(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년03월06일
(11) 등록번호 10-1499116
(24) 등록일자 2015년02월27일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) *H04L 12/24* (2006.01)
H04L 9/00 (2006.01)
(21) 출원번호 10-2013-0146603
(22) 출원일자 2013년11월28일
심사청구일자 2013년11월28일
(56) 선행기술조사문헌
KR1020060042788 A*
KR100656352 B1
KR100826884 B1
KR1020080050919 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국과학기술정보연구원
대전광역시 유성구 대학로 245 (어은동)
(72) 발명자
송보연
대전광역시 유성구 반석동로 33, 502동 2301호 (반석동, 반석마을5단지아파트)
송중석
서울특별시 강남구 선릉로90길 56, 1134호 (대치동, 대치동 대우아이빌명문가)
(뒷면에 계속)
(74) 대리인
특허법인 남앤드남

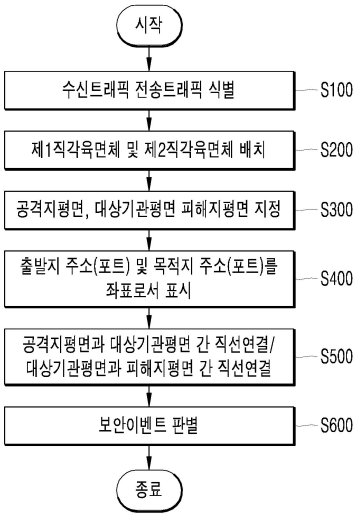
전체 청구항 수 : 총 21 항 심사관 : 장석환

(54) 발명의 명칭 **보안이벤트 판별 방법 및 이에 적용되는 장치**

(57) 요 약

본 발명은 보안이벤트 판별 방법 및 이에 적용되는 장치를 개시한다. 즉, 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하여 3차원 공간상에 가시화하여 표시하고, 수신트래픽 및 전송트래픽이 3차원 공간상에 표시되고 있는 형태로부터 보안이벤트를 판별함으로써, 대량으로 발생하는 사이버 위협을 신속하고도 정확하게 파악할 수 있다.

대 표 도 - 도6



(72) 발명자

최상수

대전광역시 유성구 노은로 353, 303동 1507호 (하기동, 송림마을3단지아파트)

박학수

대전광역시 유성구 진잠로149번길 30, 210동 501호 (교촌동, 한승미메이드아파트)

특허청구의 범위

청구항 1

대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하는 식별부;

상기 수신트래픽과 상기 전송트래픽 모두를 3차원 공간상에 가시화하여 표시하는 표시부; 및

상기 3차원 공간상에 표시되고 있는 상기 수신트래픽 및 상기 전송트래픽 중 적어도 하나로부터 상기 대상기관과 관련하여 발생하고 있는 보안이벤트를 판별하는 판별부를 포함하며,

상기 3차원 공간에는,

상기 대상기관에 해당하는 대상기관평면, 상기 수신트래픽의 출발지에 해당하는 공격지평면, 및 상기 전송트래픽의 목적지에 해당하는 피해지평면이 포함되는 것을 특징으로 하는 보안이벤트판별장치.

청구항 2

제 1 항에 있어서,

상기 3차원 공간에는,

수평면을 형성하는 X축 Y축, 및 상기 수평면에 대하여 수직면을 형성하는 Z축으로 이루어진 직각 좌표계에서, 동일한 모양과 크기를 갖는 제1직각육면체 및 제2직각육면체가 상기 X축 방향으로 서로의 수직면이 인접하도록 연속하여 위치하며,

상기 표시부는,

상기 3차원 공간에서 서로의 수직면이 인접하도록 위치하고 있는 상기 제1직각육면체 및 상기 제2직각육면체 상에서 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 하는 보안이벤트판별장치.

청구항 3

제 2 항에 있어서,

상기 제1직각육면체 및 상기 제2직각육면체 상에는,

상기 대상기관에 해당하는 대상기관평면, 상기 수신트래픽의 출발지에 해당하는 공격지평면, 및 상기 전송트래픽의 목적지에 해당하는 피해지평면 중 적어도 하나가 지정되며,

상기 표시부는,

상기 제1직각육면체와 상기 제2직각육면체가 서로 인접하고 있는 수직평면을 상기 대상기관평면으로서 지정하고, 상기 제1직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 공격지평면으로서 지정하며, 상기 제2직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 피해지평면으로서 지정하여 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 하는 보안이벤트판별장치.

청구항 4

제 3 항에 있어서,

상기 대상기관이 2 이상인 경우,

상기 표시부는,

상기 대상기관평면을 상기 2 이상의 대상기관의 개수에 대응하는 직각셀(Cell)로서 분할하여, 상기 분할된 직각셀 각각에 대하여 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 하는 보안이벤트판별장치.

청구항 5

제 3 항 또는 제 4 항에 있어서,

상기 수신트래픽 및 상기 전송트래픽 각각에는,

출발지 주소(IP), 출발지 포트(Port), 목적지 주소, 및 목적지 포트가 포함되며,

상기 표시부는,

상기 수신트래픽의 출발지 주소 및 출발지 포트의 경우 상기 공격지평면 상의 좌표로서 가시화하여 표시하며, 또한 상기 수신트래픽의 목적지 주소 및 목적지 포트, 내지는 상기 전송트래픽의 출발지 주소 및 출발지 포트의 경우, 상기 대상기관평면 상의 좌표로서 가시화하여 표시하며, 아울러 상기 전송트래픽의 목적지 주소 및 목적지 포트의 경우, 상기 피해지평면 상의 좌표로서 가시화하여 표시하는 것을 특징으로 하는 보안이벤트 판별장치.

청구항 6

제 5 항에 있어서,

상기 표시부는,

상기 공격지평면에서의 상기 Y축을 상기 수신트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 공격지평면에서의 상기 Z축을 상기 수신트래픽의 출발지 포트의 좌표로서 가시화하여 표시하며, 또한 상기 대상기관평면에서의 상기 Y축을 상기 수신트래픽의 목적지 주소 또는 상기 전송트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 대상기관평면에서의 상기 Z축을 상기 수신트래픽에서의 목적지 포트 또는 상기 전송트래픽에서의 출발지 포트의 좌표로서 가시화하여 표시하며, 아울러 상기 피해지평면에서의 상기 Y축을 상기 전송트래픽의 목적지 주소의 좌표로서 가시화하여 표시하고, 상기 피해지평면에서의 상기 Z축을 상기 전송트래픽의 출발지 포트의 좌표로서 가시화하여 표시하는 것을 특징으로 하는 보안이벤트 판별장치.

청구항 7

제 6 항에 있어서,

상기 표시부는,

상기 수신트래픽의 출발지 주소 및 출발지 포트에 해당하는 상기 공격지평면 상의 좌표와, 상기 수신트래픽의 목적지 주소 및 출발지 포트에 해당하는 상기 대상기관평면상의 좌표 상호 간을 연결하는 직선으로서 상기 수신트래픽을 가시화하여 표시하며, 또한 상기 전송트래픽의 출발지 주소 및 출발지 포트에 해당하는 상기 대상기관평면 상의 좌표와, 상기 전송트래픽의 목적지 주소 및 출발지 포트에 해당하는 상기 피해지평면 상의 좌표 상호 간을 연결하는 직선으로서 상기 전송트래픽을 가시화하여 표시하는 것을 특징으로 하는 보안이벤트판별장치.

청구항 8

제 7 항에 있어서,

상기 보안이벤트는,

상기 수신트래픽 및 상기 전송트래픽 각각의 목적지 주소 또는 목적지 포트를 기초로 판별되며,

상기 판별부는,

상기 수신트래픽 및 상기 전송트래픽 각각에서 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 포트는 동일하되 서로 상이한 목적지 주소에 해당하는 설정 개수 이상의 좌표들을 연결하는 직선들이 표시되거나, 내지는, 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 주소는 동일하되 서로 상이한 목적지 포트에 해당하는 설정 개수 이상의 좌표들을 연결하는 직선들이 표시되는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 하는 보안이벤트판별장치.

청구항 9

제 7 항에 있어서,

상기 보안이벤트는,

상기 수신트래픽 및 상기 전송트래픽 각각의 출발지 포트를 기초로 판별되며,

상기 판별부는,

상기 수신트래픽 및 상기 전송트래픽 각각에서 출발지 주소는 동일하되 서로 상이한 출발지 포트에 해당하는 설정 개수 이상의 좌표들과, 동일한 목적지 주소 및 목적지 포트에 해당하는 하나의 좌표를 연결하는 직선들이 표시되는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 하는 보안이벤트판별장치.

