(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년01월21일
(11) 등록번호 10-1940512
(24) 등록일자 2019년01월15일

(51) 국제특허분류(Int. Cl.)
G06F 21/55 (2013.01) *G06F 21/56* (2013.01)
(21) 출원번호 10-2014-0012271
(22) 출원일자 2014년02월03일
심사청구일자 2017년08월03일
(65) 공개번호 10-2015-0091713
(43) 공개일자 2015년08월12일
(56) 선행기술조사문헌
US20070226796 A1*
US20120124666 A1*
US20120137361 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
김종현
대전광역시 서구 둔산북로 215 가람아파트 10동 1206호
김익균
대전광역시 유성구 대덕대로 594 타워코리아나 904호
(74) 대리인
한양특허법인

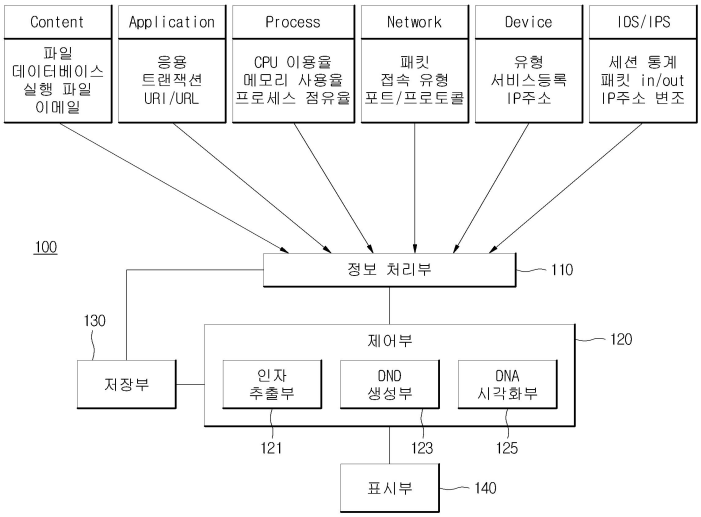
전체 청구항 수 : 총 13 항 심사관 : 정성훈

(54) 발명의 명칭 **공격특성 DNA 분석 장치 및 그 방법**

(57) 요 약

본 발명은 네트워크 환경에서 이벤트 정보를 수집하는 정보 처리부; 상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 인자 추출부; 상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 DNA 생성부; 및 상기 이벤트 정보, 상기 공격특성 DNA가 저장된 저장부;를 포함하는 것을 특징으로 하는 공격특성 DNA 생성 장치를 제공한다. 따라서 본 발명은 수집된 사이버 공격특성 인자를 사이버 공격특성 DNA 들과 비교하여, 현재 진행 중인 공격 유형이 직관적으로 인식될 수 있도록 하는 효과가 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	13-921-06-001
부처명	미래창조과학부
연구관리전문기관	한국방송통신전파진흥원
연구사업명	방송통신ETRI연구개발지원사업
연구과제명	다중소스 데이터의 Long-Term History 분석기반 사이버 표적공격 인지 및 추적기술 개발
기 여 율	1/1
주관기관	한국전자통신연구원
연구기간	2013.03.01 ~ 2017.02.28

명 세 서

청구범위

청구항 1

네트워크 환경에서 이벤트 정보를 수집하는 정보 처리부;

상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 인자 추출부;

상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 DNA 생성부; 및

상기 이벤트 정보, 상기 공격특성 DNA가 저장된 저장부;를 포함하고,

상기 공격특성 DNA는

상기 네트워크 환경에서 두 개 이상의 소스로부터 수집한 상기 이벤트 정보에서 추출된 인자들로 구성된 두 개 이상의 DNA 줄기들을 포함하고, 상기 두 개 이상의 DNA 줄기들 사이의 연관성을 분석한 연관성 정보를 포함하는 인자들로 구성된 하나의 DNA 줄기를 더 포함하는 것

을 특징으로 하는 공격특성 DNA 생성 장치.

청구항 2

제1항에 있어서,

상기 네트워크 환경은 단일 네트워크인 것

을 특징으로 하는 공격특성 DNA 생성 장치.

청구항 3

제1항에 있어서,

상기 저장부에는 상기 공격특성 DNA가 공격유형별로 분류되어 저장된 것

을 특징으로 하는 공격특성 DNA 생성 장치.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 공격특성 DNA를 시각화화는 DNA 시각화부;를 더 포함하는 것

을 특징으로 하는 공격특성 DNA 생성 장치.

청구항 5

제4항에 있어서,

상기 시각화된 공격특성 DNA를 디스플레이하는 표시부;를 더 포함하는 것

을 특징으로 하는 공격특성 DNA 생성 장치.

청구항 6

제4항에 있어서,

상기 DNA 시각화부는 상기 공격특성 DNA를 3D 형태로 시각화하는 것

을 특징으로 하는 공격특성 DNA 생성 장치.

청구항 7

네트워크 환경에서 이벤트 정보를 수집하는 정보 처리부;

상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 인자 추출부;

상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 DNA 생성부;

공격유형별로 분류된 과거 공격특성 DNA가 저장된 저장부; 및

상기 공격특성 DNA를 상기 저장부에 저장된 과거 공격특성 DNA와 비교하여 유사도를 분석하는 공격 유사도 분석부;를 포함하고,

상기 공격특성 DNA는

상기 네트워크 환경에서 두 개 이상의 소스로부터 수집한 상기 이벤트 정보에서 추출된 인자들로 구성된 두 개 이상의 DNA 줄기들을 포함하고, 상기 두 개 이상의 DNA 줄기들 사이의 연관성을 분석한 연관성 정보를 포함하는 인자들로 구성된 하나의 DNA 줄기를 더 포함하는 것

을 특징으로 하는 공격특성 DNA 분석 장치.

청구항 8

제7항에 있어서,

상기 공격 유사도 분석부는 상기 공격특성 DNA와 상기 과거 공격특성 DNA의 유사도를 수치적으로 나타낸 것

을 특징으로 하는 공격특성 DNA 분석 장치.

청구항 9

네트워크 환경에서 이벤트 정보를 수집하는 단계;

상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 단계; 및

상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 단계; 및

상기 이벤트 정보, 상기 공격특성 DNA를 저장하는 단계;를 포함하고,

상기 공격특성 DNA는

상기 네트워크 환경에서 두 개 이상의 소스로부터 수집한 상기 이벤트 정보에서 추출된 인자들로 구성된 두 개 이상의 DNA 줄기들을 포함하고, 상기 두 개 이상의 DNA 줄기들 사이의 연관성을 분석한 연관성 정보를 포함하는 인자들로 구성된 하나의 DNA 줄기를 더 포함하는 것

을 특징으로 하는 공격특성 DNA 생성 방법.

