



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0020406
(43) 공개일자 2013년02월27일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) H04L 12/22 (2006.01)
G06F 21/20 (2006.01) H04W 12/00 (2009.01)
(21) 출원번호 10-2011-0083028
(22) 출원일자 2011년08월19일
심사청구일자 2011년08월19일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스
내 (서천동, 경희대학교)
(72) 발명자
이승룡
경기도 성남시 분당구 구미동 삼환빌라 102-102
파루크 아스람 칸
파키스탄 이슬라마바드 지-9/2, 플랫 # 2, 블록 #
68-비
아쉬파크 후사인 파루키
파키스탄 이슬라마바드 지-9/2, 플랫 # 2, 블록 #
68-비
(74) 대리인
특허법인 신지

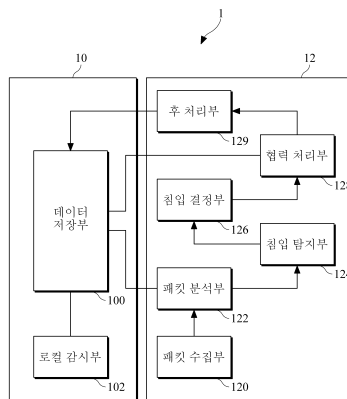
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 무선 센서 네트워크 보호를 위한 침입 탐지 장치 및 그 방법

(57) 요약

무선 센서 네트워크 보호를 위한 침입 탐지 장치 및 그 방법이 개시된다. 본 발명의 일 실시예에 따른 침입 탐지 장치는 내부공격으로부터 센서노드를 보호하기 위해서, 이벤트가 발생하는 온라인 상태에서는 이웃노드 정보와 악성노드 정보를 이용하여 미리 선언된 악성노드로부터 센서노드를 보호하고, 이벤트 발생 후 소정의 시간이 경과한 오프라인 상태에서는 탐지규칙을 규정한 명세에 기초하여 소정의 시간 동안의 침입을 탐지한다.

대표도 - 도1



특허청구의 범위

청구항 1

무선 센서 네트워크의 센서노드에 형성되어 내부공격으로부터 침입을 탐지하는 침입 탐지 장치에 있어서,
이벤트 발생시에 이웃노드 정보와 악성노드 정보를 이용하여, 미리 선언된 악성노드로부터 상기 센서노드를 보호하는 온라인 침입 차단부; 및
상기 이벤트 발생 후 소정의 시간이 경과하면 탐지규칙을 규정한 명세에 기초하여 상기 소정의 시간 동안의 침입을 탐지하고, 이웃노드와 연동하여 침입이 탐지된 대상노드의 악성 여부를 결정하며, 악성 여부 결정결과에 따라 악성노드를 선언하는 오프라인 침입 탐지부;
를 포함하는 것을 특징으로 하는 침입 탐지 장치.

청구항 2

제 1 항에 있어서, 상기 온라인 침입 차단부는,
상기 이웃노드 정보와 악성노드 정보를 저장하는 데이터 저장부; 및
노드 간 송수신되는 패킷을 감시하고, 상기 저장된 이웃노드 정보와 악성노드 정보를 이용하여 소정의 노드에 대한 패킷 수신경로를 확인하여, 상기 소정의 노드가 패킷을 악성노드로부터 수신하거나 이웃노드가 아닌 노드로부터 수신하거나 상기 소정의 노드로 전송되는 패킷이 아니면 해당 패킷을 폐기하는 로컬 감시부;
를 포함하는 것을 특징으로 하는 침입 탐지 장치.

청구항 3

제 1 항 또는 제 2 항에 있어서,
상기 이웃노드 정보는 이웃노드가 악성노드인지 여부를 나타내는 노드 상태정보를 포함하고, 상기 악성노드 정보는 악성노드에 대한 악성등급 정보를 포함하는 것을 특징으로 하는 침입 탐지 장치.

청구항 4

제 1 항에 있어서, 상기 오프라인 침입 탐지부는,
수집 패킷을 분석한 결과인 감시 데이터를 미리 설정된 기준 데이터와 비교하여 비교 결과에 따라 대상노드의 침입을 탐지하는 침입 탐지부;
상기 침입이 탐지된 대상노드의 악성등급을 결정하는 침입 결정부; 및
상기 악성등급 결정 결과 해당 등급이 중간등급인 경우 중간등급을 갖는 대상노드에 대한 상태를 이웃노드들에 요청하여 대상노드 상태정보를 수신하고 이를 반영하여 악성등급을 최종 결정하는 협력 처리부;
를 포함하는 것을 특징으로 하는 침입 탐지 장치.

