출발지 주소를 다양하게 바꾸어 한 목적지 서버를 공격하되 공격하는 목적지 포트도 다양하게 하여 목적지 서버가 과부하 상태에 이르게 한다. 네트워크 대향 도스 공격은 출발지 주소, 목적지 주소, 포트 번호 등을 무작위로 바꾸어가면서 과다한 패킷을 네트워크에 쏟아 부어 네트워크 전체를 이용 불능 상태로 만드는 공격이다.

인터넷 웜은 스스로 자신의 코드를 여러 불특정한 목적지에 전파하는 악성코드이다. 웜에 의해 만들어지는 악성 트래픽은 호스트 스캔과 그 형태가 유사하나, 호스트 스캔의 경우 그 패킷들이 데이터를 담지 않고 헤더만으로 이루어진 경우가 대부분이라 그 크기가 40Byte 혹은 48Byte (TCP 헤더의 옵션부분이 사용된 경우)가 되지만 웜에 의해 만들어지는 패킷들은 웜 자신의 코드가 데이터부분에 포함되어 있으므로 그 크기가 48Byte 이상인 경우가 대부분이며 웜의 종류에 따라 일정한 크기를 갖는다.

이외에 백스캐터와 같이 실제 공격은 아니지만 다른 공격으로 인해 만들어지는 특수한 트래픽 또한 존재한다. 백스캐터는 도스 공격을 받는 목적지에서 이에 응답하는 패킷들로 인해 만들어 지는 트래픽으로 하나의 출발지로부터 다수의 목적지와 다수 혹은 하나의 포트 값을 갖는 특이한 패턴을 갖는다.

이러한 악성 트래픽은 네트워크 사용자의 불편을 야기하고, 네트워크 대역폭의 상당 부분을 차지한다. 따라서 이러한 악성 트래픽을 좀 더 쉽게 인지하기 위한 연구가 많이 진행되고 있다.

특히, 공개 특허 제2004-0072365호에는 3차원 직교 그래프를 이용하여 네트워크의 상태를 표시하는 방법이 소개되어 있다. 그러나 3차원 직교 그래프는 생성이 용이하지 않으므로 이 방법은 구현되기 다소 쉽지 않다. 또한 입체 형상을 평면상에 나타내므로 네트워크의 상태를 한 눈에 파악하기에는 다소 어려움이 있다. 그리고 3차원 직교 그래프는 축이 3개로 한정되어 있어 네트워크의 상태를 파악하기 위한 파라미터가 3개로 한정될 수 밖에 없다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 네트워크의 상태를 시각적으로 용이하게 파악할 수 있도록 하는 감시 장치 및 감시 방법을 제공하는 것이다.

발명의 구성

본 발명의 특징에 따른 네트워크 감시 장치는 제1 네트워크를 감시하는 장치로써, 제1 네트워크의 패킷을 수집하는 네트워크 패킷 수집부, 상기 패킷에 포함되어 있는 하나 이상의 파라미터를 평행축으로 하는 평행 좌표계에 상기 패킷을 나타내는 시각화 정보를 생성하는 시각화 정보 생성부를 포함한다.

이때, 상기 네트워크 감시 장치는 상기 패킷 중에서 공격 패킷을 추출하는 공격 패킷 추출부를 더 포함하고, 상기 시각화 정보 생성부는 상기 공격 패킷으로 시각화 정보를 생성할 수 있다.

여기서, 상기 공격 패킷 추출부는 동일한 값은 1회만 저장되는 하나 이상의 파라미터 저장부, 상기 패킷에 포함된 하나 이상의 파라미터 별로 상기 파라미터의 값이 상기 파라미터 저장부에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 공격 유형 식별자 생성부, 공격 유형 별로 패킷이 저장되는 공격 패킷 저장부, 상기 공격 유형 식별자에 따라 상기 패킷을 상기 공격 패킷 저장부에 저장하는 패킷 저장 제어부, 상기 공격 패킷 저장부에 소정의 개수 이상의 패킷이 저장되는 경우 상기 공격 패킷 저장부에 저장되어 있는 패킷을 상기 시각화 정보 생성부에 제공하는 공격 패킷 제공부를 포함할 수 있다.

본 발명의 특징에 따른 네트워크 감시 방법은, 제1 네트워크를 감시하는 방법으로써, 제1 네트워크의 패킷을 수집하는 단계, 상기 패킷에 포함되어 있는 하나 이상의 파라미터를 평행축으로 하는 평행 좌표계에 상기 패킷을 나타내는 시각화 정보를 생성하는 단계를 포함한다.

이때, 상기 네트워크 감시 방법은 상기 패킷 중에서 공격 패킷을 추출하는 단계를 더 포함하고, 상기 시각화 정보를 생성하는 단계는 상기 공격 패킷으로 시각화 정보를 생성할 수 있다.

여기서, 상기 공격 패킷을 추출하는 단계는, 상기 패킷에 포함된 하나 이상의 파라미터의 값을 동일값이 다시 저장되지 않는 파라미터 저장 수단에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 단계, 상기 공격 유형 식별자에 따라 상기 패킷을 공격 유형 별로 패킷 저장 수단에 저장하는 단계를 포함할 수 있다.

본 발명의 특징에 따른 네트워크 분석 장치는 제1 네트워크를 분석하는 장치로써, 상기 제1 네트워크로부터 패킷을 수집하는 네트워크 패킷 수집부, 동일한 값은 1회만 저장되는 하나 이상의 파라미터 저장부, 상기 패킷에 포함된 하나 이상의 파라미터에 해당하는 값이 상기 파라미터 저장부에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 공격 유형 식별자 생성부를 포함한다.

이때, 상기 네트워크 분석 장치는 공격 유형 별로 패킷이 저장되는 공격 패킷 저장부, 상기 공격 유형 식별자에 따라 상기 패킷을 상기 공격 패킷 저장부에 저장하는 패킷 저장 제어부를 더 포함할 수 있다.

본 발명의 특징에 따른 패킷 공격 유형 식별 방법은 제1 네트워크 상의 패킷의 공격 유형을 식별하는 방법으로써, 상기 제1 네트워크로부터 패킷을 수집하는 단계, 상기 패킷에 포함된 하나 이상의 파라미터에 해당하는 값을 동일한 값은 1회만 저장되는 파라미터 저장 수단에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 단계를 포함한다.

본 발명의 특징에 따른 패킷 분류 방법은 제1 네트워크 상의 패킷을 공격 유형 별로 분류하는 방법으로써, 상기 제1 네트워크로부터 패킷을 수집하는 단계, 상기 패킷에 포함된 하나 이상의 파라미터에 해당하는 값을 동일한 값은 1회만 저장되는 파라미터 저장 수단에 저장 가능한 지 여부에 따라 공격 유형 식별자를 생성하는 단계, 상기 공격 유형 식별자에 따라 상기 패킷을 공격 유형 별로 패킷 저장 수단에 저장하는 단계를 포함한다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

이하에서는 본 발명의 실시예에 따른 네트워크 감시 장치가 설치된 네트워크 환경을 도 1을 참고하여 설명한다.

도 1은 본 발명의 실시예에 따른 네트워크 감시 장치가 설치된 네트워크 환경을 도시한 도면이다.

도 1에 도시된 바와 같이 본 발명의 실시예에 따른 네트워크 환경은 컴퓨터, 라우터, 서버 등의 네트워크 장치(10), 네트워크(20) 및 네트워크 감시 장치(100)를 포함한다.

네트워크(20)는 각 네트워크 장치(10) 및 네트워크 감시 장치(100)간에 정보를 교환하는 망이다. 네트워크(20)는 유선 또는 무선 네트워크 모두가 가능하다. 예를 들면 네트워크(20)는 무선랜 네트워크, TCP/IP 네트워크, 블루투스 네트워크 등이 있다. 이하에서는 TCP/IP 네트워크를 기준으로 설명한다.

이하에서는 본 발명의 제1 실시예에 따른 네트워크 감시 장치(100)를 도 2 내지 도 4를 참고하여 설명한다.

도 2는 본 발명의 제1 실시예에 따른 네트워크 감시 장치(100)를 도시한 블록도이다.

본 발명의 제1 실시예에 따른 네트워크 감시 장치(100)는 제1 네트워크(30)를 감시하며, 네트워크 패킷 수집부(110), 공격 패킷 추출부(130), 시각화 정보 생성부(140), 시각화 정보 표시부(150), 경고 정보 생성부(160), 경고 정보 표시부(170), 네트워크 상태 정보 요청 수신부(180), 네트워크 상태 정보 송신부(190)를 포함한다.

네트워크 패킷 수집부(110)는 제1 네트워크(30) 상의 트래픽 패킷을 수집한다. 네트워크 패킷 수집부(110)는 제1 네트워크(30) 상의 플로우를 수집할 수도 있다. 플로우는 동일한 출발지 주소, 목적지 주소, 목적지 포트 값을 가지는 패킷의 집합이다. 일부 라우터는 플로우를 제공하기도 하므로, 네트워크 패킷 수집부(110)는 라우터로부터 플로우를 제공받을 수도 있다. 네트워크 감시 장치(100)가 플로우를 통한 네트워크 감시를 수행하면 처리 속도가 향상될 수 있으며 라우터 등의 기존 시스템과 연동되어 사용될 수도 있다. 따라서 본 명세서에서 패킷은 플로우를 포함하는 용어로 사용된다.

공격 패킷 추출부(130)는 네트워크 패킷 수집부(110)로부터의 트래픽 패킷 중에서 공격 패킷 또는 공격 패킷으로 의심되는 패킷을 추출한다. 공격 패킷 추출부(130)는 공격 패킷 또는 공격 패킷으로 의심되는 패킷을 종류별로 구분하여 저장하고 패킷의 수가 단위 시간 내에 일정량을 초과하였을 때 해당 종류의 패킷을 시각화 정보 생성부(140)에 제공할 수 있다. 여기서 단위시간이란 시각화 시스템 내에서 미리 정해 놓은 값이거나 네트워크 관리자가 임의로 정하는 값일 수 있다. 공격 패킷의 종류에는 웜 패킷, 호스트 스캔 공격 패킷, 포트 스캔 공격 패킷, 출발지 속임 도스 공격 패킷, 다중 포트 도스 공격 패킷, 백스캐터 패킷 등이 있다.