청구항 10

제9항에 있어서,

상기 이벤트 정보, 상기 공격특성 DNA를 저장하는 단계는 상기 공격특성 DNA를 공격유형별로 분류되어 저장하는 것

을 특징으로 하는 공격특성 DNA 생성 방법.

청구항 11

제9항에 있어서,

상기 공격특성 DNA를 시각화하는 단계;를 더 포함하는 것

을 특징으로 하는 공격특성 DNA 생성 방법.

청구항 12

공격유형별로 분류된 과거 공격특성 DNA를 저장하는 단계;

네트워크 환경에서 이벤트 정보를 수집하는 단계;

상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 단계;

상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 단계; 및

상기 저장된 공격유형별로 분류된 과거 공격특성 DNA와 공격특성 DNA를 비교하여 유사도를 분석하는 단계;를 포함하고,

상기 공격특성 DNA는

상기 네트워크 환경에서 두 개 이상의 소스로부터 수집한 상기 이벤트 정보에서 추출된 인자들로 구성된 두 개 이상의 DNA 줄기들을 포함하고, 상기 두 개 이상의 DNA 줄기들 사이의 연관성을 분석한 연관성 정보를 포함하는 인자들로 구성된 하나의 DNA 줄기를 더 포함하는 것

을 특징으로 하는 공격특성 DNA 분석 방법.

청구항 13

제12항에 있어서,

상기 유사도 분석의 결과를 시각화하는 단계;를 더 포함하는 것

을 특징으로 하는 공격특성 DNA 분석 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 공격특성 DNA를 이용하여 공격특성 DNA 분석하는 기술에 관한 것으로, 상세하게는, 수집된 이벤트 정보로부터 고유의 공격특성 인자를 추출하고, 상기 공격특성 인자들간의 연관성을 DNA 구조 형태로 표현한 공격특성 DNA 분석 장치 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 인터넷은 누구나가 전 세계 어디서든지 접속하고자 하는 상대편 컴퓨터에 TCP/IP 라는 공통의 프로토콜을 적용하여 정보 전달을 자유롭게 할 수 있도록 구성된 개방형 네트워크이다. 인터넷은 국내를 비롯하여 세계적으로 사용이 급격하게 증가되면서 기존 산업의 전 부분에 걸쳐 효율성과 생산성 제고를 위한 전략적인 도구로서 중요성이 급속히 증대되고 있다.

[0003] 한편, 이러한 인터넷을 통한 통신 환경을 저해하는 요소로서 악성 프로그램을 이용하여 인터넷에 연결된 특정 대상 컴퓨터를 공격함으로써 원하는 정보를 탈취하려는 공격들이 이루어지고 있다. 악성 프로그램(malicious program)은 악의적인 목적을 위해 작성된 실행 가능한 코드의 통칭으로서, 멀웨어(malware, malicious software), 악성코드(malicious code)라고도 하며, 자기 복제 능력과 감염 대상의 유무에 따라, 바이러스(Virus), 웜바이러스(worm virus), 트로이목마(Trojan horse) 등으로 분류될 수 있다.

[0004] 종래의 악성 프로그램 피해 방지 기술은 해당 공격에 대한 시그니처를 탐지하여 차단하거나, 네트워크 단에서의 트래픽을 필터링하여 유해 트래픽을 차단하는 방법을 사용하였다. 시그니처는 수집된 바이러스 샘플로서, 바이러스의 흔적이라고 할 수 있다. 상기 시그니처는 안티 바이러스 소프트웨어를 만들기 위해 사용된다. 상기 시그니처를 바탕으로 하는 탐지 기술은 이미 수집된 악성코드의 특징을 분석해 해당 악성코드를 탐지하는 시그니처를 생성하고 상기 시그니처를 기반으로 멀웨어를 스캐닝하고, 악성 프로그램이 탐지되었을 경우 해당 악성 프로그램처리 프로세스를 수행하는 것을 말한다.

[0005] 그러나, 하루에도 수천, 수만 개의 악성코드가 생성됨으로써 공격자들이 만들어내는 신종 악성코드 수와 보안업체들이 처리하는 시그니처 수의 격차는 좀처럼 좁혀 들지 않고 있으며, 오히려 그 간격이 점차 커지고 있는 것이 오늘날의 현실이다. 또한 소스코드, 함수 등 악성코드의 내부 구조를 지속적으로 변화시켜 변종 악성코드를 만들어내는 기법이 활용되면서 백신을 우회하는 새로운 악성코드가 빠른 속도로 생성되고 있기 때문에, 사이버 공격을 탐지하고 차단하는 일은 더욱 어려워지고 있다.

[0006] 따라서 주요 IT기반 시설의 정보시스템을 겨냥한 사이버테러 수준의 표적공격이 사전 인지 및 통합 분석되기 위하여, 다중소스 정보로부터 공격특징인자를 추출하고, 분석된 상황을 효율적으로 시각화하여 기업 내에 발생하는 보안 상황을 직관적으로 파악하는 것이 필수적이다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국공개특허 제10-0942456호(클라우드 컴퓨팅을 이용한 DDoS 공격 탐지 및 차단 방법 및 서버)

발명의 내용

해결하려는 과제

[0008] 본 발명의 목적은 단일 네트워크로 구성된 환경에서 수집된 이벤트 정보로부터 추출된 공격특성 인자간의 연관성을 DNA구조 형태로 나타낸 공격특성 DNA 분석 장치 및 그 방법을 제공하기 위한 것이다.

[0009] 본 발명의 다른 목적은 수집된 이벤트 정보로부터 공격특성 DNA를 생성하여 과거의 공격유형별 공격특성 DNA와 비교분석하는 공격특성 DNA 분석 장치 및 그 방법을 제공하기 위한 것이다.

과제의 해결 수단

[0010] 본 발명의 실시의 일 측면에서, 본 발명은 네트워크 환경에서 이벤트 정보를 수집하는 정보 처리부; 상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 인자 추출부; 상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 DNA 생성부; 및 상기 이벤트 정보, 상기 공격특성 DNA가 저장된 저장부;를 포함하는 것을 특징으로 하는 공격특성 DNA 생성 장치를 제공한다.

[0011] 바람직하게는, 상기 네트워크 환경은 단일 네트워크인 것을 특징으로 하는 공격특성 DNA 생성 장치를 제공한다.

[0012] 바람직하게는, 상기 저장부에는 상기 공격특성 DNA가 공격유형별로 분류되어 저장된 것을 특징으로 하는 공격특성 DNA 생성 장치를 제공한다.