청구항 5

제 4 항에 있어서,
상기 감시 데이터는 패킷 송신률, 패킷 수신률, 패킷 포워딩률, 패킷 재전송률을 포함하는 패킷 처리율 정보를 포함하는 것을 특징으로 하는 침입 탐지 장치.

청구항 6

제 4 항에 있어서,
상기 기준 데이터는 패킷 송신률, 패킷 수신률, 패킷 포워딩률, 패킷 재전송률을 포함하는 패킷 처리율에 대한 스트레스도 값인 것을 특징으로 하는 침입 탐지 장치.

청구항 7

제 4 항에 있어서, 상기 침입 탐지부는,

대상노드에 대한 감시 데이터와 기준 데이터를 비교하여 결과값인 플래그 데이터를 출력하고,

상기 감시 데이터와 기준 데이터 비교 결과, 감시 데이터 값이 기준 데이터의 최소값(minimum threshold value)보다 작고 대상노드의 침입이 탐지되면 해당 플래그 필드를 N:miN으로 설정하고, 감시 데이터 값이 기준 데이터의 최대값(maximum threshold value)보다 크고 대상노드의 침입이 탐지되면 해당 플래그 필드를 X:maX로 설정하며, 감시 데이터 값이 N과 X 사이에 있거나, 최소값보다 작거나 최대값보다 크지만 대상노드의 침입이 탐지되지 않으면 해당 플래그 필드를 L:normal로 설정하는 것을 특징으로 하는 침입 탐지 장치.

청구항 8

제 7 항에 있어서, 상기 침입 결정부는,

상기 침입 탐지부를 통해 설정된 플래그 필드별 L의 개수 합이 소정의 수보다 적으면 대상노드의 악성등급을 HIGH(상위등급)로 결정하고, 소정의 수에 해당하면 MED(중간등급)으로 결정하며, 소정의 수보다 크면 LOW(하위등급)으로 결정하는 것을 특징으로 하는 침입 탐지 장치.

청구항 9

제 4 항에 있어서, 상기 협력 처리부는,

악성등급이 중간등급을 해당하는 대상노드 리스트를 적어도 하나의 이웃노드들에 제공하고, 상기 이웃노드들로부터 중간등급을 갖는 대상노드 각각에 대한 상태 리스트를 수신하여, 상기 수신된 상태 리스트에 포함된 악성노드 카운트 수를 미리 설정된 기준값과 비교하여 비교 결과에 따라 악성 등급을 상향 또는 하향 조정하는 것을 특징으로 하는 침입 탐지 장치.

청구항 10

제 4 항에 있어서,

상기 협력 처리부를 통해 최종 결정된 악성등급에 따라 이웃노드 정보와 악성노드 정보를 갱신하고 악성노드를 우회하는 새로운 경로를 탐색하며 갱신된 악성노드 정보를 상위단에 통지하는 후처리부;

를 더 포함하는 것을 특징으로 하는 침입 탐지 장치.

청구항 11

무선 센서 네트워크의 센서노드에 형성된 침입 탐지 장치가 내부공격으로부터의 침입을 탐지하는 방법에 있어서,

이벤트 발생시에 이웃노드 정보와 악성노드 정보를 이용하여, 미리 선언된 악성노드로부터 센서노드를 보호하는 온라인 침입 차단 단계; 및

상기 이벤트 발생 후 소정의 시간이 경과하면 탐지규칙을 규정한 명세에 기초하여 상기 소정의 시간 동안의 침입을 탐지하고, 이웃노드와 연동하여 침입이 탐지된 대상노드의 악성 여부를 결정하며, 악성 여부 결정결과에 따라 악성노드를 선언하는 오프라인 침입 탐지 단계;

를 포함하는 것을 특징으로 하는 침입 탐지 방법.

청구항 12

제 11 항에 있어서, 상기 온라인 침입 차단 단계는,

상기 이웃노드 정보와 악성노드 정보를 저장하는 단계; 및

노드 간 송수신되는 패킷을 감시하고, 상기 저장된 이웃노드 정보와 악성노드 정보를 이용하여 소정의 노드에 대한 패킷 수신경로를 확인하여, 상기 소정의 노드가 패킷을 악성노드로부터 수신하거나 이웃노드가 아닌 노드로부터 수신하거나 상기 소정의 노드로 전송되는 패킷이 아니면 해당 패킷을 폐기하는 단계;

를 포함하는 것을 특징으로 하는 침입 탐지 방법.

청구항 13

제 11 항에 있어서, 상기 오프라인 침입 탐지 단계는,

수집 패킷을 분석한 결과인 감시 데이터를 미리 설정된 기준 데이터와 비교하여 비교 결과에 따라 대상노드의 침입을 탐지하는 단계;

상기 침입이 탐지된 대상노드의 악성등급을 결정하는 단계; 및

상기 악성등급 결정 결과 해당 등급이 중간등급인 경우 중간등급을 갖는 대상노드에 대한 상태를 이웃노드들에 요청하여 대상노드 상태정보를 수신하고 이를 반영하여 악성등급을 최종 결정하는 단계;

를 포함하는 것을 특징으로 하는 침입 탐지 방법.