시각화 정보 생성부(140)는 공격 패킷 추출부(130)에서 추출된 공격 패킷으로 평행 좌표계를 사용하는 시각화 정보를 생성한다. 시각화 정보 생성부(140)는 공격 패킷 추출부(130)로부터 단일 종류의 공격 패킷을 제공받을 수도 있는데 이때 생성되는 시각화 정보는 공격 패킷의 유형에 따른 패턴이 나타나 있다. 한편 시각화 정보 생성부(140)는 네트워크 패킷 수집부(110)가 수집한 패킷을 제공받을 수도 있는데 이때 생성되는 시각화 정보는 수집 시간에의 네트워크 상태에 대한 정보

가 나타나 있다. 평행 좌표계의 축은 출발지 주소, 도착지 주소, 도착지 포트, 패킷 크기 등 공격 패킷에 포함되어 있는 파라메터이다. 본 발명의 실시예에서는 시각화 정보를 생성하기 위한 평행 좌표계의 평행축으로 출발지 주소 및 도착지 주소, 도착지 포트, 패킷 크기를 사용하지만, 일부 평행축을 제외할 수도 있고, 추가 파라메터로 평행축을 늘릴 수도 있다.

평행 좌표계는 2개 이상의 좌표축을 평면상에 평행하게 배치한 좌표계이다. 2차원 직교 좌표계 및 3차원 직교 좌표계에서 한 벡터는 점으로 나타나지만, 평행 좌표계에서 한 벡터는 굴곡선으로 나타난다. 직교 좌표계에서는 3차원 이상의 좌표축을 설정하기 어렵지만, 직교 좌표계에서는 평행축을 부가하는 방법으로 얼마든지 높은 차원의 좌표축을 설정할 수 있다. 평행 좌표계의 예를 도 3에 도시하였다.

도 3은 4차원 평행 좌표계의 한 예를 도시한 도면이다.

도 3에 도시된 평행 좌표계는 4개의 좌표축(X축, Y축, Z축, W축) 및 제1 벡터(5, 40, 35, 4), 제2 벡터(2, 60, 15, 16)을 포함한다. 도 3에 도시된 바와 같이 평행 좌표계에서 각 벡터는 각 좌표축상의 각 점을 연결한 굴곡선으로 나타난다. 또한 평행 좌표계에서는 도 3에 도시된 바와 같이 4차원 혹은 그 이상의 차원의 좌표계 또한 가능하다.

다시 도 2에 대한 설명을 계속한다.

시각화 정보 표시부(150)는 시각화 정보 생성부(140)에서 생성된 시각화 정보를 디스플레이 장치에 표시한다. 디스플레이 장치에는 음극선관(Cathode Ray Tube, CRT), 액정 표시 장치(Liquid Crystal Display, LCD), 플라즈마 표시 패널(Plasma Display Panel, PDP) 등이 있다.

공격 패킷 추출부(130)는 공격 패킷이 존재함을 판단하고 공격 패킷 존재 정보를 경고 정보 생성부(160)에 제공한다. 경고 정보 생성부(160)는 공격 패킷 존재 정보를 제공받아 경고 정보를 생성한다.

경고 정보 표시부(170)는 경고 정보 생성부(160)에서 생성된 경고 정보를 수신하고 이를 표시한다. 경고 정보 표시부(170)는 디스플레이 장치 또는 스피커 등을 통해 경고 정보를 표시한다. 경고 정보 표시부(170)는 네트워크 관리자에게 공격 패킷이 존재함을 즉각 알려 줌으로써 네트워크 관리자는 빠른 대처가 가능하다.

네트워크 상태 정보 요청 수신부(180)는 원격으로부터의 네트워크 상태 정보 요청 신호를 제1 네트워크(30)를 통해 수신한다.

네트워크 상태 정보 송신부(190)는 원격 장치로부터 네트워크 상태 정보 요청 신호가 있으면 경고 정보 생성부(160)로부터의 경고 정보 및/또는 시각화 정보 생성부(140)로부터의 시각화 정보를 제1 네트워크(30)를 통해 원격 장치에 송신한다. 이로써 관리자는 원격 네트워크의 상태를 파악할 수 있다.

또한 네트워크 상태 정보 송신부(190)는 공격 패킷이 존재할 때 네트워크 상태 정보 요청이 없어도 원격 장치에 경고 정보 및 또는 시각화 정보를 송신할 수 있다. 이로써 관리자는 원격 네트워크에 공격 패킷이 존재하는 지 여부를 빨리 파악하여 적절한 대처를 할 수 있다.

만약 네트워크 감시 장치(100)가 HTTP 서버 역할을 한다면, 관리자는 원격 장치에 설치된 인터넷 브라우저를 통해 원격의 네트워크 상태를 파악할 수도 있다.

이하에서는 공격 패킷 추출부(130)를 도 4를 참고하여 상세히 설명한다.

도 4는 본 발명의 실시예에 따른 공격 패킷 추출부(130)를 도시한 블록도이다.

도 4에 도시된 바와 같이 공격 패킷 추출부(130)는 공격 유형 식별자 생성부(131), 파라미터 저장부(132), 패킷 저장 제어부(133), 공격 패킷 저장부(134), 공격 패킷 제공부(135)를 포함한다.

공격 유형 식별자 생성부(131)는 네트워크 패킷을 입력받아 패킷에 포함되어 있는 파라미터의 값을 파라미터 저장부(132)에 저장한다.

파라미터 저장부(132)는 동일한 값은 1회만 저장 가능한 구조를 가진 저장부이다. 파라미터 저장부(132)의 구조는 링크 리스트(Linked List), 2진 검색 트리(Binary Search Tree), MULTOPS 트리, 해쉬 테이블(Hash Table) 등이 가능하다.

본 발명의 실시예에서 파라미터 저장부(132)는 출발지 저장부(132a), 목적지 저장부(132b), 목적지 포트 저장부(133c)를 포함한다. 출발지 저장부(132a)는 패킷의 출발지 주소가 저장되고, 목적지 저장부(132b)는 패킷의 목적지 주소가 저장된다. 그리고 목적지 포트 저장부(133c)는 패킷의 목적지 포트가 저장된다. 공격 유형 식별자 생성부(131)는 네트워크 패킷을 입력 받아 패킷의 출발지 주소, 목적지 주소 및 목적지 포트를 출발지 저장부(132a), 목적지 저장부(132b), 목적지 포트 저장부(133c)에 각각 저장한다. 이때 공격 유형 식별자 생성부(131)는 각 파라미터의 값이 파라미터 저장부(132)에 이미 존재하는 값인지 혹은 새로운 값인지의 여부로 공격 유형 식별자를 생성한다. 본 발명의 실시예에서는 공격 유형 식별자의 형태를 <s, d, p>로 둔다. 여기서 s, d, p는 각각 출발지 주소, 목적지 주소, 목적지 포트가 파라미터 저장부(132)에 이미 존재하는 값인지의 여부를 나타낸다. 그리고 본 발명의 실시예에서는 저장하는 값이 파라미터 저장부(132)에 이미 존재하는 값이면 1로 두고, 새로운 값이면 0으로 둔다. 만약 공격 유형 식별자 생성부(131)가 패킷의 출발지 주소, 목적지 주소 및 목적지 포트를 파라미터 저장부(132)에 저장하는데 이 패킷의 출발지 주소 및 목적지 주소가 출발지 저장부(132a) 및 목적지 저장부(132b)에 이미 존재하고 있으면, 공격 유형 식별자 생성부(131)는 <1, 1, 0>인 공격 유형 식별자를 생성한다.

한편 공격 유형 식별자 생성부(131)는 파라미터 값 유지 주기를 가지고 있어서 이 주기에 도달할 경우 파라미터 저장부(132)에 저장된 파라미터 값을 삭제할 수도 있다. 이로써 파라미터 저장부(132)가 장기간에 걸친 파라미터 값을 가지고 있어 공격 유형 식별자 생성부(131)는 네트워크 패킷의 공격 유형을 잘못 판단할 수 있는 가능성을 줄일 수 있다.

공격 패킷 저장부(134)는 네트워크 패킷을 공격 유형 별로 저장한다. 본 발명의 실시예에서 공격 패킷 저장부(134)는 웜 패킷 저장부(134a), 호스트 스캔 공격 패킷 저장부(134b), 포트 스캔 공격 저장부(134c), 출발지 속임 도스 공격 패킷 저장부(134d), 다중 포트 도스 공격 패킷 저장부(134e), 백스캐터 패킷 저장부(134f), 분산 호스트 스캔 공격 패킷 저장부(134g)를 포함한다. 웜 패킷 저장부(134a)에는 웜으로 판단(또는 의심)되는 패킷이 저장되고, 호스트 스캔 공격 패킷 저장부(134b)에는 호스트 스캔 공격으로 판단되는 패킷이 저장된다. 그리고 포트 스캔 공격 저장부(134c)에는 포트 스캔 공격으로 판단되는 패킷이 저장되는 저장 장소이며, 출발지 속임 도스 공격 패킷 저장부(134d)에는 출발지 속임 도스 공격으포 판단되는 패킷이 저장된다. 다중 포트 도스 공격 패킷 저장부(134e)에는 다중 포트 도스 공격으로 판단되는 패킷이 저장되고, 백스캐터 패킷 저장부(134f)에는 백스캐터 패킷 저장부로 판단되는 패킷이 저장되며, 분산 호스트 스캔 공격 패킷 저장부(134g)에는 분산 호스트 스캔 공격 패킷으로 판단되는 패킷이 저장된다.

패킷 저장 제어부(133)는 공격 유형 식별자를 바탕으로 네트워크 패킷의 공격 유형을 판단하여 공격 유형 별로 네트워크 패킷을 공격 패킷 저장부(134)에 저장한다. 예를 들어 패킷 저장 제어부(133)는 네트워크 패킷의 공격 유형 식별자가 <1,1,0>이면 이 패킷의 공격 유형을 포트 스캔 공격으로 판단하여 이 패킷을 포트 스캔 공격 패킷 저장부(134c)에 저장한다. 또, 패킷 저장 제어부(133)는 네트워크 패킷의 공격 유형 식별자가 <1,0,1>이고 이 패킷의 크기가 48Byte 보다 크면, 패킷의 공격 유형을 웜으로 판단하여 이 패킷을 웜 스캔 공격 패킷 저장부(134c)에 저장한다.