[0013] 바람직하게는, 상기 공격특성 DNA를 시각화화는 DNA 시각화부;를 더 포함하는 것을 특징으로 하는 공격특성 DNA 생성 장치를 제공한다.

[0014] 바람직하게는, 상기 시각화된 공격특성 DNA를 디스플레이하는 표시부;를 더 포함하는 것을 특징으로 하는 공격특성 DNA 생성 장치를 제공한다.

[0015] 본 발명의 실시의 다른 측면에서, 네트워크 환경에서 이벤트 정보를 수집하는 정보 처리부; 상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 인자 추출부; 상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 DNA 생성부; 공격유형별로 분류된 과거 공격특성 DNA가 저장된 저장부; 및 상기 공격특성 DNA를 상기 저장부에 저장된 과거 공격특성 DNA와 비교하여 유사도를 분석하는 공격 유사도 분석부;를 포함하는 것을 특징으로 하는 공격특성 DNA 분석 장치를 제공한다.

[0016] 바람직하게는, 상기 공격 유사도 분석부는 상기 공격특성 DNA와 상기 공격유형별 공격특성 DNA의 유사도를 수치적으로 나타낸 것을 특징으로 하는 공격특성 DNA 분석 장치를 제공한다.

[0017] 본 발명의 실시의 또 다른 측면에서, 네트워크 환경에서 이벤트 정보를 수집하는 단계; 상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 단계; 상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 단계; 및 상기 이벤트 정보, 상기 공격특성 DNA를 저장하는 단계;를 포함하는 것을 특징으로 하는 공격특성 DNA 생성 방법을 제공한다.

[0018] 본 발명의 실시의 또 다른 측면에서, 공격유형별로 분류된 과거 공격특성 DNA를 저장하는 단계; 네트워크 환경에서 이벤트 정보를 수집하는 단계; 상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출하는 단계; 상기 공격특성 인자의 상기 정상 인자와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA를 생성하는 단계; 및 상기 저장된 공격유형별로 분류된 과거 공격특성 DNA와 공격특성 DNA를 비교하여 유사도를 분석하는 단계;를 포함하는 것을 특징으로 하는 공격특성 DNA 분석 방법을 제공한다.

발명의 효과

[0019] 본 발명은 빅데이터 플랫폼 기술을 활용하여 과거에 발생하였던 사이버공격에 대한 공격특성 DNA 프로파일을 구

축하고 관리함으로써 공격유형을 효과적으로 판단하는 효과가 있다.

[0020] 또한, 본 발명은 수집된 사이버 공격특성 인자를 사이버 공격특성 DNA 들과 비교하여, 현재 진행 중인 공격 유형이 직관적으로 인식될 수 있도록 하는 효과가 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 바람직한 일 실시예에 따른 공격특성 DNA 생성 장치의 구성도를 나타내는 도면이다.

도 2는 본 발명의 바람직한 다른 실시예에 따른 공격특성 DNA 분석 장치의 구성도를 나타내는 도면이다.

도 3은 본 발명의 바람직한 일 실시예에 따른 공격특성 DNA가 디스플레이된 표시부의 예시도를 나타내는 도면이다.

도 4는 본 발명의 바람직한 다른 실시예에 따른 공격 유사도 분석이 디스플레이된 표시부의 예시도를 나타내는 도면이다.

도 5는 본 발명의 바람직한 일 실시예에 따른 공격특성 DNA 생성 장치의 흐름도를 나타내는 도면이다.

도 6은 본 발명의 바람직한 다른 실시예에 따른 공격특성 DNA 분석 장치의 흐름도를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 한편, 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 또한 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면 번호에 상관없이 동일한 수단에 대해서는 동일한 참조 번호를 사용하기로 한다.

[0023] 도 1은 본 발명의 바람직한 일 실시예에 따른 공격특성 DNA 생성 장치의 구성도를 나타내는 도면이다.

[0024] 도 1을 참조하면, 공격특성 DNA 생성 장치(100)는 정보 처리부(110), 제어부(120), 저장부(130) 및 표시부(140)를 포함한다. 제어부(120)는 인자 추출부(121), DNA 생성부(123) 및 DNA 시각화부(125)를 포함한다.

[0025] 정보 처리부(110)는 네트워크 환경에서 이벤트 정보를 수집하여 처리한다. 정보 처리부(110)는 수집한다. 정보 처리부(110)는 인자 추출부(121)로부터 전송 신호를 수신하면, 수집된 상기 이벤트 정보를 인자 추출부(121)로 전송한다. 정보 처리부(110)는 수집된 상기 이벤트 정보를 저장부(130)로 전송하여 저장한다.

[0026] 이벤트 정보는 네트워크, 네트워크 장비, 사용자PC 및 서버 등과 같은 네트워크 구성요소들에 관한 정보를 의미한다. 상기 이벤트 정보는 다양한 소스(Source)로부터 야기되는 정보이다. 상기 이벤트 정보는 로그(log)형태의 정보일 수 있다. 또한, 상기 이벤트 정보는 콘텐츠 정보, 어플리케이션 정보, 프로세스 정보, 네트워크 정보, 디바이스 정보, IDS/IPS 정보를 포함할 수 있다. 상기 콘텐츠 정보는 파일, 데이터베이스, 실행 파일 및 이메일에 관한 정보를 포함하고, 상기 어플리케이션 정보는 트랜잭션, URI(Uniform Resource Identifier), URL(Uniform Resource Locator), URN(Uniform Resource Name)에 관한 정보를 포함하고, 상기 프로세스 정보는 CPU 이용율, 메모리 사용율, 프로세스 점유율에 관한 정보를 포함하고, 상기 네트워크 정보는 패킷, 접속 유형, 포트 및 프로토콜에 관한 정보를 포함하고, 상기 디바이스 정보는 유형, IP(Internet Protocol)주소에 관한 정보를 포함하고, 상기 IDS(Intrusion Detecting System)/IPS(Intrusion Preventing System) 정보는 세션 통계,

패킷 In/Out, IP주소 변조여부에 관한 정보를 포함한다.

[0027] 이벤트 정보는 공격 정보를 포함한다. 상기 공격 정보는 악성 프로그램에 관한 정보를 포함한다. 네트워크를 공격하는 침입자는 상기 악성 프로그램을 포함하는 공격 정보를 통하여 네트워크 구성요소들에 위해를 가한다.

[0028] 이벤트 정보는 인자 추출부(121)에 의하여 인자(Factor)를 추출하기 위하여 이용된다. 상기 이벤트 정보의 공격 정보는 공격특성 인자(320)로 추출되고, 상기 공격 정보가 아닌 이벤트 정보는 정상 인자(310)로 추출된다.