청구항 10

제 7 항에 있어서,

상기 보안이벤트는,

상기 전송트래픽의 목적지 주소, 및 목적지 포트를 기초로 판별되며,

상기 판별부는,

상기 수신트래픽이 존재하지 않은 상태에서, 상기 전송트래픽의 목적지 주소 및 목적지 포트가 기 설정된 특정 대상기관에 해당하는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 하는 보안이벤트판별장치.

청구항 11

대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하는 식별단계;

상기 수신트래픽과 상기 전송트래픽 모두를 3차원 공간상에 가시화하여 표시하는 표시단계; 및

상기 3차원 공간상에 표시되고 있는 상기 수신트래픽 및 상기 전송트래픽 중 적어도 하나로부터 상기 대상기관과 관련하여 발생하고 있는 보안이벤트를 판별하는 판별단계를 포함하며,

상기 3차원 공간에는,

상기 대상기관에 해당하는 대상기관평면, 상기 수신트래픽의 출발지에 해당하는 공격지평면, 및 상기 전송트래픽의 목적지에 해당하는 피해지평면이 포함되는 것을 특징으로 하는 보안이벤트판별장치의 동작 방법.

청구항 12

제 11 항에 있어서,

상기 3차원 공간에는,

수평면을 형성하는 X축 Y축, 및 상기 수평면에 대하여 수직면을 형성하는 Z축으로 이루어진 직각 좌표계에서, 동일한 모양과 크기를 갖는 제1직각육면체 및 제2직각육면체가 상기 X축 방향으로 서로의 수직면이 인접하도록 연속하여 위치하며,

상기 표시단계는,

상기 3차원 공간에서 서로의 수직면이 인접하도록 위치하고 있는 상기 제1직각육면체 및 상기 제2직각육면체 상에서 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 하는 보안이벤트판별장치의 동작 방법.

청구항 13

제 12 항에 있어서,

상기 제1직각육면체 및 상기 제2직각육면체 상에는,

상기 대상기관에 해당하는 대상기관평면, 상기 수신트래픽의 출발지에 해당하는 공격지평면, 및 상기 전송트래픽의 목적지에 해당하는 피해지평면 중 적어도 하나가 지정되며,

상기 표시단계는,

상기 제1직각육면체와 상기 제2직각육면체가 서로 인접하고 있는 수직평면을 상기 대상기관평면으로서 지정하고, 또한 상기 제1직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 공격지평면으로서 지정하며, 아울러 상기 제2직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 피해지평면으로서 지정하여 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 하는 보안이벤트판별장치의 동작 방법.

청구항 14

제 13 항에 있어서,

상기 대상기관이 2 이상인 경우,

상기 표시단계는,

상기 대상기관평면을 상기 2 이상의 대상기관의 개수에 대응하는 직각셀(Cell)로서 분할하여, 상기 분할된 직각셀 각각에 대하여 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 하는 보안이벤트판별장치의 동작 방법.

청구항 15

제 13 항 또는 제 14 항에 있어서,

상기 수신트래픽 및 상기 전송트래픽 각각에는,

출발지 주소(IP), 출발지 포트(Port), 목적지 주소, 및 목적지 포트가 포함되며,

상기 표시단계는,

상기 수신트래픽의 출발지 주소 및 출발지 포트의 경우 상기 공격지평면 상의 좌표로서 가시화하여 표시하며, 또한 상기 수신트래픽의 목적지 주소 및 목적지 포트, 내지는 상기 전송트래픽의 출발지 주소 및 출발지 포트의 경우, 상기 대상기관평면 상의 좌표로서 가시화하여 표시하며, 아울러 상기 전송트래픽의 목적지 주소 및 목적지 포트의 경우, 상기 피해지평면 상의 좌표로서 가시화하여 표시하는 것을 특징으로 하는 보안이벤트 판별장치의 동작 방법.

청구항 16

제 15 항에 있어서,

상기 표시단계는,

상기 공격지평면에서의 상기 Y축을 상기 수신트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 공격지평면에서의 상기 Z축을 상기 수신트래픽의 출발지 포트의 좌표로서 가시화하여 표시하며, 또한 상기 대상기관평면에서의 상기 Y축을 상기 수신트래픽의 목적지 주소 또는 상기 전송트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 대상기관평면에서의 상기 Z축을 상기 수신트래픽에서의 목적지 포트 또는 상기 전송트래픽에서의 출발지 포트의 좌표로서 가시화하여 표시하며, 아울러 상기 피해지평면에서의 상기 Y축을 상기 전송트래픽의 목적지 주소의 좌표로서 가시화하여 표시하고, 상기 피해지평면에서의 상기 Z축을 상기 전송트래픽의 출발지 포트의 좌표로서 가시화하여 표시하는 것을 특징으로 하는 보안이벤트 판별장치의 동작 방법.

청구항 17

제 16 항에 있어서,

상기 표시단계는,

상기 수신트래픽의 출발지 주소 및 출발지 포트에 해당하는 상기 공격지평면 상의 좌표와, 상기 수신트래픽의 목적지 주소 및 출발지 포트에 해당하는 상기 대상기관평면상의 좌표 상호 간을 연결하는 직선으로서 상기 수신트래픽을 가시화하여 표시하며, 또한 상기 전송트래픽의 출발지 주소 및 출발지 포트에 해당하는 상기 대상기관평면 상의 좌표와, 상기 전송트래픽의 목적지 주소 및 출발지 포트에 해당하는 상기 피해지평면 상의 좌표 상호 간을 연결하는 직선으로서 상기 전송트래픽을 가시화하여 표시하는 것을 특징으로 하는 보안이벤트판별장치의 동작 방법.

청구항 18

제 17 항에 있어서,

상기 보안이벤트는,

상기 수신트래픽 및 상기 전송트래픽 각각의 목적지 주소 또는 목적지 포트를 기초로 판별되며,

상기 판별단계는,

상기 수신트래픽 및 상기 전송트래픽 각각에서 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 포트는 동일하되 서로 상이한 목적지 주소에 해당하는 설정 개수 이상의 좌표들을 연결하는 직선들이 표시되거나, 내지는, 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 주소는 동일하되 서로 상이한 목적지 포트에 해당하는 설정 개수 이상의 좌표들을 연결하는 직선들이 표시되는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 하는 보안이벤트판별장치의 동작 방법.

청구항 19

제 17 항에 있어서,

상기 보안이벤트는,

상기 수신트래픽 및 상기 전송트래픽 각각의 출발지 포트를 기초로 판별되며,

상기 판별단계는,

상기 수신트래픽 및 상기 전송트래픽 각각에서 출발지 주소는 동일하되 서로 상이한 출발지 포트에 해당하는 설정 개수 이상의 좌표들과, 동일한 목적지 주소 및 목적지 포트에 해당하는 하나의 좌표를 연결하는 직선들이 표시되는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 하는 보안이벤트판별장치의 동작 방법.

청구항 20

제 17 항에 있어서,

상기 보안이벤트는,

상기 전송트래픽의 목적지 주소, 및 목적지 포트를 기초로 판별되며,

상기 판별단계는,

상기 수신트래픽이 존재하지 않은 상태에서, 상기 전송트래픽의 목적지 주소 및 목적지 포트가 기 설정된 특정 대상기관에 해당하는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 하는 보안이벤트판별장치의 동작 방법.

청구항 21

대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하는 식별단계;

상기 수신트래픽과 상기 전송트래픽 모두를 3차원 공간상에 가시화하여 표시하는 표시단계; 및

상기 3차원 공간상에 표시되고 있는 상기 수신트래픽 및 상기 전송트래픽 중 적어도 하나로부터 상기 대상기관과 관련하여 발생하고 있는 보안이벤트를 판별하는 판별단계를 수행하기 위한 명령들을 포함하며,

상기 3차원 공간에는,

상기 대상기관에 해당하는 대상기관평면, 상기 수신트래픽의 출발지에 해당하는 공격지평면, 및 상기 전송트래픽의 목적지에 해당하는 피해지평면이 포함되는 것을 특징으로 하는 컴퓨터 판독 가능 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수

신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하여 3차원 공간상에 가시화하여 표시함으로써, 수신트래픽 및 전송트래픽이 3차원 공간상에서 표시되고 있는 형태로부터 보안이벤트를 효과적으로 판별하기 위한 방안에 관한 것이다.

배 경 기 술

[0002] 급변하는 사이버 위협상황에서 이에 대한 신속하고도 정확한 보안관제 및 침해대응을 수행하기 위해서는, 침해위협정보에 대한 효과적인 관제 및 대응이 요구된다.