한편, 패킷 저장 제어부(133)는 공격 패킷 추출 주기를 가지고 있어서 이 주기에 도달하면 공격 패킷 저장부(134)에 저장된 패킷을 모두 삭제할 수도 있다. 이로써 공격 패킷 저장부(134)는 공격 패킷을 일정 시간 동안에만 유지하게 되므로 공격 패킷 추출부(130)는 더욱 효과적으로 공격 패킷을 추출할 수 있다. 이는 공격 패킷 저장부(134)가 장기간 공격 패킷을 저장하는 경우 여러 공격 패킷이 혼합되어 공격의 유형이 잘못 판단될 수도 있기 때문이다.

공격 패킷 제공부(135)는 공격 패킷 저장부(134)에 소정의 개수 이상의 패킷이 저장되는 경우 공격 패킷이 존재한다고 판단하고 이 패킷에 대한 정보를 시각화 정보 생성부(140)에 제공한다. 예를 들어 다중 포트 도스 공격 패킷 저장부(134e)에 저장되어 있는 패킷이 50개(임의의 개수임) 이상인 경우, 공격 패킷 제공부(135)는 다중 포트 도스 공격이 있다고 판단하고, 이 패킷에 대한 정보를 시각화 정보 생성부(140)에 제공한다. 이때 시각화 정보 생성부(140)는 제공받은 정보를 바탕으로 평행 좌표계에 표시함으로써 시각화 정보를 생성한다.

한편, 공격 패킷 제공부(135)는 공격 패킷이 존재함을 경고 정보 생성부(160)에 알릴 수도 있다. 앞서 설명한 바와 같이, 다중 포트 도스 공격 패킷 저장부(134e)에 저장되어 있는 패킷이 50개(임의의 개수임) 이상인 경우, 공격 패킷 제공부(135)는 다중 포트 도스 공격이 있다고 판단하고, 이 정보를 경고 정보 생성부(160)에 제공한다. 이때 경고 정보 생성부(160)는 다중 포트 도스 공격이 있다는 경고 정보를 생성하여 이 경고 정보를 경고 정보 표시부(170) 또는 네트워크 상태 정보 송신부(190)에 전달한다. 경고 정보를 수신한 경고 정보 표시부(170)는 디스플레이 장치 또는 스피커를 통해 네트워크 감시 장치(100) 부근의 네트워크 관리자에게 네트워크 공격이 있음을 알릴 수 있다. 또 경고 정보를 수신한 네트워크 상태 정보 송신부(190)는 이 경고 정보를 제1 네트워크(30)를 통해 원격의 네트워크 관리자에게 네트워크 공격이 있음을 알릴 수 있다.

이하에서는 본 발명의 제2 실시예에 따른 네트워크 감시 장치(200)를 도 5를 참고하여 설명한다.

도 5는 본 발명의 제2 실시예에 따른 네트워크 감시 장치(200)를 도시한 블록도이다.

본 발명의 제2 실시예에 따른 네트워크 감시 장치(200)는 제1 네트워크(30)를 감시하며, 네트워크 패킷 수집부(210), 공격 패킷 추출부(230), 시각화 정보 생성부(240), 시각화 정보 표시부(250), 경고 정보 생성부(260), 경고 정보 표시부(270), 네트워크 상태 정보 요청 수신부(280), 네트워크 상태 정보 송신부(290)를 포함한다.

본 발명의 제2 실시예에 따른 네트워크 감시 장치(200)가 포함하는 구성 요소(210 내지 270)는 도 2에 도시된 제1 실시예에 따른 네트워크 감시 장치(100)의 구성 요소(110 내지 170)의 역할과 동일하므로 설명을 생략한다.

네트워크 상태 정보 요청 수신부(280)는 원격으로부터의 네트워크 상태 정보 요청 신호를 제2 네트워크(40)를 통해 수신한다.

네트워크 상태 정보 송신부(290)는 원격 장치로부터 네트워크 상태 정보 요청 신호가 있으면 경고 정보 생성부(260)로부터의 경고 정보 및/또는 시각화 정보 생성부(240)로부터의 시각화 정보를 제2 네트워크(40)를 통해 원격 장치에 송신한다. 이로써 관리자는 원격 네트워크의 상태를 파악할 수 있으며 특히 제1 네트워크가 공격 패킷으로 인해 이용 불가한 상태이더라도 제1 네트워크와는 다른 제2 네트워크를 통해 제1 네트워크의 상태를 파악할 수 있다. 제2 네트워크는 제1 네트워크와 마찬가지로 유선 또는 무선으로 구성 가능하며, 제1 네트워크보다는 안정적인 네트워크라면 더욱 효과적일 수 있다.

또한 네트워크 상태 정보 송신부(290)는 공격 패킷이 존재할 때 네트워크 상태 정보 요청이 없어도 원격 장치에 경고 정보 및 또는 시각화 정보를 제2 네트워크를 통해 송신할 수 있다. 이로써 관리자는 원격 네트워크에 공격 패킷이 존재하는 지 여부를 빨리 파악하여 적절한 대처를 할 수 있다.

이하에서는 공격 패킷의 유형에 따른 시각화 정보의 예를 도 6 내지 도 10을 참고하여 설명한다. 앞서 설명한 바와 같이 본 발명의 실시예에 따른 시각화 정보는 평행 좌표계를 사용하고 평행 좌표축이 나타내는 파라미터로 출발지 주소 및 도착지 주소, 도착지 포트, 패킷 크기를 사용한다.

도 6은 본 발명의 실시예에 따른 출발지 속임 도스 공격이 반영된 시각화 정보를 도시한 도면이다. 도 6에는 출발지 주소가 111.11.8.50에서 111.11.248.207에 걸쳐 있고 목적지 주소가 192.168.50.30이며, 대상 포트는 80이고 평균 패킷 크기는 40 Byte인 출발지 속임 도스 공격의 시각화 정보가 도시되어 있다.

도 7은 본 발명의 실시예에 따른 포트 스캔 공격이 반영된 시각화 정보를 도시한 도면이며, 도 8은 본 발명의 실시예에 따른 호스트 스캔 공격이 반영된 시각화 정보를 도시한 도면이고, 도 9는 본 발명의 실시예에 따른 웜이 반영된 시각화 정보를 도시한 도면이다.

도 6 내지 도 9에 도시된 시각화 정보는 공격 유형에 따라 그 형상이 서로 매우 상이하여, 네트워크 관리자는 시각화 정보를 통해 네트워크 상에 존재하는 공격 유형을 용이하게 파악할 수 있다.

도 10은 다양한 공격 유형에 따른 시각화 정보의 패턴 및 분산을 도시한 도면이다.

도 10에서 알 수 있는 바와 같이 분산 형태에 따라 분류되는 여러 네트워크 공격은 그 패턴(시각화 정보의 패턴)이 서로 상이하여 네트워크 관리자는 시각화 정보를 통해 네트워크 상에 존재하는 공격 유형을 용이하게 파악할 수 있다.

이하에서는 도 11을 참고하여 네트워크 분석 장치(300)를 상세히 설명한다.

도 11은 본 발명의 실시예에 따른 네트워크 분석 장치(300)를 도시한 블록도이다.

도 11에 도시된 바와 같이 네트워크 분석 장치(300)는 제1 네트워크(30) 상의 네트워크 패킷을 분석하며, 네트워크 패킷 수집부(310), 공격 유형 식별자 생성부(320), 파라미터 저장부(330), 패킷 저장 제어부(340), 공격 패킷 저장부(350)을 포함한다.

네트워크 패킷 수집부(310)는 제1 네트워크(30) 상의 네트워크 패킷을 수집한다.

공격 유형 식별자 생성부(320)는 네트워크 패킷 수집부(310)에서 수집된 패킷으로부터 공격 유형 식별자를 생성하고, 도 4의 공격 유형 식별자 생성부(도 4의131)에 대응되므로 설명을 생략한다.

네트워크 분석 장치(300)의 구성 요소(330 내지 350)은 도 4의 구성 요소(132 내지 134)에 대응되므로 설명을 생략한다.

본 발명의 실시예에 따른 네트워크 분석 장치(300)를 통해 공격 패킷으로 의심되는 패킷을 용이하게 패킷 별로 구분하여 취합할 수 있다. 이렇게 취합된 패킷을 이용하여 다양한 네트워크 분석이 가능하다.

이하에서는 본 발명의 실시예에 따른 네트워크 감시 방법을 도 12 및 도 13을 참고하여 상세히 설명한다.

도 12는 본 발명의 실시예에 따른 네트워크 감시 방법을 도시한 흐름도이고, 도 13은 본 발명의 실시예에 따른 네트워크 감시 방법에서 공격 패킷 추출 단계를 도시한 흐름도이다.

제1 네트워크를 감시하기 위해서 우선 네트워크 패킷 수집부(110)는 제1 네트워크 상의 패킷을 수집한다(S100).

다음, 공격 패킷 추출부(130)는 수집한 패킷으로부터 공격 패킷으로 판단(혹은 의심)되는 패킷을 추출한다(S200). 더 구체적으로 공격 유형 식별자 생성부(131)는 파라미터 저장부(132)에 패킷의 파라미터 값을 저장할 수 있는 지 여부로 공격 유형 식별자를 생성한다(S210). 그 후, 패킷 저장 제어부(133)는 공격 유형 식별자를 바탕으로 수집한 패킷을 공격 유형 별로 공격 패킷 저장부(134)에 저장한다(S220). 공격 패킷 제공부(135)는 공격 패킷이 존재 여부를 공격 패킷 저장부(134)에 저장되어 있는 패킷의 수로 판단할 수도 있다.

만약 공격 패킷이 존재하면(S300), 시각화 정보 생성부(S140)는 패킷에 포함되어 있는 파라미터를 평행축으로 하는 평행 좌표계에 공격 패킷을 나타낸 시각화 정보를 생성한다(S400).

그리고, 시각화 정보 표시부(150)는 생성된 시각화 정보를 디스플레이 장치 등에 표시한다. 이로써 네트워크 감시 장치(100)를 사용하는 네트워크 관리자는 제1 네트워크의 상태를 시각적으로 인식할 수 있다. 또한 네트워크 관리자는 제1 네트워크 상에 존재하는 공격 패킷을 용이하게 인식할 수 있고, 새로운 유형의 공격 패킷이 나타나더라도 이 새로운 유형의 공격 패킷의 존재를 용이하게 인식할 수 있다.