[0029] 인자 추출부(121)는 상기 이벤트 정보로부터 인자(Factor)를 추출한다. 인자 추출부(121)는 정보 처리부(110)로 상기 이벤트 정보 전송 신호를 전송하면, 정보 처리부(110)로부터 인자가 추출될 이벤트 정보를 수신한다. 인자 추출부(121)는 상기 이벤트 정보 중의 공격 정보로부터 공격특성 인자(320)를 추출하고, 상기 공격 정보가 아닌 이벤트 정보로부터 정상 인자(310)를 추출한다. 인자 추출부(121)는 상기 이벤트 정보로부터 표적공격을 탐지하기 위한 다양한 분석 알고리즘을 통하여 인자를 추출한다.

[0030] 인자는 파일 DNA(이하, DNA라 통칭함)를 구성하는 기본적인 객체로서, 원자키(Atomic Key)라고도 일컬어진다. 상기 인자는 정상 인자(310)와 공격특성 인자(320)를 포함한다. 공격특성 인자(320)는 상기 이벤트 정보에 포함된 공격 정보로부터 형성되고, 정상 인자(310)는 공격 정보가 아닌 이벤트 정보로부터 형성된다. 정상 인자(310) 및 공격특성 인자(320)를 포함하는 모든 인자는 서로의 연관성에 상응하도록 결합하고, 상기 인자들의 결합이 하나의 DNA를 형성한다.

[0031] DNA 생성부(123)는 인자간의 연관성을 분석하고, 상기 연관성 분석 결과를 DNA구조로 나타낸다. DNA 생성부(123)는 네트워크, 네트워크 장비, 사용자PC 및 서버 등과 같은 네트워크 구성요소들로부터 수집된 유형별 이벤트 정보에 대한 정상 인자(310)들을 정상 인자(310)의 연관성에 상응하도록 결합하여 정상 DNA(313)를 형성한다.

[0032] DNA 생성부(123)는 정상 인자(310)와 공격특성 인자(320)를 기반으로 공격특성 DNA(323)를 형성한다. DNA 생성부(123)는 공격 정보에 대한 공격특성 인자(320)들을 정상 인자(310) 및 공격특성 인자(320)들의 연관성에 상응하도록 정상 인자(310)들과 결합하여 공격특성 DNA(323)를 형성한다. DNA 생성부(123)는 정상 DNA(313)에 공격특성 인자(320)들을 해당 DNA 부분에 위치시켜 결합하여 공격특성 DNA(323)를 형성한다. DNA 생성부(123)는 형성한 공격특성 DNA(323)를 저장부(130)에 저장한다.

[0033] DNA 시각화부(125)는 공격특성 DNA(323)를 시각화한다. DNA 시각화부(125)는 정상 인자(310), 공격특성 인자(320), 정상 DNA(313) 및 공격특성 DNA(323) 등을 시각적으로 표현하여 표시부(140로 하여금 디스플레이 하도록 한다. DNA 시각화부(125)는 정상 인자(310)들의 리스트(List)인 정상 인자 목록(311)을 만들고, 공격특성 인자(320)들의 리스트(List)인 공격특성 인자 목록(321)을 만든다. DNA 시각화부(125)는 DNA 생성부(123)가 생성한 정상 DNA(313)를 시각화하고, 정상 DNA(313)에 공격특성 인자(320)들을 해당 DNA 부분에 표현함으로써 DNA 생성부(123)가 생성한 공격특성 DNA(323)를 시각화한다.

[0034] DNA 시각화부(125)는 DNA 시각화부(125)는 정상 인자(310), 공격특성 인자(320), 정상 DNA(313) 및 공격특성 DNA(323) 등을 2D 또는 3D로 시각화할 수 있고, 이 경우 해당 포맷에 상응하는 시각화 엔진을 사용한다. DNA 시각화부(125)는 DNA를 다양한 각도로 회전시키고, 확대 및 축소가 가능하도록 하여 네트워크에 공격여부를 직관적으로 알 수 있도록 한다.

[0035] 저장부(130)에는 상기 이벤트 정보, 공격특성 DNA(323)가 저장된다. DNA 생성부(123)는 공격특성 DNA(323)를 저장부(130)에 저장한다. 저장된 공격특성 DNA(323)는 공격유형별로 분류되어 저장된다. 저장된 공격특성 DNA(323)는 과거 공격특성 DNA(401, 403, 405, 407)가 되어 공격특성 DNA(323)와 비교분석의 대상이 된다.

[0036] 표시부(140)는 상기 시각화된 정상 인자(310), 공격특성 인자(320), 정상 DNA(313) 및 공격특성 DNA(323) 등을 스크린(Screen)에 디스플레이한다.

[0037] 공격특성 DNA 생성장치(100)가 연결된 네트워크는 단일 네트워크(Single Network)인 것으로 외부 네트워크와 연결되지 않은 하나의 독립망일 수 있다. 가령, 단일 네트워크는 어느 한 기업 또는 단체의 자체망일 수 있다. 공격특성 DNA 생성 장치(100)는 단일 네트워크 이외에, 클라우드 컴퓨팅 환경과 같은 외부 네트워크와 연결된 환경에서도 동작할 수 있다.

[0038] 도 2는 본 발명의 바람직한 다른 실시예에 따른 공격특성 DNA 분석 장치의 구성도를 나타내는 도면이다.

[0039] 도 2를 참조하면, 공격특성 DNA 분석 장치(200)는 정보 처리부(110), 제어부(120), 저장부(130) 및 표시부(140)에 공격 유사도 분석부(201)를 더 포함한다.

[0040] 인자 추출부(121)는 상기 이벤트 정보 중에서 공격 정보가 포함된 경우, 상기 공격 정보로부터 공격특성 인자(320)를 추출한다. 네트워크에 공격이 이뤄지고 상기 공격 정보가 포함될 때마다, 인자 추출부(121)는 상기 이벤트 정보 중에서 상기 공격 정보를 추출하여 공격특성 인자(320)를 생성한다. 공격특성 인자(320)는 과거 공격특성 DNA(401, 403, 405, 407)를 구성하는 객체(Atomic key)가 된다.