[0003] 이를 위한, 침해위협분석시스템(TMS: Threat Management System)의 경우, 관제하고자 하는 대상기관의 네트워크단에 센서를 설치하여 네트워크 트래픽을 수집하고, 수집된 네트워크 트래픽으로부터 보안이벤트를 실시간으로 관제할 수 있는 사용자 인터페이스를 제공하는 것이 일반적이다.

[0004] 이처럼, 침해위협분석시스템에서 관제할 수 있는 보안이벤트의 경우, 관제하는 대상기관이 증가할수록, 또한 인터넷의 사용 증가에 따른 사이버 위협이 증가할수록 큰 폭으로 증가하는 추세이다.

[0005] 헌데, 전술한 침해위협분석시스템에서 제공하는 사용자 인터페이스의 경우 텍스트(Text) 기반으로서 제공되게 되며, 이에, 방대한 분량의 보안이벤트에 대한 직관적 분석이 어렵고, 뿐만 아니라 관제요원의 과중한 업무 부하를 초래한다는 문제점이 존재하게 된다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 상기한 사정을 감안하여 창출된 것으로서, 본 발명에서 도달하고자 하는 목적은, 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하여 3차원 공간상에 가시화하여 표시하고, 수신트래픽 및 전송트래픽이 3차원 공간상에 표시되고 있는 형태로부터 보안이벤트를 판별함으로써, 대량으로 발생하는 사이버 위협을 신속하고도 정확하게 파악할 수 있도록 하는데 있다.

과제의 해결 수단

[0007] 상기 목적을 달성하기 위한 본 발명의 제 1 관점에 따른 보안이벤트판별장치는, 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하는 식별부; 상기 수신트래픽과 상기 전송트래픽 모두를 3차원 공간상에 가시화하여 표시하는 표시부; 및 상기 3차원 공간상에 표시되고 있는 상기 수신트래픽 및 상기 전송트래픽 중 적어도 하나로부터 상기 대상기관과 관련하여 발생하고 있는 보안이벤트를 판별하는 판별부를 포함하는 것을 특징으로 한다.

[0008] 보다 구체적으로, 상기 3차원 공간에는, 수평면을 형성하는 X축 Y축, 및 상기 수평면에 대하여 수직면을 형성하는 Z축으로 이루어진 직각 좌표계에서, 동일한 모양과 크기를 갖는 제1직각육면체 및 제2직각육면체가 상기 X축 방향으로 서로의 수직면이 인접하도록 연속하여 위치하며, 상기 표시부는, 상기 3차원 공간에서 서로의 수직면이 인접하도록 위치하고 있는 상기 제1직각육면체 및 상기 제2직각육면체 상에서 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 한다.

[0009] 보다 구체적으로, 상기 제1직각육면체 및 상기 제2직각육면체 상에는, 상기 대상기관에 해당하는 대상기관평면, 상기 수신트래픽의 출발지에 해당하는 공격지평면, 및 상기 전송트래픽의 목적지에 해당하는 피해지평면 중 적어도 하나가 지정되며, 상기 표시부는, 상기 제1직각육면체와 상기 제2직각육면체가 서로 인접하고 있는 수직평면을 상기 대상기관평면으로서 지정하고, 상기 제1직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 공격지평면으로서 지정하며, 상기 제2직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 피해지평면으로서 지정하여 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 한다.

[0010] 보다 구체적으로, 상기 대상기관이 2 이상인 경우, 상기 표시부는, 상기 대상기관평면을 상기 2 이상의 대상기관의 개수에 대응하는 직각셀(Cell)로서 분할하여, 상기 분할된 직각셀 각각에 대하여 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 한다.

[0011] 보다 구체적으로, 상기 수신트래픽 및 상기 전송트래픽 각각에는, 출발지 주소(IP), 출발지 포트(Port), 목적지 주소, 및 목적지 포트가 포함되며, 상기 표시부는, 상기 수신트래픽의 출발지 주소 및 출발지 포트의 경우 상기 공격지평면 상의 좌표로서 가시화하여 표시하며, 또한 상기 수신트래픽의 목적지 주소 및 목적지 포트, 내지는 상기 전송트래픽의 출발지 주소 및 출발지 포트의 경우, 상기 대상기관평면 상의 좌표로서 가시화하여 표시하며, 아울러 상기 전송트래픽의 목적지 주소 및 목적지 포트의 경우, 상기 피해지평면 상의 좌표로서 가시화하여 표시하는 것을 특징으로 한다.

[0012] 보다 구체적으로, 상기 표시부는, 상기 공격지평면에서의 상기 Y축을 상기 수신트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 공격지평면에서의 상기 Z축을 상기 수신트래픽의 출발지 포트의 좌표로서 가시화하여 표시하며, 또한 상기 대상기관평면에서의 상기 Y축을 상기 수신트래픽의 목적지 주소 또는 상기 전송트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 대상기관평면에서의 상기 Z축을 상기 수신트래픽에서의 목적지 포트 또는 상기 전송트래픽에서의 출발지 포트의 좌표로서 가시화하여 표시하며, 아울러 상기 피해지평면에서의 상기 Y축을 상기 전송트래픽의 목적지 주소의 좌표로서 가시화하여 표시하고, 상기 피해지평면에서의 상기 Z축을 상기 전송트래픽의 출발지 포트의 좌표로서 가시화하여 표시하는 것을 특징으로 한다.

[0013] 보다 구체적으로, 상기 표시부는, 상기 수신트래픽의 출발지 주소 및 출발지 포트에 해당하는 상기 공격지평면 상의 좌표와, 상기 수신트래픽의 목적지 주소 및 출발지 포트에 해당하는 상기 대상기관평면상의 좌표 상호 간을 연결하는 직선으로서 상기 수신트래픽을 가시화하여 표시하며, 또한 상기 전송트래픽의 출발지 주소 및 출발지 포트에 해당하는 상기 대상기관평면 상의 좌표와, 상기 전송트래픽의 목적지 주소 및 출발지 포트에 해당하는 상기 피해지평면 상의 좌표 상호 간을 연결하는 직선으로서 상기 전송트래픽을 가시화하여 표시하는 것을 특징으로 한다.

[0014] 보다 구체적으로, 상기 보안이벤트는, 상기 수신트래픽 및 상기 전송트래픽 각각의 목적지 주소 또는 목적지 포트를 기초로 판별되며, 상기 판별부는, 상기 수신트래픽 및 상기 전송트래픽 각각에서 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 포트는 동일하되 서로 상이한 목적지 주소에 해당하는 설정 개수 이상의 좌표들을 연결하는 직선들이 표시되거나, 내지는, 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 주소는 동일하되 서로 상이한 목적지 포트에 해당하는 설정 개수 이상의 좌표들을 연결하는 직선들이 표시되는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 한다.

[0015] 보다 구체적으로, 상기 보안이벤트는, 상기 수신트래픽 및 상기 전송트래픽 각각의 출발지 포트를 기초로 판별되며, 상기 판별부는, 상기 수신트래픽 및 상기 전송트래픽 각각에서 출발지 주소는 동일하되 서로 상이한 출발지 포트에 해당하는 설정 개수 이상의 좌표들과, 동일한 목적지 주소 및 목적지 포트에 해당하는 하나의 좌표를 연결하는 직선들이 표시되는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 한다.

[0016] 보다 구체적으로, 상기 보안이벤트는, 상기 전송트래픽의 목적지 주소, 및 목적지 포트를 기초로 판별되며, 상기 판별부는, 상기 수신트래픽이 존재하지 않은 상태에서, 상기 전송트래픽의 목적지 주소 및 목적지 포트가 기설정된 특정 대상기관에 해당하는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 한다.

[0017] 상기 목적을 달성하기 위한 본 발명의 제 2 관점에 따른 보안이벤트판별장치의 동작 방법은, 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하는 식별단계; 상기 수신트래픽과 상기 전송트래픽 모두를 3차원 공간상에 가시화하여 표시하는 표시단계; 및 상기 3차원 공간상에 표시되고 있는 상기 수신트래픽 및 상기 전송트래픽 중 적어도 하나로부터 상기 대상기관과 관련하여 발생하고 있는 보안이벤트를 판별하는 판별단계를 포함하는 것을 특징으로 한다.

[0018] 보다 구체적으로, 상기 3차원 공간에는, 수평면을 형성하는 X축 Y축, 및 상기 수평면에 대하여 수직면을 형성하는 Z축으로 이루어진 직각 좌표계에서, 동일한 모양과 크기를 갖는 제1직각육면체 및 제2직각육면체가 상기 X축 방향으로 서로의 수직면이 인접하도록 연속하여 위치하며, 상기 표시단계는, 상기 3차원 공간에서 서로의 수직면이 인접하도록 위치하고 있는 상기 제1직각육면체 및 상기 제2직각육면체 상에서 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 한다.