그리고, 경고 정보 생성부(160)는 공격 패킷 추출부(130)로부터 공격 패킷이 존재함을 통보받아 경고 정보를 생성한다(S600).

경고 정보 표시부(170)는 경고 정보를 디스플레이 장치 또는 스피커를 통해 경고 정보를 표시한다(S700). 이로써 네트워크 관리자는 시각화 정보를 분석하기 전에도 경고 메시지를 통해 공격 패킷이 있음을 빨리 인지할 수 있다.

그리고 네트워크 상태 정보 요청 수신부(180)가 원격의 서버으로부터 네트워크 상태 정보 요청을 수신하면(S800), 네트워크 상태 정보 송신부(190)는 경고 정보와 시각화 정보 중 적어도 하나를 원격의 서버로 송신한다(S900). 이로써 네트워크 관리자는 원격에서 제1 네트워크의 상태를 파악할 수 있다.

한편, 그리고 네트워크 상태 정보 요청 수신부(180)가 원격의 서버으로부터 네트워크 상태 정보 요청을 수신하지 않더라도, 네트워크 상태 정보 송신부(190)는 경고 정보와 시각화 정보 중 적어도 하나를 원격의 서버로 송신할 수도 있다(S900). 이때 네트워크 상태 정보 송신부(190)는 공격 패킷이 존재하는 경우 경고 정보와 시각화 정보 중 적어도 하나를 원격의 서버로 송신할 수도 있다. 이로써 네트워크 관리자는 네트워크 감시 장치(100)에 상태 정보를 요청하지 않더라도 제1 네트워크의 상태를 파악할 수 있다.

이하에서는 본 발명의 실시예에 따른 네트워크 패킷의 공격 유형 식별 방법에 대하여 도 14을 참고하여 상세히 설명한다.

도 14는 본 발명의 실시예에 따른 네트워크 패킷의 공격 유형 식별 방법을 도시한 흐름도이다.

제1 네트워크 상의 패킷의 공격 유형을 식별하기 위하여, 네트워크 패킷 수집부(310)는 제1 네트워크로부터 패킷을 수집한다(S1100).

다음 공격 유형 식별자 생성부(320)는 수집한 패킷에 포함되어 있는 하나 이상의 파라미터 값을 동일값에 대해서는 1회만 저장되는 파라미터 저장부(330)에 저장을 시도한다(S1200).

그 후, 공격 유형 식별자 생성부(320)는 파라미터 값이 파라미터 저장부(330)에 저장 가능한 지 여부를 통해 공격 유형 식별자를 생성한다(S1300).

본 발명의 실시예에 따른 네트워크 패킷의 공격 유형 식별 방법을 사용하면 패킷을 공격 유형 별로 저장할 수도 있고, 공격 유형 별로 분류하여 다양한 포맷의 시각화 정보를 생성할 수도 있다.

이하에서는 본 발명의 실시예에 따른 네트워크 패킷 분류 방법에 대하여 도 15를 참고하여 상세히 설명한다.

도 15는 본 발명의 실시예에 따른 네트워크 패킷 분류 방법을 도시한 흐름도이다.

제1 네트워크 상의 패킷을 공격 유형별로 분류하기 위하여, 네트워크 패킷 수집부(310)는 제1 네트워크로부터 패킷을 수집한다(S2100).

다음 공격 유형 식별자 생성부(320)는 수집한 패킷에 포함되어 있는 하나 이상의 파라미터 값을 동일값에 대해서는 1회만 저장되는 파라미터 저장부(330)에 저장을 시도한다(S2200).

그 후, 공격 유형 식별자 생성부(320)는 파라미터 값이 파라미터 저장부(330)에 저장 가능한 지 여부를 통해 공격 유형 식별자를 생성한다(S2300).

그리고, 패킷 저장 제어부(340)는 생성된 공격 유형 식별자를 바탕으로 수집한 패킷을 공격 유형별로 저장한다(S2400).

본 발명의 실시예에 따른 네트워크 패킷 분류 방법을 사용하면 네트워크 상의 무수히 많은 패킷을 공격 유형 별로 분류하여 저장할 수 있고, 네트워크 관리자는 분류된 공격 패킷을 자세하게 검토할 수도 있다. 또한 본 발명의 실시예에 따른 네트워크 패킷 분류 방법을 사용하면 네트워크 상의 많은 패킷을 공격 유형 별로 분류하여 공격 유형에 따른 시각화 정보를 생성할 수도 있다.

이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

발명의 효과

본 발명에 따르면 네트워크 상의 패킷을 평행 좌표계 상에 나타내어 시각적으로 용이하게 공격을 파악할 수 있는 효과가 있다.

또한 본 발명에 따르면 평행 좌표계의 좌표축을 1개 더 늘리는 방법으로 분석용 파라미터의 추가가 용이하다.

본 발명에 따르면 네트워크 상의 패킷을 시각적으로 나타내므로 새로운 네트워크 공격이 발생하는 경우라도 해당 공격을 쉽게 파악할 수 있는 효과가 있다.

또한 본 발명에 따르면 네트워크 패킷의 파라미터 값을 동일한 값은 1회만 저장되는 파라미터 저장 수단에 저장 가능한 지 여부에 따라 생성되는 공격 유형 식별자를 사용하여 네트워크 패킷을 공격 유형 별로 용이하게 추출, 분석, 저장할 수 있다.

도면의 간단한 설명

도 1은 본 발명의 실시예에 따른 네트워크 감시 장치가 설치된 네트워크 환경을 도시한 도면이다.

도 2는 본 발명의 제1 실시예에 따른 네트워크 감시 장치를 도시한 블록도이다.

도 3은 4차원 평행 좌표계의 한 예를 도시한 도면이다.

도 4는 본 발명의 실시예에 따른 공격 패킷 추출부를 도시한 블록도이다.

도 5는 본 발명의 제2 실시예에 따른 네트워크 감시 장치를 도시한 블록도이다.

도 6은 본 발명의 실시예에 따른 출발지 속임 도스 공격이 반영된 시각화 정보를 도시한 도면이다.

도 7은 본 발명의 실시예에 따른 포트 스캔 공격이 반영된 시각화 정보를 도시한 도면이다.

도 8은 본 발명의 실시예에 따른 호스트 스캔 공격이 반영된 시각화 정보를 도시한 도면이다.

도 9는 본 발명의 실시예에 따른 웜이 반영된 시각화 정보를 도시한 도면이다.

도 10은 다양한 공격 유형에 따른 시각화 정보의 패턴 및 분산을 도시한 도면이다.

도 11은 본 발명의 실시예에 따른 네트워크 분석 장치를 도시한 블록도이다.

도 12는 본 발명의 실시예에 따른 네트워크 감시 방법을 도시한 흐름도이다.

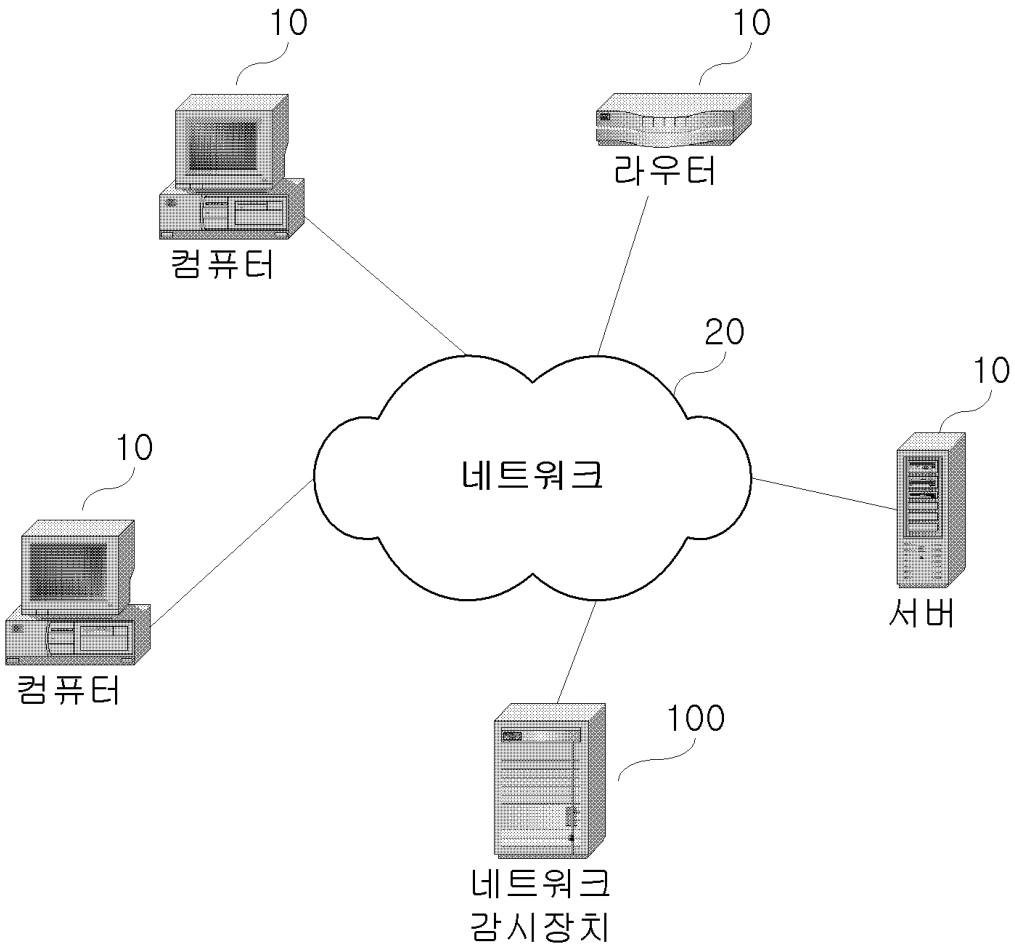
도 13은 본 발명의 실시예에 따른 네트워크 감시 방법에서 공격 패킷 추출 단계를 도시한 흐름도이다.

도 14는 본 발명의 실시예에 따른 네트워크 패킷의 공격 유형 식별 방법을 도시한 흐름도이다.