[0041] DNA 생성부(123)는 공격특성 인자(320)의 정상 인자(310) 연관성을 분석하여 상기 연관성 분석의 결과를 DNA구조로 나타낸 과거 공격특성 DNA(401, 403, 405, 407)를 생성한다. DNA 생성부(123)는 네트워크, 네트워크 장비, 사용자PC 및 서버 등과 같은 네트워크 구성요소들로부터 수집된 유형별 공격 정보에 대한 공격특성 인자(320)들을 공격특성 인자(320)와 정상 인자(310)간의 연관성에 상응하도록 결합하여 과거 공격특성 DNA(401, 403, 405, 407)를 형성한다. 과거 공격특성 DNA(401, 403, 405, 407)는 정상 DNA(313)와 공격특성 DNA(323)와 동일한 방식으로 생성되고, 과거부터 현재까지의 이벤트 정보 중에 포함된 공격 정보만을 추출하여 공격유형별로 정리되어 분류된 DNA 데이터이다. 즉, 과거 공격특성 DNA(401, 403, 405, 407)는 과거 공격을 받았던 양상을 기록해놓은 DNA와 같다. DNA 생성부(123)는 생성한 과거 공격특성 DNA(401, 403, 405, 407)를 저장부(130)에 저장한다.

[0042] 공격 유사도 분석부(201)는 공격특성 DNA(323)와 저장부(130)에 저장된 과거 공격특성 DNA(401, 403, 405, 407)를 비교하여 유사여부를 분석한다. 공격 유사도 분석부(201)는 공격특성 DNA(323)와 과거 공격특성 DNA(401, 403, 405, 407)의 DNA구조를 매칭시켜서 공격특성 DNA(323)가 특정한 과거 공격특성 DNA(401, 403, 405, 407)와 일치하는 정도를 판단한다.

[0043] 공격 유사도 분석부(201)는 공격 유사도를 수치적으로 나타낸다. 공격 유사도 분석부(201)는 공격 유사도에 대한 수치를 비율 또는 예/아니오 등으로 유사도를 나타낼 수 있다.

[0044] 도 3은 본 발명의 바람직한 일 실시예에 따른 공격특성 DNA가 디스플레이된 표시부의 예시도를 나타내는 도면이다.

[0045] 도 3을 참조하면, 표시부(140)에 디스플레이된 정상 DNA(313) 및 공격특성 DNA(323) 화면의 예시가 도시되어 있다. 표시부(140)는 DNA 시각화부(125)에 의하여 시각화된 정상 인자(310), 정상 인자(310)로 구성된 정상 인자 목록(311), 정상 DNA(313), 공격특성 인자(320), 공격특성 인자(320)로 구성된 공격특성 인자 목록(321) 및 공격특성 DNA(323)를 디스플레이한다.

[0046] 표시부(140)는 정상 DNA(313)를 좌측의 normal state영역에, 공격특성 DNA(323)를 우측의 abnormal state영역에 표시한다. 디스플레이 되는 위치는 본 예시에 한정되지 아니하고, 다양하게 변할 수 있다.

[0047] 정상 DNA(313) 및 공격특성 DNA(323)를 포함하는 DNA는 좌측 DNA 줄기(301), 우측 DNA 줄기(303) 및 중앙 DNA 줄기(305) 이렇게 3부분으로 구성된다. DNA 줄기(301, 303, 305)는 각각 서로 다른 정보들을 포함하는 인자들로 구성된다. 바람직하게는, 좌측 DNA 줄기(301)는 호스트 및 서버에 관련된 정보를 포함하는 인자로 구성되고, 우측 DNA 줄기(303)는 네트워크에 관련된 정보를 포함하는 인자로 구성되며, 중앙 DNA 줄기(305)는 상기 호스트 및 서버에 관련된 정보와 네트워크에 관련된 정보의 연관성 정보를 포함하는 인자로 구성된다. DNA 줄기(301, 303, 305)가 포함하는 정보는 실시예에 한정되지 않고, 상기 호스트, 서버 또는 네트워크 이외에 다른 정보들이 될 수 있다.

[0048] 사용자는 양 상태의 DNA를 비교하면서 DNA 중 어느 부분에 공격특성 인자(320)가 위치하는지 알 수 있고, 어떤 공격유형인지 직관적으로 인식할 수 있다.

[0049] 도 4는 본 발명의 바람직한 다른 실시예에 따른 공격 유사도 분석이 디스플레이된 표시부의 예시도를 나타내는 도면이다.

[0050] 도 4를 참조하면, 표시부(140)에 디스플레이된 과거 공격특성 DNA(401, 403, 405, 407) 화면의 예시가 도시되어 있다. 표시부(140)는 DNA 시각화부(125)에 의하여 시각화된 공격특성 DNA(323)와 과거 공격특성 DNA(401, 403, 405, 407)를 디스플레이 한다.

[0051] 표시부(140)는 공격특성 DNA(323)를 중간의 abnormal state영역에, 과거 공격특성 DNA(401, 403, 405, 407)를 공격특성 DNA(323) 주변에 표시한다. 디스플레이 되는 위치는 본 예시에 한정되지 아니하고, 다양하게 변할 수 있다.

[0052] DNA 생성부(123)는 공격특성 인자를 가지고 해당하는 과거 공격특성 DNA(401, 403, 405, 407)를 생성한다. DNA 시각화부(125)는 과거 공격특성 DNA(401, 403, 405, 407)를 사용자가 볼 수 있도록 시각화한다. 표시부(140)는 공격유형별 공격특성 DNA(401, 403, 405, 407)를 화면에 디스플레이 한다.

[0053] 공격 유사도 분석부(201)는 공격 유사도를 수치적으로 나타낼 수 있는데, 표시부(140)는 상기 공격 유사도를 비율 또는 예/아니오 등으로 화면에 디스플레이 한다.

[0054] 본 도면에서, 과거 공격특성 DNA(401)는 2009년 7월 7일 DDoS공격에 대한 DNA이고 공격 유사도가 35%이다. 과거 공격특성 DNA(403)는 2013년 6월 25일 APT공격에 대한 DNA이고 공격 유사도가 78%이다. 과거 공격특성 DNA(405)는 2011년 3월 4일 DDoS공격에 대한 DNA이고 공격 유사도가 46%이다. 과거 공격특성 DNA(407)는 2013년 3월 20일 APT공격에 대한 DNA이고 공격 유사도가 96%이다. 사용자는 4개의 과거 공격특성 DNA(401, 403, 405, 407) 중에서, 현재 탐지된 공격의 공격특성 DNA(323)와 가장 유사한 것은 유사도가 96%인 2013년 3월 20일 APT공격인 것을 알 수 있다. 사용자는 과거 공격특성 DNA(407)를 통하여 현재 탐지된 공격을 파악할 수 있고 이

에 대한 대응책을 수립할 수 있다.

[0055] 도 5는 본 발명의 바람직한 일 실시예에 따른 공격특성 DNA 생성 장치의 흐름도를 나타내는 도면이다.