[0019] 보다 구체적으로, 상기 제1직각육면체 및 상기 제2직각육면체 상에는, 상기 대상기관에 해당하는 대상기관평면, 상기 수신트래픽의 출발지에 해당하는 공격지평면, 및 상기 전송트래픽의 목적지에 해당하는 피해지평면 중 적어도 하나가 지정되며, 상기 표시단계는, 상기 제1직각육면체와 상기 제2직각육면체가 서로 인접하고 있는 수직평면을 상기 대상기관평면으로서 지정하고, 또한 상기 제1직각육면체에서 상기 대상기관평면으로 지정된 수직평

면의 맞은편에 위치하는 수직평면을 상기 공격지평면으로서 지정하며, 아울러 상기 제2직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 피해지평면으로서 지정하여 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 한다.

[0020] 보다 구체적으로, 상기 대상기관이 2 이상인 경우, 상기 표시단계는, 상기 대상기관평면을 상기 2 이상의 대상기관의 개수에 대응하는 직각셀(Cell)로서 분할하여, 상기 분할된 직각셀 각각에 대하여 상기 수신트래픽과 상기 전송트래픽 모두를 가시화하여 표시하는 것을 특징으로 한다.

[0021] 보다 구체적으로, 상기 수신트래픽 및 상기 전송트래픽 각각에는, 출발지 주소(IP), 출발지 포트(Port), 목적지 주소, 및 목적지 포트가 포함되며, 상기 표시단계는, 상기 수신트래픽의 출발지 주소 및 출발지 포트의 경우 상기 공격지평면 상의 좌표로서 가시화하여 표시하며, 또한 상기 수신트래픽의 목적지 주소 및 목적지 포트, 내지는 상기 전송트래픽의 출발지 주소 및 출발지 포트의 경우, 상기 대상기관평면 상의 좌표로서 가시화하여 표시하며, 아울러 상기 전송트래픽의 목적지 주소 및 목적지 포트의 경우, 상기 피해지평면 상의 좌표로서 가시화하여 표시하는 것을 특징으로 한다.

[0022] 보다 구체적으로, 상기 표시단계는, 상기 공격지평면에서의 상기 Y축을 상기 수신트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 공격지평면에서의 상기 Z축을 상기 수신트래픽의 출발지 포트의 좌표로서 가시화하여 표시하며, 또한 상기 대상기관평면에서의 상기 Y축을 상기 수신트래픽의 목적지 주소 또는 상기 전송트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 대상기관평면에서의 상기 Z축을 상기 수신트래픽에서의 목적지 포트 또는 상기 전송트래픽에서의 출발지 포트의 좌표로서 가시화하여 표시하며, 아울러 상기 피해지평면에서의 상기 Y축을 상기 전송트래픽의 목적지 주소의 좌표로서 가시화하여 표시하고, 상기 피해지평면에서의 상기 Z축을 상기 전송트래픽의 출발지 포트의 좌표로서 가시화하여 표시하는 것을 특징으로 한다.

[0023] 보다 구체적으로, 상기 표시단계는, 상기 수신트래픽의 출발지 주소 및 출발지 포트에 해당하는 상기 공격지평면 상의 좌표와, 상기 수신트래픽의 목적지 주소 및 출발지 포트에 해당하는 상기 대상기관평면상의 좌표 상호 간을 연결하는 직선으로서 상기 수신트래픽을 가시화하여 표시하며, 또한 상기 전송트래픽의 출발지 주소 및 출발지 포트에 해당하는 상기 대상기관평면 상의 좌표와, 상기 전송트래픽의 목적지 주소 및 출발지 포트에 해당하는 상기 피해지평면 상의 좌표 상호 간을 연결하는 직선으로서 상기 전송트래픽을 가시화하여 표시하는 것을 특징으로 한다.

[0024] 보다 구체적으로, 상기 보안이벤트는, 상기 수신트래픽 및 상기 전송트래픽 각각의 목적지 주소 또는 목적지 포트를 기초로 판별되며, 상기 판별단계는, 상기 수신트래픽 및 상기 전송트래픽 각각에서 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 포트는 동일하되 서로 상이한 목적지 주소에 해당하는 설정 개수 이상의 좌표들을 연결하는 직선들이 표시되거나, 내지는, 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 주소는 동일하되 서로 상이한 목적지 포트에 해당하는 설정 개수 이상의 좌표들을 연결하는 직선들이 표시되는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 한다.

[0025] 보다 구체적으로, 상기 보안이벤트는, 상기 수신트래픽 및 상기 전송트래픽 각각의 출발지 포트를 기초로 판별되며, 상기 판별단계는, 상기 수신트래픽 및 상기 전송트래픽 각각에서 출발지 주소는 동일하되 서로 상이한 출발지 포트에 해당하는 설정 개수 이상의 좌표들과, 동일한 목적지 주소 및 목적지 포트에 해당하는 하나의 좌표를 연결하는 직선들이 표시되는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 한다.

[0026] 보다 구체적으로, 상기 보안이벤트는, 상기 전송트래픽의 목적지 주소, 및 목적지 포트를 기초로 판별되며, 상기 판별단계는, 상기 수신트래픽이 존재하지 않은 상태에서, 상기 전송트래픽의 목적지 주소 및 목적지 포트가 기 설정된 특정 대상기관에 해당하는 경우를 상기 보안이벤트로서 판별하는 것을 특징으로 한다.

[0027] 상기 목적을 달성하기 위한 본 발명의 제 3 관점에 따른 컴퓨터 판독 가능 기록매체는, 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하는 식별단계; 상기 수신트래픽과 상기 전송트래픽 모두를 3차원 공간상에 가시화하여 표시하는 표시단계; 및 상기 3차원 공간상에 표시되고 있는 상기 수신트래픽 및 상기 전송트래픽 중 적어도 하나로부터 상기 대상기관과 관련하여 발생하고 있는 보안이벤트를 판별하는 판별단계를 수행하기 위한 명령들을 포함하는 것을 특징으로 한다.

발명의 효과

[0028] 이에, 본 발명의 보안이벤트 판별 방법 및 이에 적용되는 장치에 의하면, 대상기관과 관련하여 수집되는 네트워

크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하여 3차원 공간상에 가시화하여 표시하고, 수신트래픽 및 전송트래픽이 3차원 공간상에 표시되고 있는 형태로부터 보안이벤트를 판별함으로써, 대량으로 발생하는 사이버 위협을 신속하고도 정확하게 파악할 수 있다.

도면의 간단한 설명

[0029] 도 1은 본 발명의 일 실시예에 따른 보안이벤트판별장치의 개략적인 구성도.

도 2 및 3은 본 발명의 일 실시예에 따른 수신트래픽 및 전송트래픽이 3차원 공간상에 가시화하여 표시되는 형태를 설명하기 위한 도면.

도 4 및 도 5는 본 발명의 일 실시예에 따른 3차원 공간상에 표시되고 있는 수신트래픽 및 전송트래픽으로부터 판별되는 보안이벤트의 종류를 설명하기 위한 도면.

도 6은 본 발명의 일 실시예에 따른 보안이벤트판별장치에서의 동작 흐름을 설명하기 위한 순서도.

발명을 실시하기 위한 구체적인 내용

[0030] 이하, 첨부된 도면을 참조하여 본 발명의 일 실시예에 대하여 설명한다.

[0031] 도 1은 본 발명의 일 실시예에 따른 보안이벤트판별장치를 도시한 도면이다.

[0032] 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 보안이벤트판별장치는 실시간 관제가 요구되는 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 수신트래픽 및 전송트래픽을 식별하는 식별부(100), 식별된 수신트래픽 및 전송트래픽을 3차원 공간상에 가시화하여 표시하는 표시부(200), 및 3차원 공간상에 표시되고 있는 수신트래픽 및 전송트래픽으로부터 보안이벤트를 판별하는 판별부(300)를 포함하는 구성을 갖는다.

[0033] 또한, 본 발명의 일 실시예에 따른 보안이벤트판별장치는, 전술한 구성 이외에, 실시간 관제가 요구되는 대상기관의 네트워크 단에 설치된 센서로부터 네트워크 트래픽을 수집하는 수집부(도시안됨)을 더 포함하는 구성을 가질 수 있다.