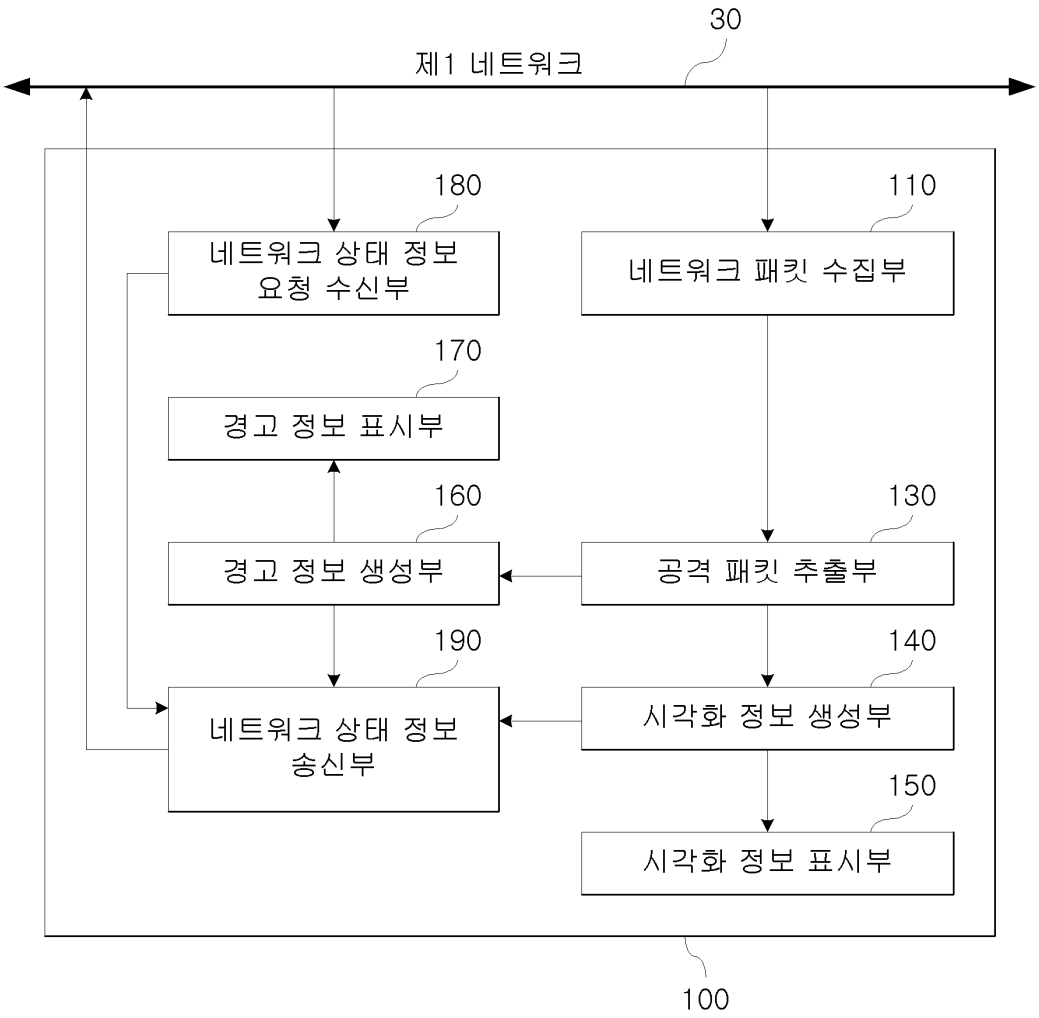
도 15는 본 발명의 실시예에 따른 네트워크 패킷 분류 방법을 도시한 흐름도이다.

도면

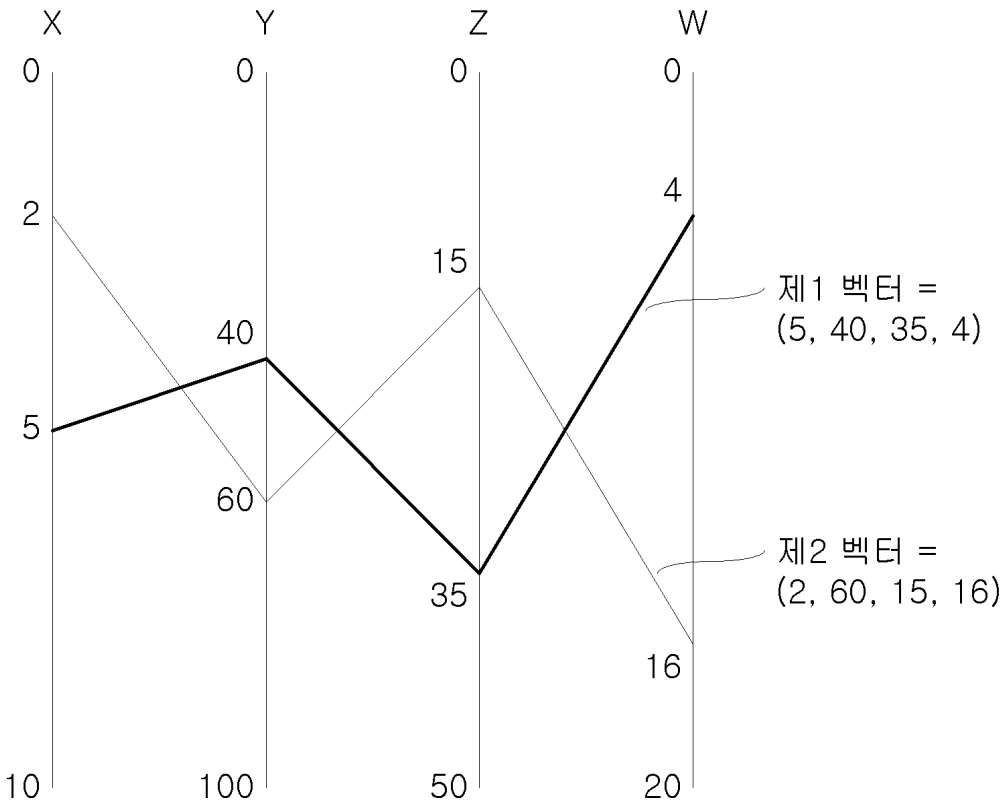
도면1



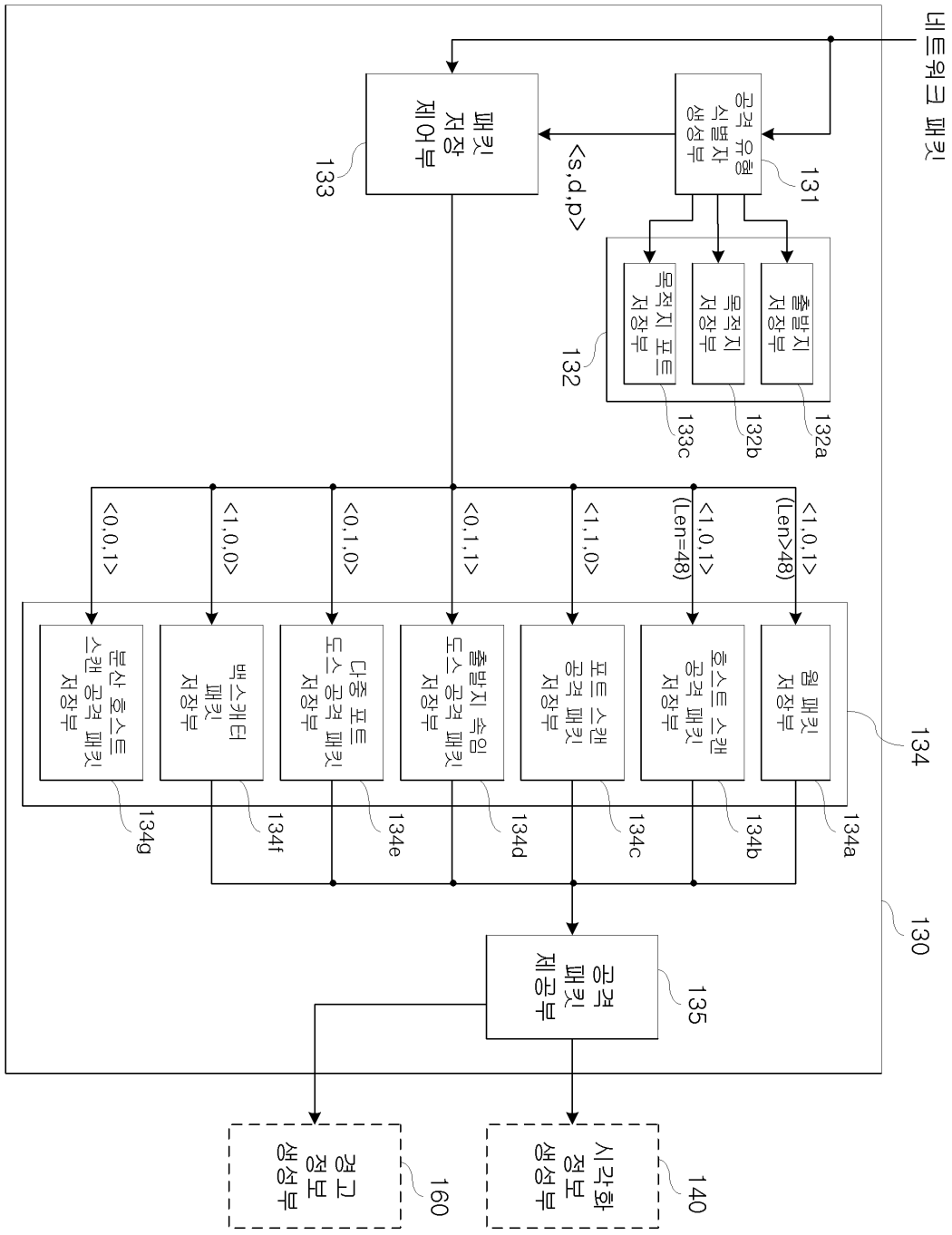
도면2


30
제1 네트워크
180
네트워크 상태 정보 요청 수신부
110
네트워크 패킷 수집부
170
경고 정보 표시부
160
경고 정보 생성부
130
공격 패킷 추출부
190
네트워크 상태 정보 송신부
140
시각화 정보 생성부
150
시각화 정보 표시부
100