[0056] 도 5를 참조하면, S501단계에서, 정보 처리부(110)는 네트워크, 네트워크 장비, 사용자PC 및 서버 등과 같은 네트워크 구성요소들로부터 이벤트 정보를 수집하여 저장한다.

[0057] S503단계에서, 인자 추출부(121)는 상기 이벤트 정보로부터 정상 인자(310)와 공격특성 인자(320)들을 추출한다.

[0058] S505단계에서, DNA 생성부(123)는 공격특성 인자(320)의 정상 인자(310)와의 연관성을 분석하고, 공격특성 인자(320)와 정상 인자(310)의 결합을 통하여 상기 연관성 분석의 결과를 DNA구조로 나타내는 공격특성 DNA(323)를 생성한다.

[0059] S507단계에서, DNA 생성부(123)는 상기 이벤트 정보 및 공격특성 DNA(323)를 저장부(130)에 저장한다. 이 때, DNA 생성부(123)는 공격특성 DNA(323)를 공격유형별로 분류하여 저장한다.

[0060] S509단계에서, DNA 시각화부(125)는 정상 인자(310), 정상 DNA(313), 공격특성 인자(320), 공격특성 DNA(323) 및 과거 공격특성 DNA(401, 403, 405, 407)를 시각화한다.

[0061] S511단계에서, 표시부(150)는 시각화된 정상 인자(310), 정상 DNA(313), 공격특성 인자(320), 공격특성 DNA(323) 및 과거 공격특성 DNA(401, 403, 405, 407)를 디스플레이 한다.

[0062]

[0063] 도 6은 본 발명의 바람직한 다른 실시예에 따른 공격특성 DNA 분석 장치의 흐름도를 나타내는 도면이다.

[0064] 도 6을 참조하면, 공격특성 DNA 분석 장치(200)가 공격 유사도를 분석하는 방법의 흐름이 도시되어 있다.

[0065] S601단계에서, DNA 생성부(123)는 공격유형별로 분류하여 과거 공격특성 DNA(401, 403, 405, 407)를 저장부(130)에 저장한다.

[0066] S603단계에서, 정보 처리부(110)는 상기 이벤트 정보를 수집한다.

[0067] S605단계에서, 인자 추출부(121)는 상기 이벤트 정보로부터 정상 인자(310)와 공격특성 인자(320)를 추출한다.

[0068] S607단계에서, DNA 생성부(123)는 공격특성 인자의 정상 인자(310)와의 연관성을 분석한 후, 상기 연관성 분석 결과를 DNA 구조로 나타낸 공격특성 DNA(323)를 생성한다.

[0069] S609단계에서, 공격 유사도 분석부(201)는 저장된 공격유형별로 분류된 과거 공격특성 DNA(401, 403, 405, 407)와 공격특성 DNA(323)를 비교하여 유사도를 분석한다. 유사도 분석 결과는 수치적으로 나타내어 질 수

있는데, 바람직하게는, 확률로 나타낼 수 있다.

[0070] S611단계에서, DNA 시각화부(125)는 저장된 공격유형별로 분류된 과거 공격특성 DNA(401, 403, 405, 407)와 공격특성 DNA(323)를 비교분석한 유사도 분석 결과를 시각화한다.

[0071] S613단계에서, 표시부(150)는 상기 유사도 분석 결과를 화면에 디스플레이 한다.

[0072] 상기에서는 본 발명의 실시예를 참조하여 설명하였지만, 해당 기술분야에서 통상의 지식을 가진 자라면 하기의 특허 청구 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0073] 100 : 공격특성 DNA 생성 장치