[0034] 여기서, 식별부(100), 표시부(200), 판별부(300) 및 수집부(도시안됨)를 포함하는 본 발명의 일 실시예에 따른 보안이벤트판별장치의 전술한 구성 전체 내지는 그 일부는, 프로세서에 의해 실행되는 소프트웨어 모듈 형태로서 구현되거나, 내지는 하드웨어로서 구현될 수 있다.

[0035] 이러한, 보안이벤트판별장치는, 가시화되는 수신트래픽 및 전송트래픽을 표시할 수 있는 디스플레이패널을 구비하고 있는 다양한 기기를 일컫는다.

[0036] 예를 들어, 보안이벤트판별장치는, PC, 테블릿 PC, 및 PDA, 등이 해당될 수 있으며, 이에 제한되는 것이 아닌, 가시화되는 수신트래픽 및 전송트래픽을 표시할 수 있는 디스플레이패널을 구비한 기기는 모두 포함될 수 있을 것이다.

[0037] 한편, 본 발명의 일 실시예에 따르면, 실시간 관제가 요구되는 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 보안이벤트를 실시간으로 판별하기 사용자 인터페이스를 제공하게 된다.

[0038] 이처럼, 보안이벤트를 판별하기 위해 제공되는 사용자인터페이스의 경우, 텍스트(Text) 기반으로서 제공되는 것이 일반적이었다.

[0039] 헌데, 보안이벤트의 경우 관제하는 대상기관이 증가할수록, 또한 인터넷의 사용 증가에 따른 사이버 위협이 증가할수록 큰 폭으로 증가하게 되나, 전술한 바와 같이 텍스트 기반의 사용자인터페이스를 제공하는 경우에는, 방대한 분량의 보안이벤트에 대한 직관적 분석이 어렵고, 뿐만 아니라 관제요원의 과중한 업무 부하를 초래하게 된다.

[0040] 이렇듯, 관제하는 대상기관 및 사이버 위협이 증가하는 환경에서, 방대한 분량의 보안이벤트를 신속하고도 정확하게 판별하기 위해서는, 이에 대한 효과적인 관제 및 대응을 위한 새로운 방안이 요구된다 할 것이다

[0041] 이에, 본 발명의 일 실시예에서는, 관제가 요구되는 다수의 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 보안이벤트를 신속하고도 정확하게 판별하기 위한 새로운 방안을 제안하고자 하며, 이하에서는 이를 구체적으로 설명하기로 한다.

[0042] 우선, 식별부(100)는 대상기관과 관련하여 수집되는 네트워크 트래픽을 식별하는 기능을 수행한다.

[0043] 보다 구체적으로, 식별부(100)는 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽과, 반대로 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별한다.

[0044] 이때, 식별부(100)는 네트워크 트래픽으로부터 상기 수신트래픽 및 상기 전송트래픽 각각에 대한 출발지 주소(IP)와 출발지 포트(Port), 목적지 주소와 목적지 포트를 식별하게 된다.

[0045] 또한, 식별부(100)는 상기 수신트래픽 및 전송트래픽 각각을 식별함에 있어서, 수신트래픽 및 전송트래픽 각각에 대하여 네트워크 프로토콜(예: TCP, UDP, ICMP), 식별시간(탐지시간), 및 패킷(Packets) 양(예: bps, Kbps, Mbps) 등을 추가로 식별할 수 있다.

[0046] 그리고, 표시부(200)는 수신트래픽과 전송트래픽을 가시화하여 표시하는 기능을 수행한다.

[0047] 보다 구체적으로, 표시부(200)는 대상기관에 대한 수신트래픽 및 전송트래픽이 식별부(100)에서 식별되면, 3차원 공간상에 서로 인접하도록 위치시킨 제1직각육면체 및 제2직각육면체 상에서 식별된 수신트래픽 및 전송트래픽 모두를 가시화하여 표시하게 된다.

[0048] 이때, 표시부(200)는 도 2에 도시한 바와 같이 수평면을 형성하는 X축 Y축, 및 수평면에 대하여 수직면을 형성하는 Z축으로 이루어진 3차원 공간의 직각 좌표계에서, 동일한 모양과 크기를 갖는 제1직각육면체 및 제2직각육면체가 상기 X축 방향으로 서로의 수직면이 인접하도록 연속하여 위치시키게 된다.

[0049] 여기서, 제1직각육면체 및 제2직각육면체 상에는, 대상기관에 해당하는 대상기관평면, 상기 수신트래픽의 출발지에 해당하는 공격지평면, 및 상기 전송트래픽의 목적지에 해당하는 피해지평면이 지정될 수 있다.

[0050] 이에, 표시부(200)는 제1직각육면체와 제2직각육면체가 서로 인접하고 있는 수직평면을 대상기관평면으로서 지정하고, 또한 상기 제1직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 공격지평면으로서 지정하며, 아울러, 상기 제2직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 피해지평면으로서 지정하게 된다.

[0051] 아울러, 표시부(200)는 전술한 바와 같이, 3차원 공간 상에 위치시킨 제1지각육면체 및 제2직각육면체 상에서 공격지평면, 대상기관평면, 및 피해지평면이 지정되는 경우, 우선 공격지평면과 대상기관평면 상에 수신트래픽을 가시화하여 표시함과 아울러 대상기관평면과, 피해지평면 상에 전송트래픽을 가시화하여 표시하게 된다.

[0052] 여기서, 수신트래픽의 출발지 주소 및 출발지 포트의 경우, 공격지평면 상의 좌표로서 표시되고, 또한 수신트래픽의 목적지 주소 및 목적지 포트, 내지는 상기 전송트래픽의 출발지 주소 및 출발지 포트의 경우, 상기 대상기관평면 상의 좌표로서 가시화하여 표시되며, 아울러, 전송트래픽의 목적지 주소 및 목적지 포트의 경우, 피해지평면 상의 좌표로서 가시화하여 표시될 수 있다.

[0053] 이에, 표시부(200)는 공격지평면에서의 Y축을 수신트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 공격지평면에서의 상기 Z축을 상기 수신트래픽의 출발지 포트의 좌표로서 가시화하여 표시하게 된다.

[0054] 또한, 표시부(200)는 대상기관평면에서의 Y축을 수신트래픽의 목적지 주소 또는 상기 전송트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 대상기관평면에서의 Z축을 상기 수신트래픽에서의 목적지 포트 또는 상기 전송트래픽에서의 출발지 포트의 좌표로서 가시화하여 표시하게 된다.

[0055] 아울러, 표시부(200)는 피해지평면에서의 Y축을 상기 전송트래픽의 목적지 주소의 좌표로서 가시화하여 표시하고, 상기 피해지평면에서의 상기 Z축을 상기 전송트래픽의 출발지 포트의 좌표로서 가시화하여 표시하게 된다.

[0056] 한편, 전술한 바와 같이 공격지평면, 대상기관평면 및 피해지평면 각각에서 출발지 주소와 출발지 포트 내지는 목적지 주소와 목적지 포트를 좌표로서 표시함에 있어서, 다음과 같은 방식이 적용될 수 있다.

[0057] 우선, 공격지평면에 표시되는 수신트래픽의 출발지 주소와, 대상기관평면에 표시되는 전송트래픽의 출발지 주소의 경우, 예컨대, 출발지 주소의 십진수 변환값을 선형적으로 나열하는 방식인 선형방식(Linear Method)이 적용될 수 있다.

[0058] 이에, 수신트래픽의 출발지 주소가 표시되는 공격지평면과, 전송트래픽의 출발지 주소가 표시되는 대상기관평면의 Y축의 경우 출발지 주소의 최소값(0.0.0.0)을 십진수로 변환한 값인 '0'부터 출발지 주소의 최대값(255.255.255.255)를 십진수로 변환한 값인 '4,294,967,295' 사이의 좌표를 갖게 된다.

[0059] 반대로, 대상기관평면에 표시되는 수신트래픽의 목적지 주소와, 피해지평면에 표시되는 전송트래픽의 목적지 주소의 경우, 예컨대, 목적지 주소를 뒤집은 후, 뒤집은 목적지 주소의 십진수 변환값을 선형적으로 나열하는 방식인 역변환방식(Reversed Octet Method)이 적용될 수 있다.

[0060] 이에, 수신트래픽의 목적지 주소가 표시되는 대상기관평면의 Y축과, 전송트래픽의 목적지 주소가 표시되는 피해지평면의 Y축의 경우, 출발지 주소의 최소값(0.0.0.0)을 십진수로 변환한 값인 '0'부터 출발지 주소의 최대값(255.255.255.255)를 십진수로 변환한 값인 '4,294,967,295' 사이의 좌표를 갖게 된다.