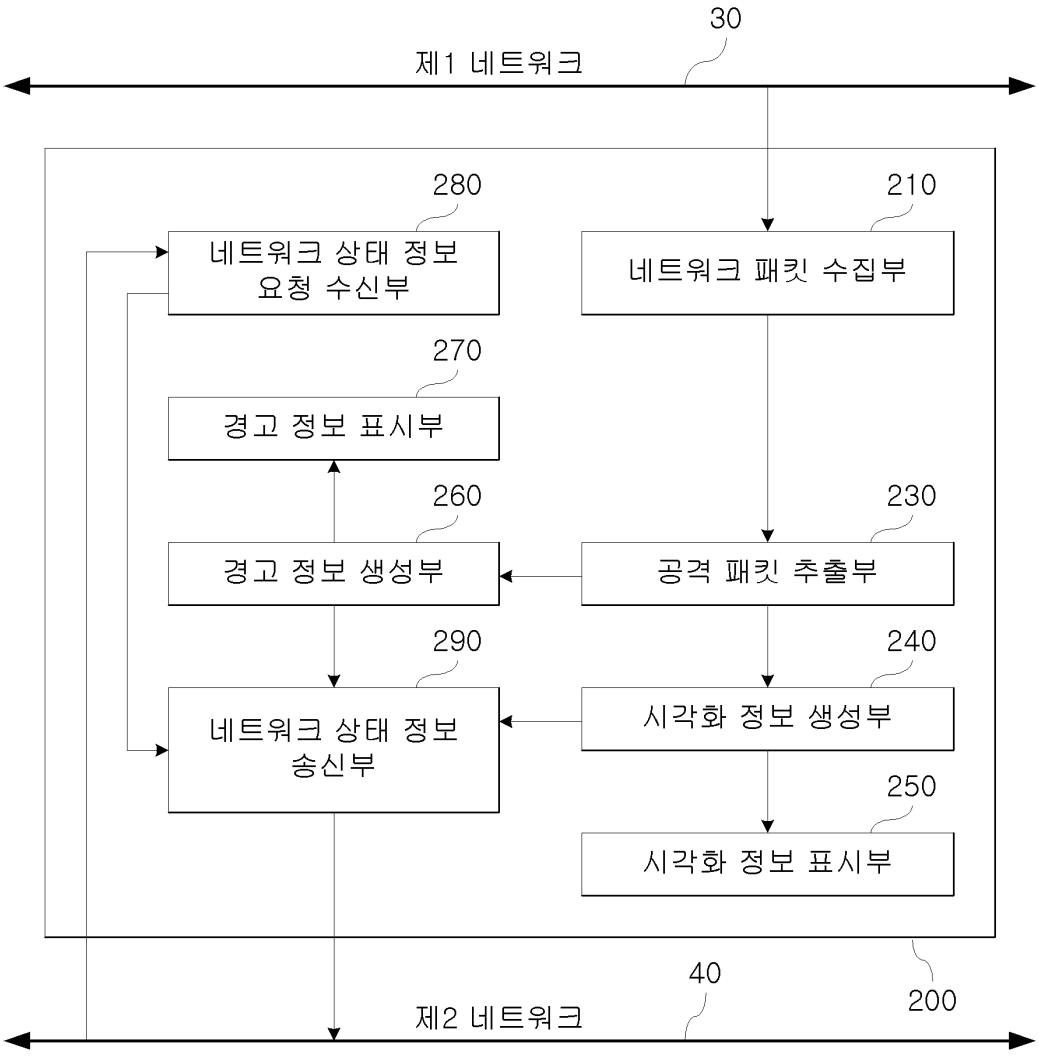
도면3


X
Y
Z
W
0
0
0
0
2
4
15
40
5
60
35
16
10
100
50
20
제1 벡터 =
(5, 40, 35, 4)
제2 벡터 =
(2, 60, 15, 16)

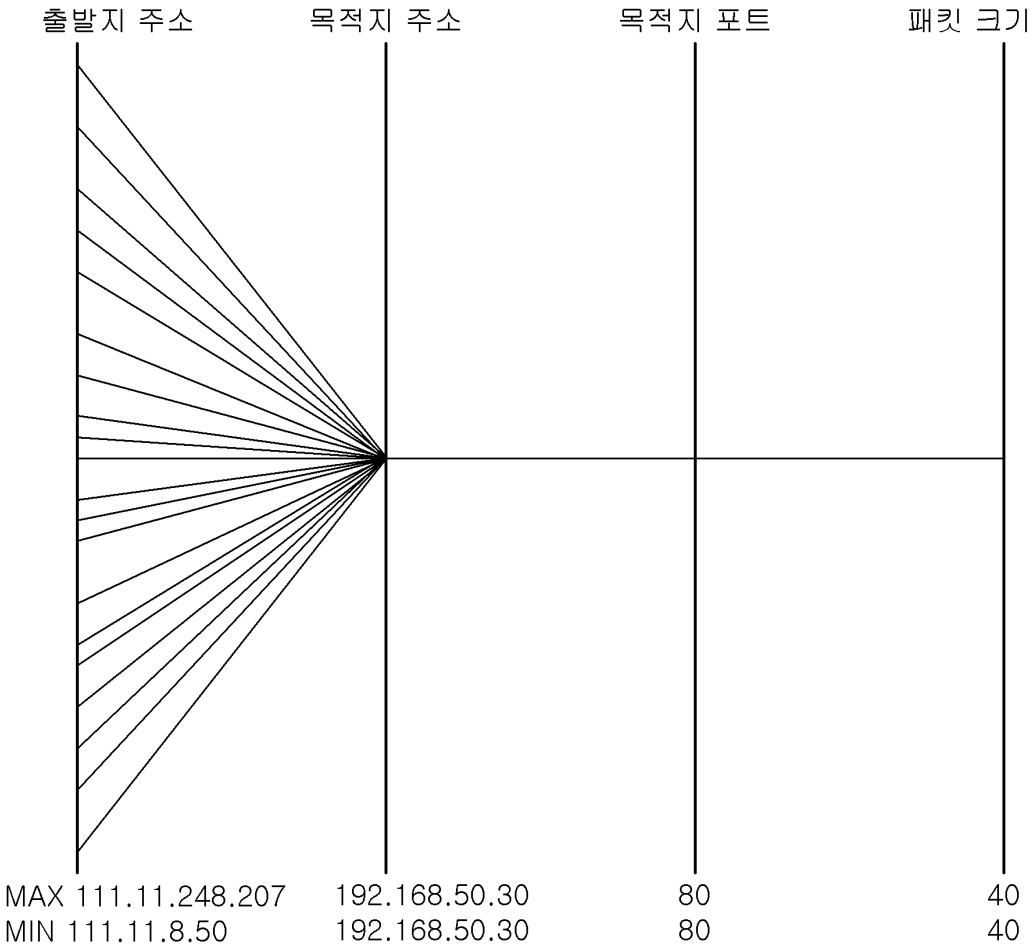
도면4


네트워크 패킷
130
공격 유형 식별자 생성부
131
<s,d,p>
패킷 저장 제어부
133
출발지 저장부
132a
목적지 저장부
132b
목적지 포트 저장부
133c
132
웜 패킷 저장부
134a
호스트 스캔 공격 패킷 저장부
134b
포트 스캔 공격 패킷 저장부
134c
출발지 속임 도스 공격 패킷 저장부
134d
다중 포트 도스 공격 패킷 저장부
134e
백스캐터 패킷 저장부
134f
분산 호스트 스캔 공격 패킷 저장부
134g
134
<1,0,1> (Len>48)
<1,0,1> (Len=48)
<1,1,0>
<0,1,1>
<0,1,0>
<1,0,0>
<0,0,1>
공격 패킷 제공부
135
시각화 정보 생성부
140
경고 정보 생성부
160

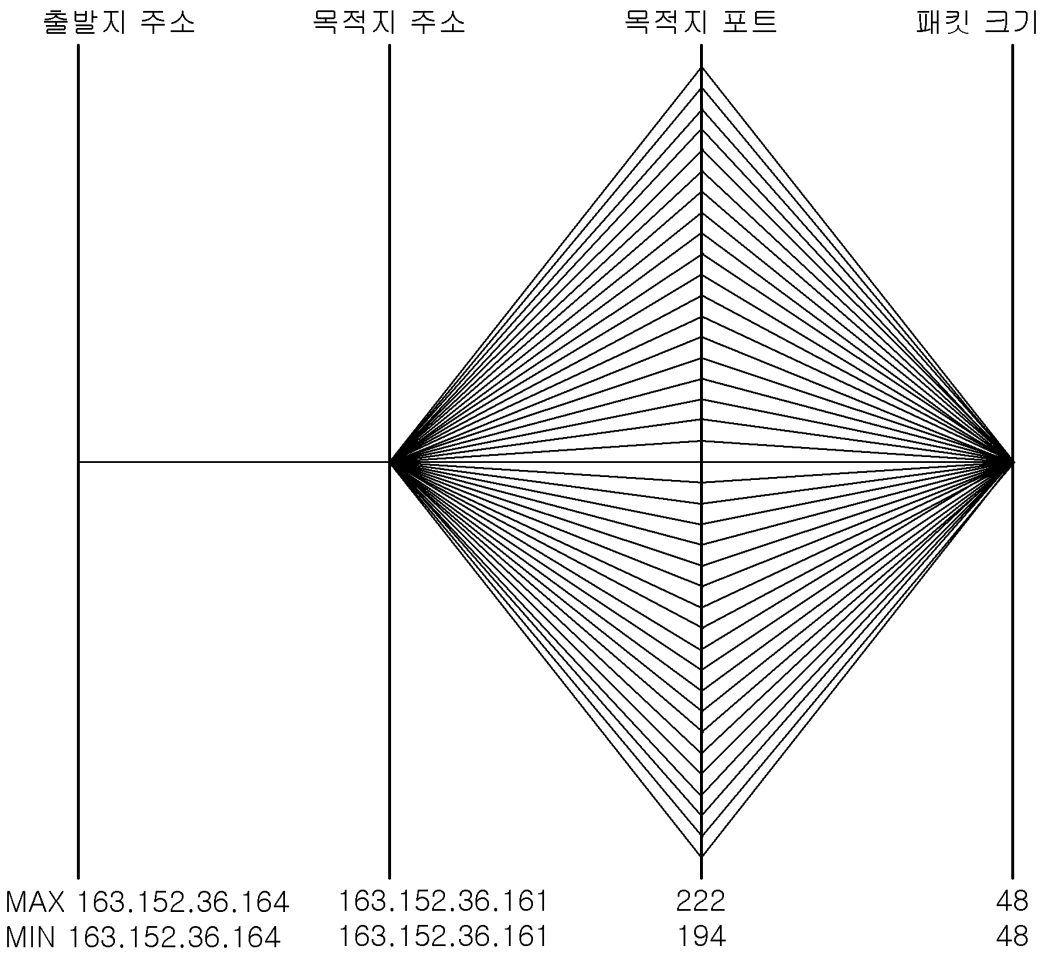
도면5


30
제1 네트워크
280
네트워크 상태 정보 요청 수신부
210
네트워크 패킷 수집부
270
경고 정보 표시부
260
경고 정보 생성부
230
공격 패킷 추출부
290
네트워크 상태 정보 송신부
240
시각화 정보 생성부
250
시각화 정보 표시부
200
40
제2 네트워크