110 : 정보 처리부

120 : 제어부

121 : 인자 추출부

123 : DNA 생성부

125 : DNA 시각화부

130 : 저장부

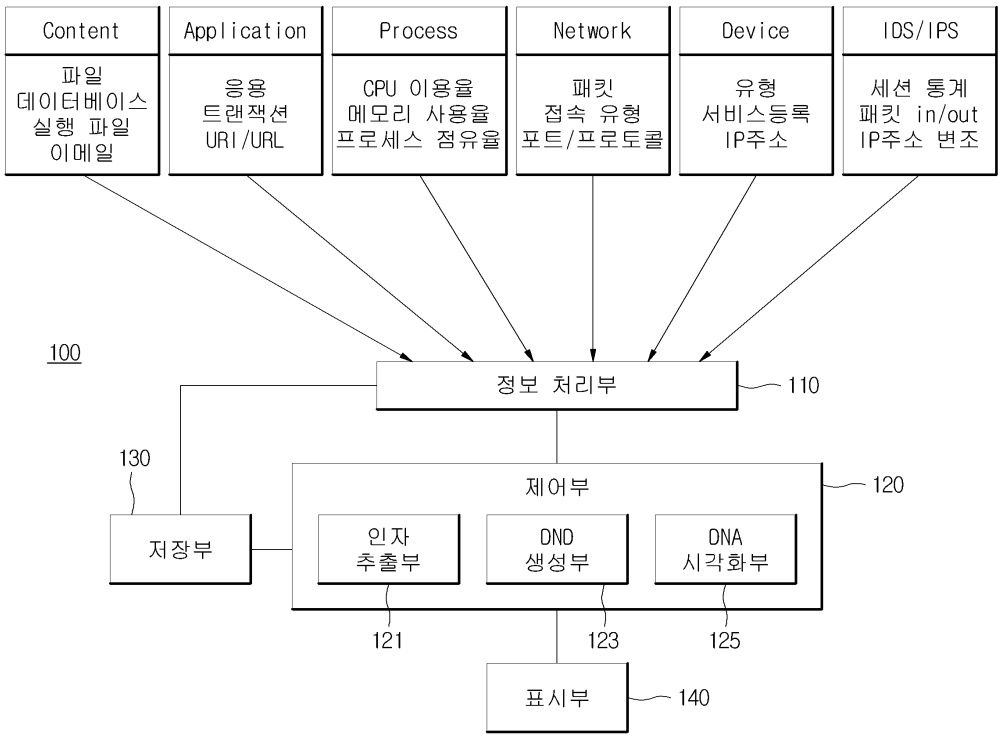
140 : 표시부

200 : 공격특성 DNA 분석 장치

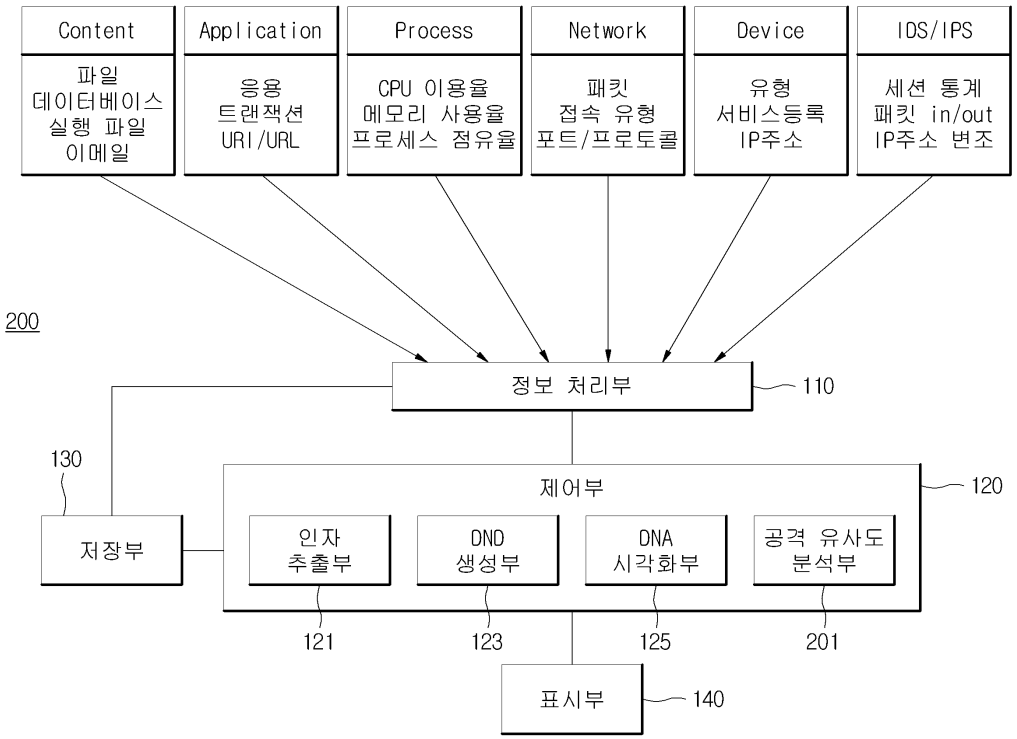
201 : 공격 유사도 분석부

도면

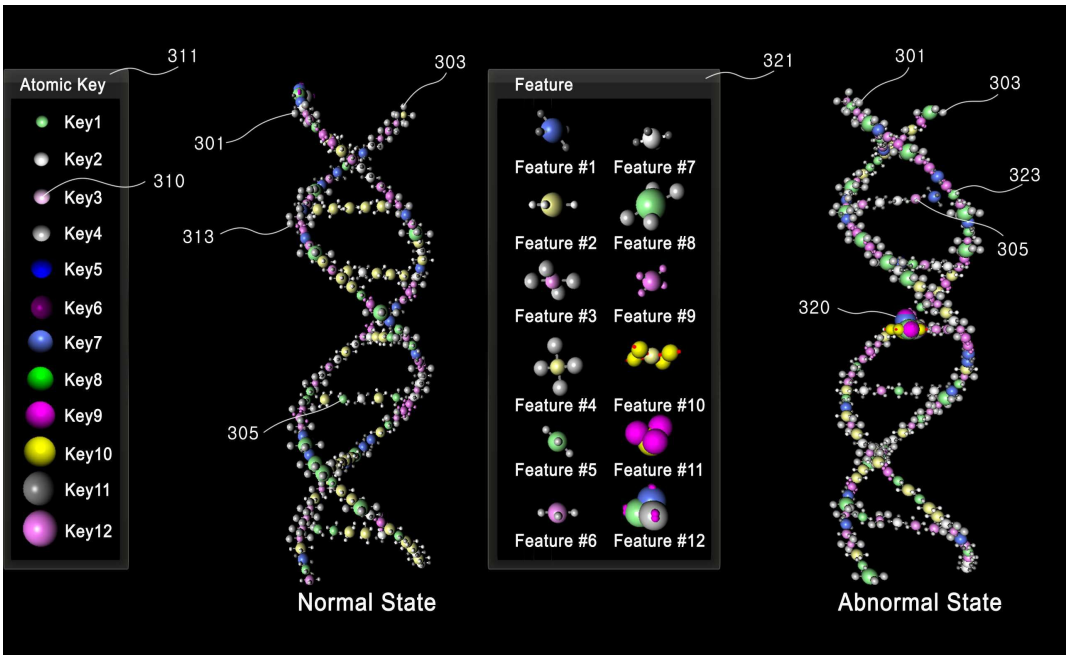
도면1


Content
파일
데이터베이스
실행 파일
이메일
Application
응용
트랜잭션
URI/URL
Process
CPU 이용율
메모리 사용율
프로세스 점유율
Network
패킷
접속 유형
포트/프로토콜
Device
유형
서비스등록
IP주소
IDS/IPS
세션 통계
패킷 in/out
IP주소 변조
100
정보 처리부
110
130
제어부
120
저장부
인자
추출부
DND
생성부
DNA
시각화부
121
123
125
표시부
140