[0061] 예를 들어, 목적지 주소가 '192.168.0.5'인 경우에 전술한 역변환방식을 적용하면, 목적지 주소는 '5.0.168.192'가 되고, 이를 십진수 값으로 변환하면, '83,929,280'이 되어, 이는 대상기관평면 또는 피해지평면의 Z축에서 좌표값이 될 수 있다.

[0062] 이처럼, 목적지 주소의 좌표값으로서 역변환방식을 적용하는 것은, 보안이벤트 중 하나로서 목적지 포트는 고정된 상태에서 목적지 주소를 변동하여 스캔하는 네트워크 스캔을 용이하게 식별하기 위함이다.

[0063] 즉, 수신트래픽 또는 전송트래픽의 목적지 주소가 1씩 증가하는 경우, 역변환방식에서의 실질적인 십진수 변환값은, 1씩 증가하는 것이 아닌, 2^24(16,777,216)씩 증가하게 되므로, 그 식별이 용이하게 때문이다.

[0064] 다음, 공격지평면에 표시되는 수신트래픽의 출발지 포트, 대상기관평면에 표시되는 수신트래픽의 목적지 포트와 전송트래픽의 출발지 포트, 그리고 피해지평면에 표시되는 전송트래픽의 목적지 포트의 경우, 예컨대, 포트 값을 상용로그 값으로 환산하는 상용로그방식(Common Logarithmic Method)이 적용될 수 있다.

[0065] 이에, 수신트래픽의 출발지 포트가 표시되는 공격지평면의 Z축, 수신트래픽의 목적지 포트와 전송트래픽의 출발지 포트가 표시되는 대상기관평면의 Z축, 전송트래픽의 목적지 포트가 표시되는 피해지평면의 Z축의 경우, 최소값인 '0'부터 출발지 포트의 최대값(65535)을 상용로그로 환산한 값인 '4.8164733038' 사이의 좌표를 갖게 된다.

[0066] 나아가, 표시부(200)는 전술한 바와 같이 공격지평면, 대상기관평면 및 피해지평면 각각에서 출발지 주소와 출발지 포트 내지는 목적지 주소와 목적지 포트를 좌표로서 표시되면, 공격지평면과 대상기관평면 사이를 연결하는 직선으로서 수신트래픽을 가시화하여 표시하며, 대상기관평면과 피해지평면 사이를 연결하는 직선으로서 전송트래픽을 가시화하여 표시하게 된다.

[0067] 즉, 표시부(200)는 수신트래픽의 출발지 주소 및 출발지 포트에 해당하는 공격지평면 상의 좌표와, 수신트래픽의 목적지 주소 및 출발지 포트에 해당하는 대상기관평면상의 좌표 상호 간을 연결하는 직선으로서 수신트래픽을 가시화하여 표시하며, 또한 전송트래픽의 출발지 주소 및 출발지 포트에 해당하는 대상기관평면 상의 좌표와, 전송트래픽의 목적지 주소 및 출발지 포트에 해당하는 피해지평면 상의 좌표 상호 간을 연결하는 직선으로서 상기 전송트래픽을 가시화하여 표시한다.

[0068] 한편, 대상기관평면에는 하나의 대상기관만이 아닌 다수의 대상기관이 표시될 수 있다.

[0069] 이에, 표시부(200)는 도 3(a)에 도시한 바와 같이, 대상기관평면을 관제가 요구되는 대상기관의 개수(예: 47개)에 대응하는 각각의 직각셀(Cell)로서 분할하고, 분할된 직각셀 각각에 대하여 수신트래픽과 상기 전송트래픽 모두를 개별적으로 가시화하여 표시하게 된다.

[0070] 이때, 표시부(200)는 대상기관평면에 표시중인 특정 대상기관(예: KS)가 선택되는 경우에는, 도 3(b)에 도시한 바와 같이, 선택된 상기 특정 대상기관에 대해서만, 독립적으로 수신트래픽과 상기 전송트래픽를 개별적으로 가시화하여 표시할 수 있다.

[0071] 덧붙여, 표시부(200)는 전술한 바와 같이 수신트래픽과 전송트래픽을 3차원공간에 가시화하여 표시함에 있어서, 수신트래픽과 전송트래픽을 네트워크 프로토콜(예: TCP, UDP, ICMP) 및 포트에 따른 그룹으로 분류하고, 분류된 그룹에 따른 명칭과 색상으로 가시화하여 표시할 수 있다.

[0072] 예를 들어, 네트워크 프로토콜이 TCP인 경우, HTTP와 관련된 포트[80(of HTTP), 8080(of Tomcat), 443(of HTTPS)], Remote Access와 관련된 포트[3389(of RDP), 22(of SSH)], NetBIOS와 관련된 포트[139(of NetBIOS)], e-mail과 관련된 포트[25(of SMTP), 110(of POP3), 143(of IMAP)], DB와 관련된 포트[1433(of MS-SQL), 1521(of Oracle), 3306(of My SQL)], 및 잘 알려진(well-known) 포트[0 ~ 1023 (위에서 언급한 포트는 제외) 등으로 분류될 수 있다.

[0073] 또한, 네트워크 프로토콜이 UDP인 경우, DNS와 관련된 포트[53(of DNS), 잘 알려진(well-known) 포트[0 ~

1023(위에서 언급한 포트는 제외)] 등으로 분류될 수 있다.

[0074] 아울러, 네트워크 프로토콜 IMCP인 경우에는 포트와 상관없이 한 개의 그룹의 분류될 수 있다.

[0075] 그 밖에, 표시부(200)는 3차원 공간에 직선의 형태로서 표시되고 있는 수신트래픽 또는 전송트래픽이 사용자에 의해 선택되는 경우에는, 예컨대, 네트워크 프로토콜, 출발지 주소(포트), 목적지 주소(포트), 식별 시간(탐지 시간), 패킷의 양, 대상기관명칭(국가) 등의 부가정보를 함께 표시할 수 있을 것이다.

[0076] 그리고, 판별부(300)는 보안이벤트를 판별하는 기능을 수행한다.

[0077] 보다 구체적으로, 판별부(300)는 3차원 공간상에 표시되고 있는 수신트래픽 및 전송트래픽의 표시 형태로부터 대상기관과 관련하여 발생하고 있는 다양한 보안이벤트를 판별하게 된다.

[0078] 여기서, 판별부(300)에서 판별되는 보안이벤트의 경우, 예컨대, 네트워크 스캔 이벤트, 포트 스캔 이벤트, 디도스(DDoS) 이벤트가 해당될 수 있다.

[0079] 예를 들어, 판별부(300)는 도 4 (a)에 도시한 바와 같이, 수신트래픽 및 상기 전송트래픽 각각에서 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 포트는 동일하되 서로 상이한 목적지 주소에 해당하는 다수의 좌표들을 연결하는 직선들이 표시되는 경우, 이를 네트워크 스캔 이벤트로서 판별할 수 있다.

[0080] 다른 예로서, 판별부(300)는 도 4 (b)에 도시한 바와 같이, 수신트래픽 및 상기 전송트래픽 각각에서 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 주소는 동일하되 서로 상이한 목적지 포트에 해당하는 다수의 좌표들을 연결하는 직선들이 표시되는 경우, 이를 포트 스캔 이벤트로서 판별할 수 있다.

[0081] 또 다른 예로서, 판별부(300)는 도 5 (a)에 도시한 바와 같이, 수신트래픽 및 전송트래픽 각각에서 출발지 주소는 동일하되 서로 상이한 출발지 포트에 해당하는 다수의 좌표들과, 동일한 목적지 주소 및 목적지 포트에 해당하는 하나의 좌표를 연결하는 직선들이 표시되는 경우, 이를 디도스 이벤트로서 판별할 수 있다.

[0082] 그 밖의 예로서, 판별부(300)는 도 5 (b)에 도시한 바와 같이, 수신트래픽이 존재하지 않은 상태에서, 전송트래픽의 목적지 주소 및 목적지 포트가 기 설정된 특정 대상기관에 해당하는 경우, 즉, 전송트래픽이 대상기관을 출발지로 하여 또 다른 대상기관을 목적지로 하는 경우에는 보안 이벤트로서 판별할 수 있다.

[0083] 이상에서 살펴본 바와 같이, 본 발명의 일 실시예에 따른 보안이벤트판별장치에 따르면, 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하여 3차원 공간상에 가시화하여 표시하고, 수신트래픽 및 전송트래픽이 3차원 공간상에 표시되고 있는 형태로부터 보안이벤트를 판별함으로써, 대량으로 발생하는 사이버 위협을 신속하고도 정확하게 파악할 수 있다.

[0084] 이하에서는 도 6을 참조하여, 본 발명의 일 실시예에 따른 보안이벤트판별장치의 동작 방법을 설명하도록 한다.