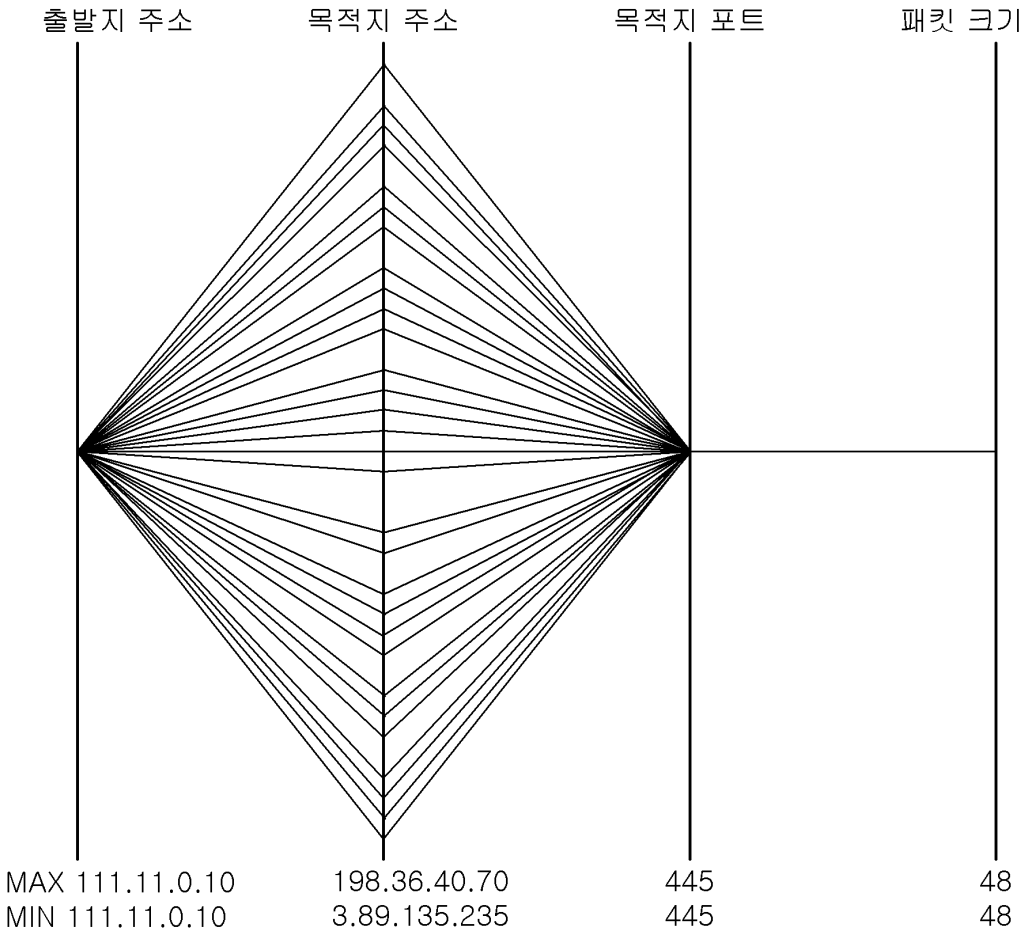
도면6


출발지 주소
목적지 주소
목적지 포트
패킷 크기
MAX 111.11.248.207
MIN 111.11.8.50
192.168.50.30
192.168.50.30
80
80
40
40

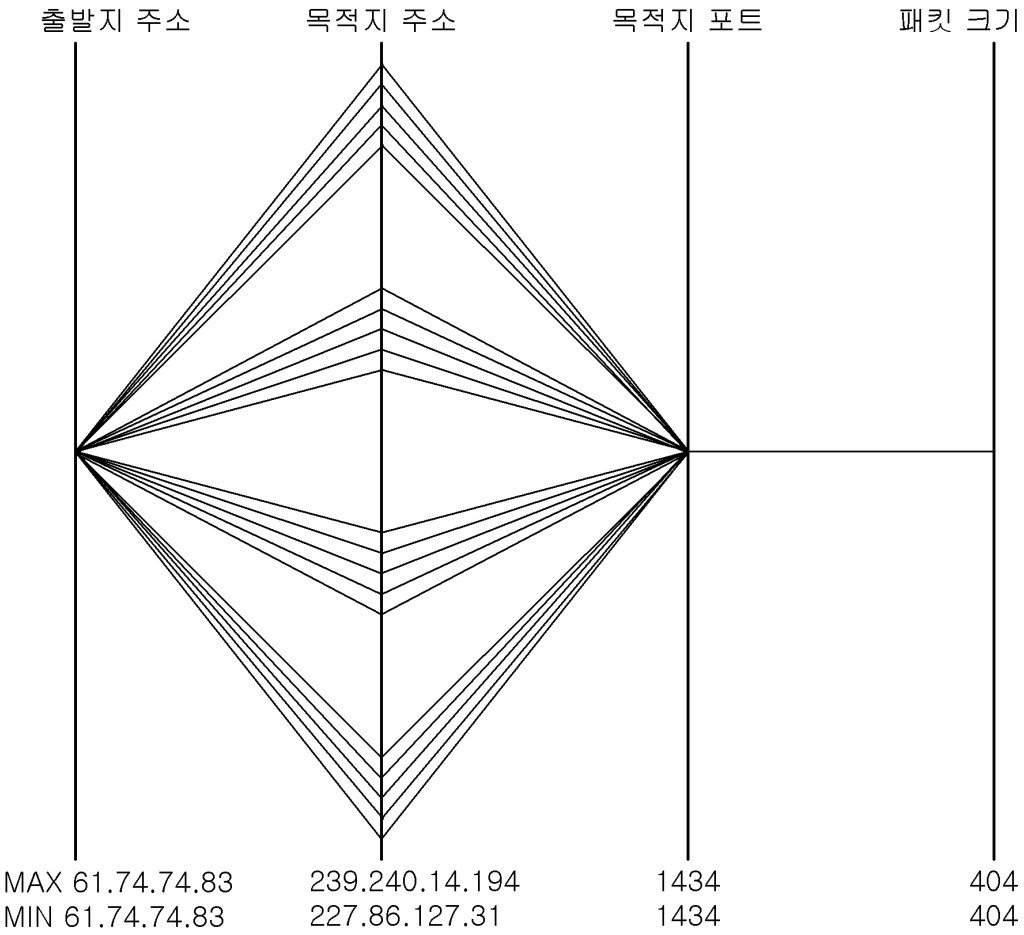
도면7


출발지 주소
목적지 주소
목적지 포트
패킷 크기
MAX 163.152.36.164
MIN 163.152.36.164
163.152.36.161
163.152.36.161
222
194
48
48

도면8


출발지 주소
목적지 주소
목적지 포트
패킷 크기
MAX 111.11.0.10
MIN 111.11.0.10
198.36.40.70
3.89.135.235
445
445
48
48