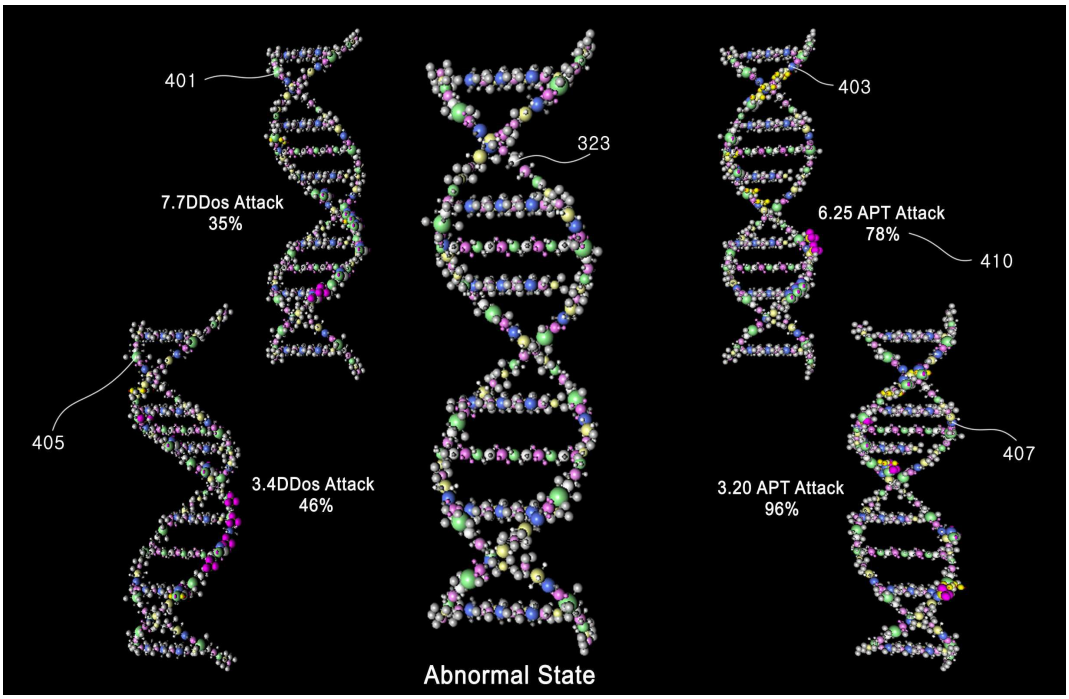
도면2


Content
파일
데이터베이스
실행 파일
이메일
Application
응용
트랜잭션
URI/URL
Process
CPU 이용율
메모리 사용율
프로세스 점유율
Network
패킷
접속 유형
포트/프로토콜
Device
유형
서비스등록
IP주소
IDS/IPS
세션 통계
패킷 in/out
IP주소 변조
200
정보 처리부
110
130
제어부
120
저장부
인자
추출부
DND
생성부
DNA
시각화부
공격 유사도
분석부
121
123
125
201
표시부
140

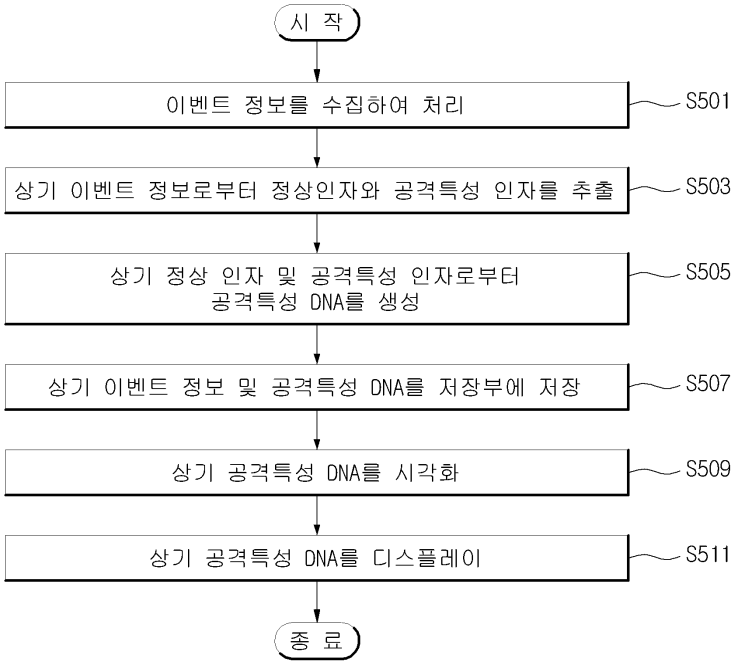
도면3


311
Atomic Key
Key1
Key2
Key3
Key4
Key5
Key6
Key7
Key8
Key9
Key10
Key11
Key12
303
301
310
313
305
Normal State
321
Feature
Feature #1
Feature #7
Feature #2
Feature #8
Feature #3
Feature #9
Feature #4
Feature #10
Feature #5
Feature #11
Feature #6
Feature #12
301
303
323
305
320
Abnormal State

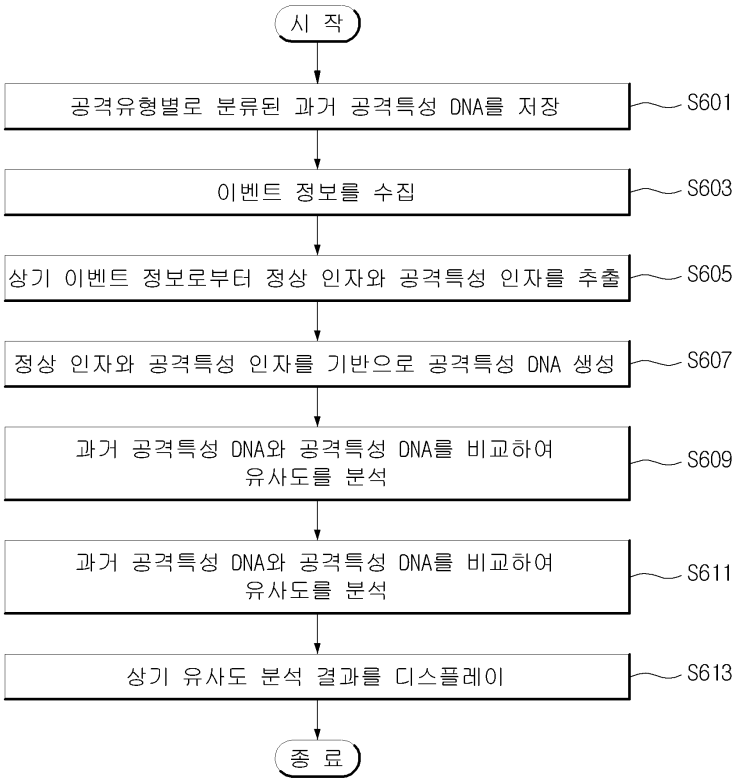
도면4


401
7.7DDos Attack
35%
405
3.4DDos Attack
46%
323
Abnormal State
403
6.25 APT Attack
78%
410
407
3.20 APT Attack
96%

도면5


시 작
이벤트 정보를 수집하여 처리
S501
상기 이벤트 정보로부터 정상인자와 공격특성 인자를 추출
S503
상기 정상 인자 및 공격특성 인자로부터
공격특성 DNA를 생성
S505
상기 이벤트 정보 및 공격특성 DNA를 저장부에 저장
S507
상기 공격특성 DNA를 시각화
S509
상기 공격특성 DNA를 디스플레이
S511
종 료

도면6


시 작
공격유형별로 분류된 과거 공격특성 DNA를 저장
S601
이벤트 정보를 수집
S603
상기 이벤트 정보로부터 정상 인자와 공격특성 인자를 추출
S605
정상 인자와 공격특성 인자를 기반으로 공격특성 DNA 생성
S607
과거 공격특성 DNA와 공격특성 DNA를 비교하여
유사도를 분석
S609
과거 공격특성 DNA와 공격특성 DNA를 비교하여
유사도를 분석
S611
상기 유사도 분석 결과를 디스플레이
S613
종 료