[0085] 여기서, 설명의 편의를 위해 전술한 도 1에 도시된 구성은 해당 참조번호를 언급하여 설명하겠다.

[0086] 먼저, 식별부(100)는 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽과, 반대로 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별한다(S100).

[0087] 이때, 식별부(100)는 네트워크 트래픽으로부터 상기 수신트래픽 및 상기 전송트래픽 각각에 대한 출발지 주소(IP)와 출발지 포트(Port), 목적지 주소와 목적지 포트를 식별하게 된다.

[0088] 또한, 식별부(100)는 상기 수신트래픽 및 전송트래픽 각각을 식별함에 있어서, 수신트래픽 및 전송트래픽 각각에 대하여 네트워크 프로토콜(예: TCP, UDP, ICMP), 식별시간(탐지시간), 및 패킷(Packets) 양(예: bps, Kbps, Mbps) 등을 추가로 식별할 수 있다.

[0089] 그런 다음, 표시부(200)는 대상기관에 대한 수신트래픽 및 전송트래픽이 식별부(100)에서 식별되면, 3차원 공간상에서 제1직각육면체 및 제2직각육면체를 서로 인접하도록 위치시킨다(S200).

[0090] 이때, 표시부(200)는 수평면을 형성하는 X축 Y축, 및 수평면에 대하여 수직면을 형성하는 Z축으로 이루어진 3차원 공간의 직각 좌표계에서, 동일한 모양과 크기를 갖는 제1직각육면체 및 제2직각육면체가 상기 X축 방향으로 서로의 수직면이 인접하도록 연속하여 위치시키게 된다.

[0091] 다음으로, 표시부(200)는 제1직각육면체와 제2직각육면체가 서로 인접하고 있는 수직평면을 대상기관평면으로서 지정하고, 또한 상기 제1직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면

을 상기 공격지평면으로서 지정하며, 아울러, 상기 제2직각육면체에서 상기 대상기관평면으로 지정된 수직평면의 맞은편에 위치하는 수직평면을 상기 피해지평면으로서 지정한다(S300).

[0092] 그리고 나서, 표시부(200)는 수신트래픽의 출발지 주소 및 출발지 포트를 공격지평면 상의 좌표로서 표시하고, 또한 수신트래픽의 목적지 주소 및 목적지 포트, 내지는 상기 전송트래픽의 출발지 주소 및 출발지 포트를 대상기관평면 상의 좌표로서 가시화하여 표시하며, 아울러, 전송트래픽의 목적지 주소 및 목적지 포트를 피해지평면 상의 좌표로서 가시화하여 표시한다(S400).

[0093] 이때, 표시부(200)는 공격지평면에서의 Y축을 수신트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 상기 공격지평면에서의 상기 Z축을 상기 수신트래픽의 출발지 포트의 좌표로서 가시화하여 표시하게 된다.

[0094] 또한, 표시부(200)는 대상기관평면에서의 Y축을 수신트래픽의 목적지 주소 또는 전송트래픽의 출발지 주소의 좌표로서 가시화하여 표시하고, 대상기관평면에서의 Z축을 상기 수신트래픽에서의 목적지 포트 또는 상기 전송트래픽에서의 출발지 포트의 좌표로서 가시화하여 표시하게 된다.

[0095] 아울러, 표시부(200)는 피해지평면에서의 Y축을 상기 전송트래픽의 목적지 주소의 좌표로서 가시화하여 표시하고, 상기 피해지평면에서의 상기 Z축을 상기 전송트래픽의 출발지 포트의 좌표로서 가시화하여 표시하게 된다.

[0096] 나아가, 표시부(200)는 전술한 바와 같이 공격지평면, 대상기관평면 및 피해지평면 각각에서 출발지 주소와 출발지 포트 내지는 목적지 주소와 목적지 포트를 좌표로서 표시되면, 공격지평면과 대상기관평면 사이를 연결하는 직선으로서 수신트래픽을 가시화하여 표시하며, 대상기관평면과 피해지평면 사이를 연결하는 직선으로서 전송트래픽을 가시화하여 표시한다(S500).

[0097] 이때, 표시부(200)는 수신트래픽의 출발지 주소 및 출발지 포트에 해당하는 공격지평면 상의 좌표와, 수신트래픽의 목적지 주소 및 출발지 포트에 해당하는 대상기관평면상의 좌표 상호 간을 연결하는 직선으로서 수신트래픽을 가시화하여 표시하며, 또한 전송트래픽의 출발지 주소 및 출발지 포트에 해당하는 대상기관평면 상의 좌표와, 전송트래픽의 목적지 주소 및 출발지 포트에 해당하는 피해지평면 상의 좌표 상호 간을 연결하는 직선으로서 상기 전송트래픽을 가시화하여 표시한다.

[0098] 이후, 판별부(300)는 3차원 공간상에 표시되고 있는 수신트래픽 및 전송트래픽의 표시 형태로부터 대상기관과 관련하여 발생하고 있는 다양한 보안이벤트를 판별한다(S600).

[0099] 이때, 판별부(300)는 수신트래픽 및 상기 전송트래픽 각각에서 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 포트는 동일하되 서로 상이한 목적지 주소에 해당하는 다수의 좌표들을 연결하는 직선들이 표시되는 경우, 이를 네트워크 스캔 이벤트로서 판별하게 된다.

[0100] 또한, 판별부(300)는 수신트래픽 및 상기 전송트래픽 각각에서 동일한 출발지 주소 및 출발지 포트에 해당하는 하나의 좌표와, 목적지 주소는 동일하되 서로 상이한 목적지 포트에 해당하는 다수의 좌표들을 연결하는 직선들이 표시되는 경우, 이를 포트 스캔 이벤트로서 판별하게 된다.

[0101] 아울러, 판별부(300)는 수신트래픽 및 전송트래픽 각각에서 출발지 주소는 동일하되 서로 상이한 출발지 포트에 해당하는 다수의 좌표들과, 동일한 목적지 주소 및 목적지 포트에 해당하는 하나의 좌표를 연결하는 직선들이 표시되는 경우, 이를 디도스 이벤트로서 판별하게 된다.

[0102] 그 밖에, 판별부(300)는 수신트래픽이 존재하지 않은 상태에서, 전송트래픽의 목적지 주소 및 목적지 포트가 기설정된 특정 대상기관에 해당하는 경우, 즉, 전송트래픽이 대상기관을 출발지로 하여 또 다른 대상기관을 목적지로 하는 경우에는 이를 보안 이벤트로서 판별하게 된다.

[0103] 이상에서 살펴본 바와 같이, 본 발명의 일 실시예에 따른 보안이벤트판별장치의 동작 방법에 따르면, 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하여 3차원 공간상에 가시화하여 표시하고, 수신트래픽 및 전송트래픽이 3차원 공간상에 표시되고 있는 형태로부터 보안이벤트를 판별함으로써, 대량으로 발생하는 사이버 위협을 신속하고도 정확하게 파악할 수 있다.

[0104] 한편, 여기에 제시된 실시예들과 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거

나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0105] 지금까지 본 발명을 바람직한 실시 예를 참조하여 상세히 설명하였지만, 본 발명이 상기한 실시 예에 한정되는 것은 아니며, 이하의 특허청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 또는 수정이 가능한 범위까지 본 발명의 기술적 사상이 미친다 할 것이다.

산업상 이용가능성

[0106] 본 발명의 보안이벤트 판별 방법 및 이에 적용되는 장치에 따르면, 대상기관과 관련하여 수집되는 네트워크 트래픽으로부터 상기 대상기관을 목적지로 하여 수신되는 수신트래픽 및 상기 대상기관을 출발지로 하여 전송되는 전송트래픽을 식별하여 3차원 공간상에 가시화하여 표시함으로써, 상기 3차원 공간상에 표시되고 있는 상기 수신트래픽 및 상기 전송트래픽으로부터 보안이벤트를 효과적으로 판별할 수 있다는 점에서, 기존 기술의 한계를 뛰어 넘음에 따라 관련 기술에 대한 이용만이 아닌 적용되는 장치의 시판 또는 영업의 가능성이 충분할 뿐만 아니라 현실적으로 명백하게 실시할 수 있는 정도이므로 산업상 이용가능성이 있는 발명이다.