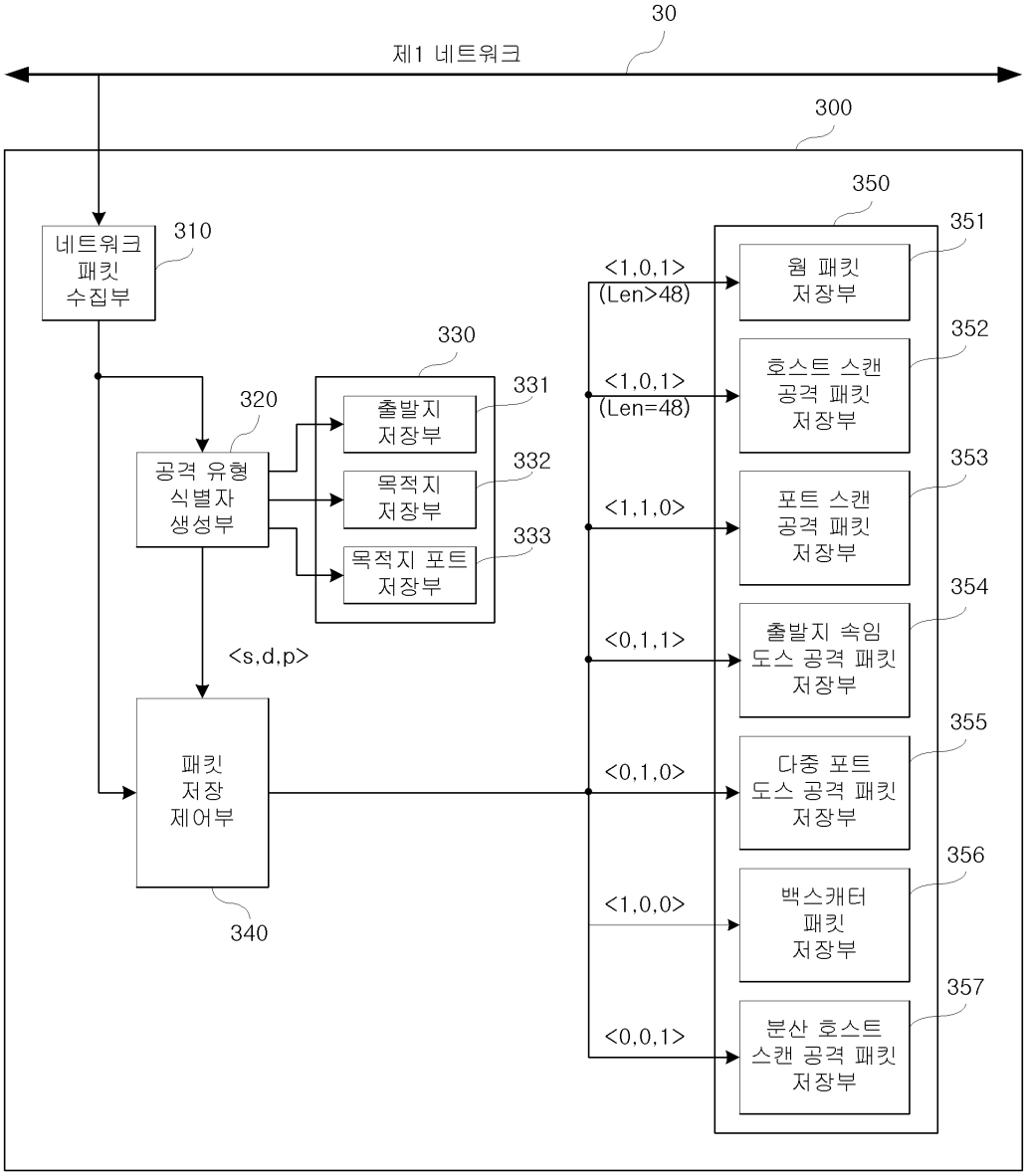
도면9



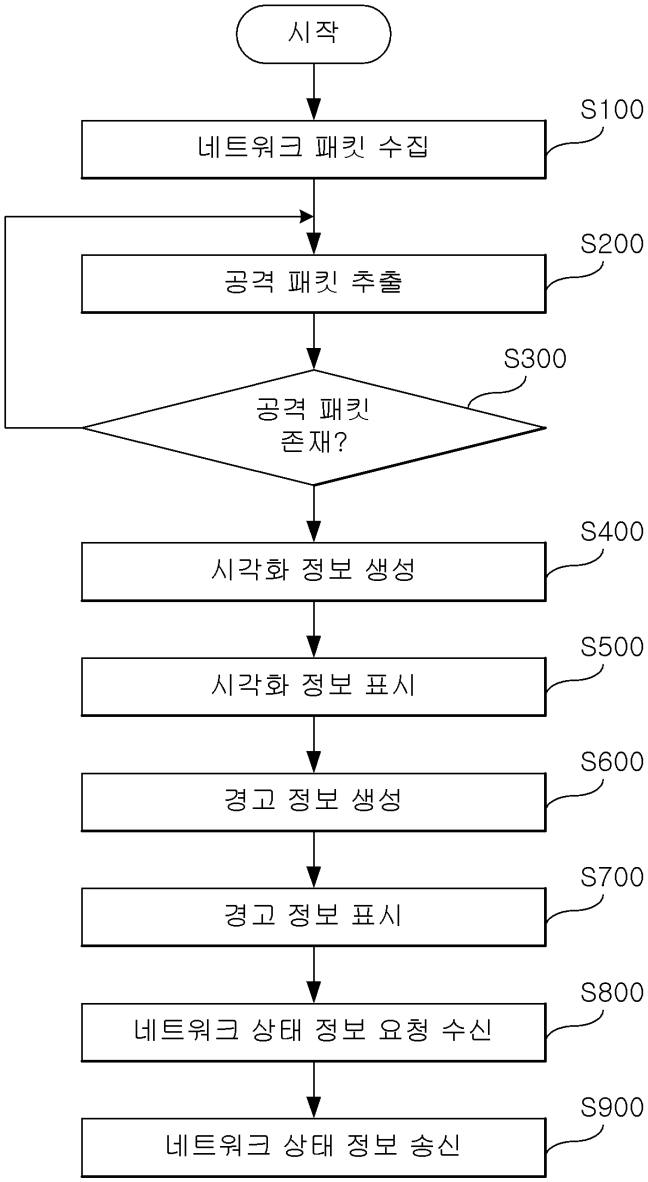
도면10

네트워크 공격	패턴	분산
포트 스캔 공격		1:1:m:1
호스트 스캔 공격		1:m:1:1
웜		1:m:1:1
출발지 속임 도스 공격		m:1:1:1
백캐스터		1:m:m:1
다중 포트 도스 공격		m:1:m:1
분산 호스트 스캔 공격		m:m:1:1
네트워크-대향 도스 공격		m:m:m:1
단일 출발지 도스 공격		1:1:1:1

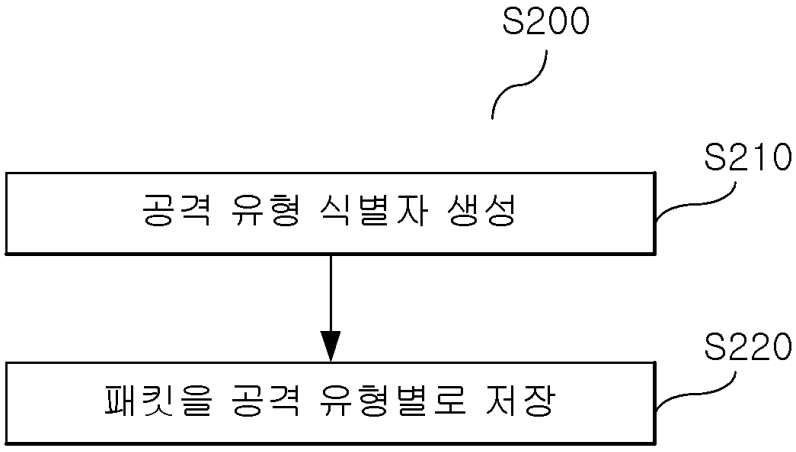
도면11


30
제1 네트워크
300
네트워크 패킷 수집부
310
320
공격 유형 식별자 생성부
330
출발지 저장부
331
목적지 저장부
332
목적지 포트 저장부
333
<s,d,p>
패킷 저장 제어부
340
350
<1,0,1> (Len>48)
웜 패킷 저장부
351
<1,0,1> (Len=48)
호스트 스캔 공격 패킷 저장부
352
<1,1,0>
포트 스캔 공격 패킷 저장부
353
<0,1,1>
출발지 속임 도스 공격 패킷 저장부
354
<0,1,0>
다중 포트 도스 공격 패킷 저장부
355
<1,0,0>
백스캐터 패킷 저장부
356
<0,0,1>
분산 호스트 스캔 공격 패킷 저장부
357

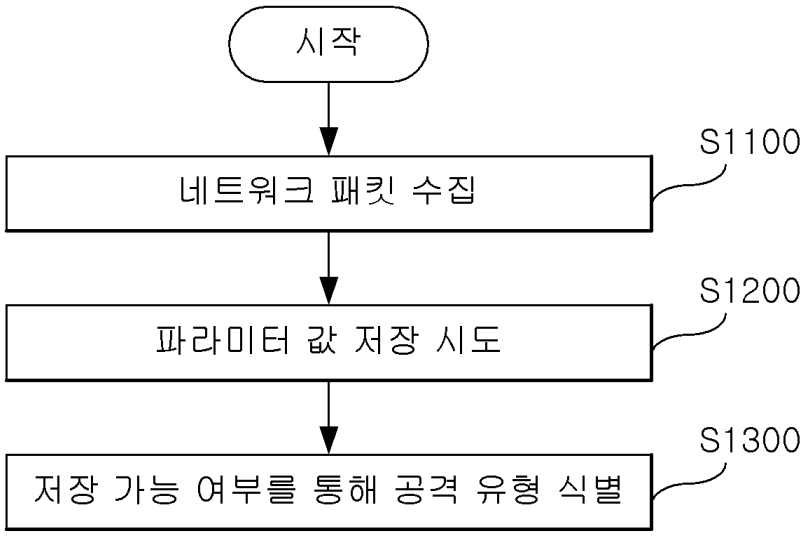
도면12


시작
S100
네트워크 패킷 수집
S200
공격 패킷 추출
S300
공격 패킷
존재?
S400
시각화 정보 생성
S500
시각화 정보 표시
S600
경고 정보 생성
S700
경고 정보 표시
S800
네트워크 상태 정보 요청 수신
S900
네트워크 상태 정보 송신

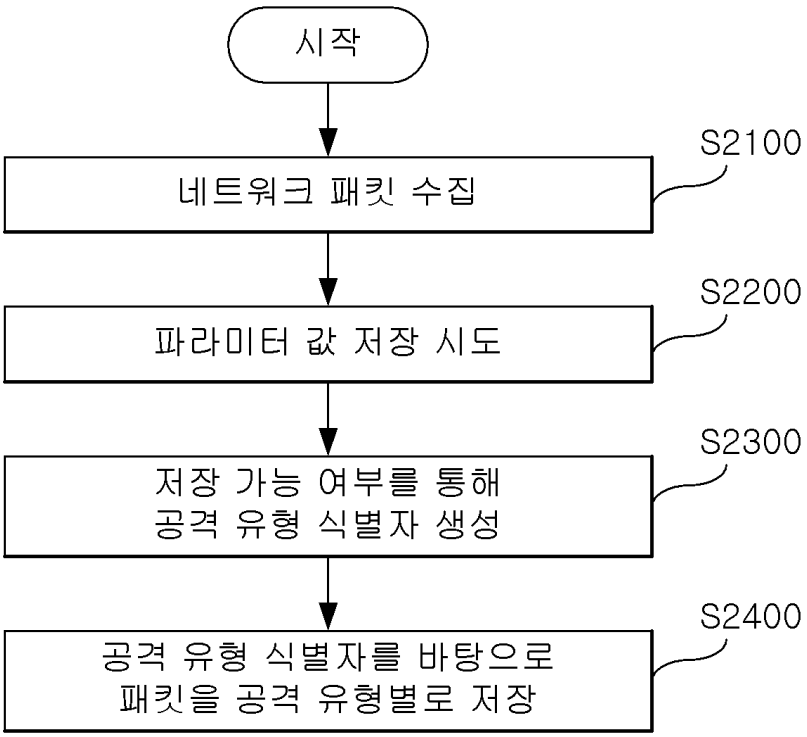
도면13


S200
S210
공격 유형 식별자 생성
S220
패킷을 공격 유형별로 저장

도면14


시작
S1100
네트워크 패킷 수집
S1200
파라미터 값 저장 시도
S1300
저장 가능 여부를 통해 공격 유형 식별

도면15


시작
S2100
네트워크 패킷 수집
S2200
파라미터 값 저장 시도
S2300
저장 가능 여부를 통해
공격 유형 식별자 생성
S2400
공격 유형 식별자를 바탕으로
패킷을 공격 유형별로 저장