부호의 설명

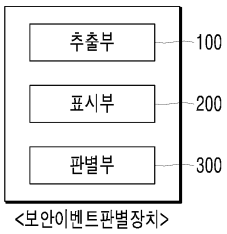
[0107] 100: 식별부

200: 표시부

300: 판별부

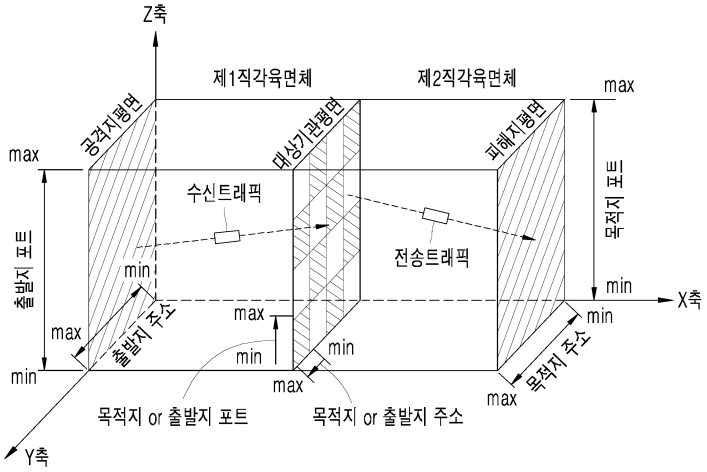
도면

도면1

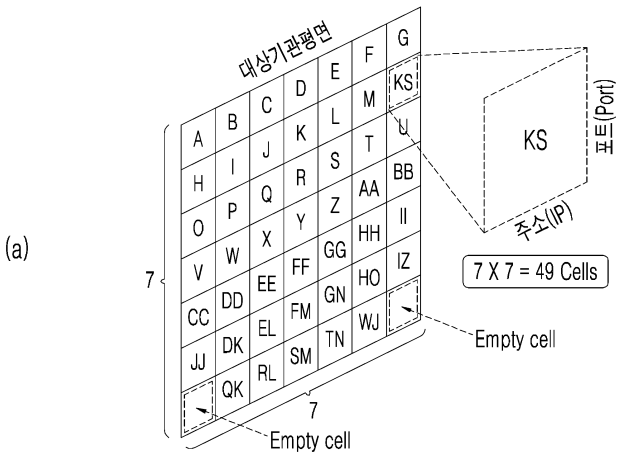


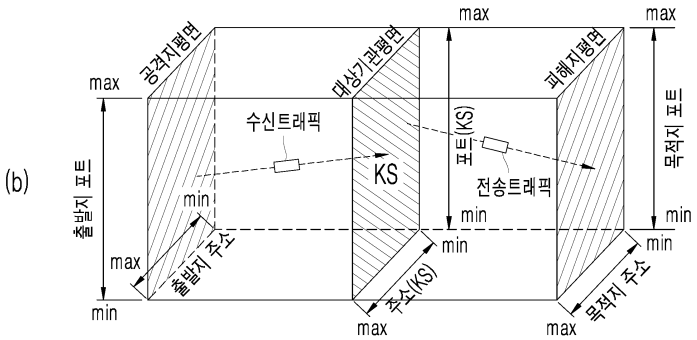
<보안이벤트판별장치>

도면2

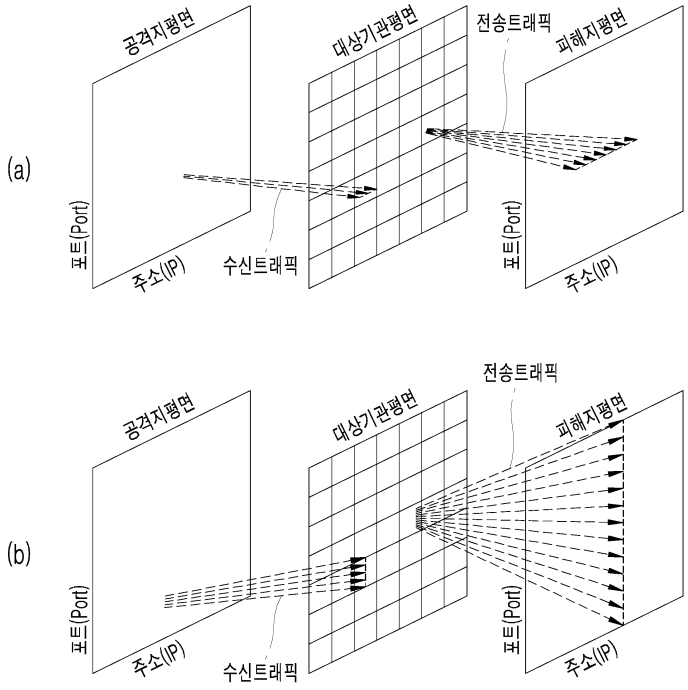

Z축
제1직각육면체
제2직각육면체
공격지평면
대상기관평면
피해지평면
max
min
수신트래픽
전송트래픽
출발지 포트
목적지 포트
출발지 주소
목적지 주소
목적지 or 출발지 포트
목적지 or 출발지 주소
X축
Y축

도면3

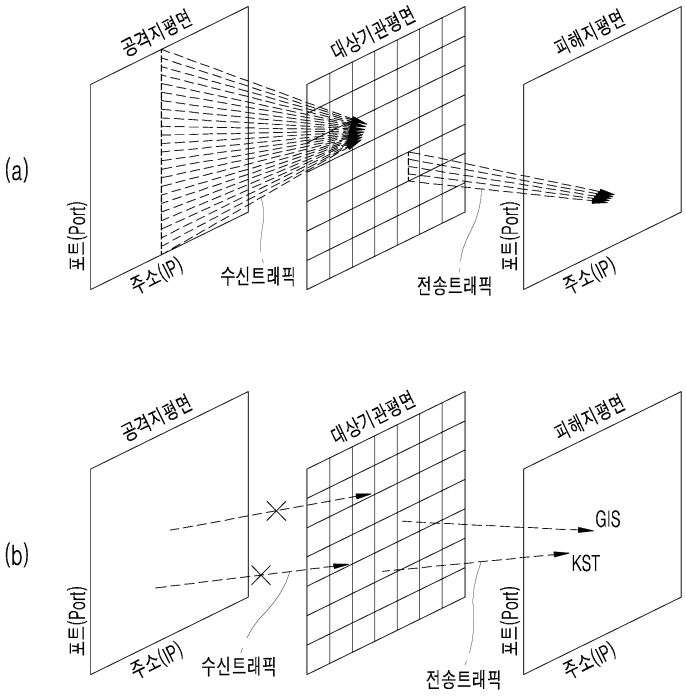

(a)
대상기관평면
KS
포트(Port)
주소(IP)
7 X 7 = 49 Cells
Empty cell
Empty cell
7
7


(b)
공격지평면
대상기관평면
피해지평면
수신트래픽
KS
포트(KS)
전송트래픽
출발지 포트
목적지 포트
출발지 주소
주소(KS)
목적지 주소
max
min

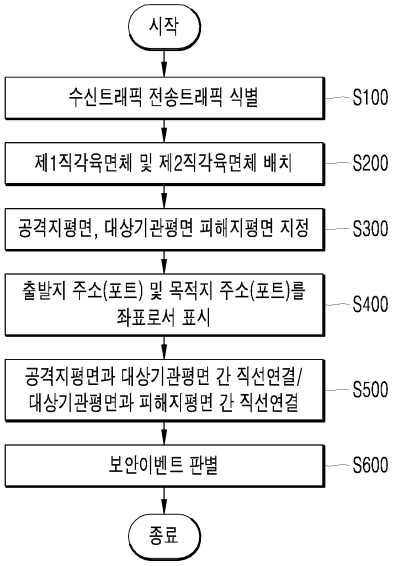
도면4


(a)
공격지평면
대상기관평면
전송트래픽
피해지평면
포트(Port)
주소(IP)
수신트래픽
포트(Port)
주소(IP)
(b)
전송트래픽
공격지평면
대상기관평면
피해지평면
포트(Port)
주소(IP)
수신트래픽
포트(Port)
주소(IP)

도면5


(a)
공격지평면
대상기관평면
피해지평면
포트(Port)
주소(IP)
수신트래픽
전송트래픽
포트(Port)
주소(IP)
(b)
공격지평면
대상기관평면
피해지평면
GIS
KST
포트(Port)
주소(IP)
수신트래픽
전송트래픽
포트(Port)
주소(IP)

도면6


시작
수신트래픽 전송트래픽 식별
S100
제1직각육면체 및 제2직각육면체 배치
S200
공격지평면, 대상기관평면 피해지평면 지정
S300
출발지 주소(포트) 및 목적지 주소(포트)를 좌표로서 표시
S400
공격지평면과 대상기관평면 간 직선연결/ 대상기관평면과 피해지평면 간 직선연결
S500
보안이벤트 판별
S600
종료