청구항 14

제 13 항에 있어서, 상기 침입을 탐지하는 단계는,

감시 데이터와 기준 데이터를 비교하는 단계; 및

상기 비교 결과값인 플래그 데이터를 출력하는 단계; 를 포함하고,

상기 플래그 데이터를 출력하는 단계는,

감시 데이터 값이 기준 데이터의 최소값(minimum threshold value)보다 작고 대상노드의 침입이 탐지되면 해당 플래그 필드를 N:min으로 설정하고, 감시 데이터 값이 기준 데이터의 최대값(maximum threshold value)보다 크고 대상노드의 침입이 탐지되면 해당 플래그 필드를 X:max로 설정하며, 감시 데이터 값이 N과 X 사이에 있거나, 최소값보다 작거나 최대값보다 크지만 대상노드의 침입이 탐지되지 않으면 해당 플래그 필드를 L:normal로 설정하는 것을 특징으로 하는 침입 탐지 방법.

청구항 15

제 14 항에 있어서, 상기 대상노드의 악성등급을 결정하는 단계는,

플래그 필드별 L의 개수 합이 소정의 수보다 적으면 대상노드의 악성등급을 HIGH(상위등급)로 결정하고, 소정의 수에 해당하면 MED(중간등급)으로 결정하며, 소정의 수보다 크면 LOW(하위등급)으로 결정하는 것을 특징으로 하는 침입 탐지 방법.

청구항 16

제 13 항에 있어서, 상기 악성등급을 최종 결정하는 단계는,

악성등급이 중간등급에 해당하는 대상노드 리스트를 적어도 하나의 이웃노드들에 제공하고, 상기 이웃노드들로부터 중간등급을 갖는 대상노드 각각에 대한 상태 리스트를 수신하여, 상기 수신된 상태 리스트에 포함된 악성노드 카운트 수를 미리 설정된 기준값과 비교하여 비교 결과에 따라 악성 등급을 상향 또는 하향 조정하는 것을 특징으로 하는 침입 탐지 방법.

청구항 17

제 13 항에 있어서,

상기 최종 결정된 악성등급에 따라 이웃노드 정보와 악성노드 정보를 갱신하고 악성노드를 우회하는 새로운 경로를 탐색하며 갱신된 악성노드 정보를 상위단에 통지하는 단계;

를 더 포함하는 것을 특징으로 하는 침입 탐지 방법.

명세서

기술분야

[0001] 본 발명의 일 양상은 보안 기술에 관한 것으로, 보다 상세하게는 무선 센서 네트워크 보호를 위한 내부공격 탐

지 기술에 관한 것이다.

배경 기술

- [0002] 무선 센서 네트워크(Wireless Sensor Network : WSN)는 센서 노드, 센서 노드로부터 수집된 정보를 가공하는 프로세서 및 가공된 정보를 전송하는 무선 송수신 장치로 구성된 네트워크이다. 이는 의사소통뿐만 아니라 자동화된 원격정보 수집이 가능하여 네트워크 내의 센서 노드의 추적, 감시, 제어 등 다양한 응용 개발에 폭넓게 활용되고 있다. 이러한 무선센서 네트워크는 인간 중심의 유비쿼터스 패러다임이 확대되면서 유비쿼터스 센서 네트워크(Ubiquitous sensor network : USN)로 발전하고 있다.
- [0003] 보안은 네트워크 패러다임을 위한 주요한 과제 중 하나다. 무선 네트워크는 무선매체를 사용하고 자원에 대한 애드혹 접근을 제공하기 때문에 유선 네트워크보다 위협에 취약하다. 안전한 무선 센서 네트워크는 전장 감시, 헬스케어, 재해 복구, 환경 모니터링 등의 다양한 애플리케이션을 위한 미래의 수요이다.
- [0004] 선행기술 [A. P. R. Da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and W. C. Wong, "Decentralized Intrusion Detection in wireless sensor networks," in Proc. of the 1st ACM International workshop on Quality of Service & Security in Wireless and Mobile networks, Quebec, Canada, pp. 16-23, 2005]에는 간단한 IDS(Intrusion detection system) 에이전트 프레임워크 기술에 대해 개시하고 있다.
- [0005] 또한, 선행기술 [R. Roman, J. Zhou, and J. Lopez, "Applying Intrusion Detection Systems to wireless sensor networks," in Proc. of 3rd IEEE Consumer Communications and Networking Conference, pp. 640-644, 2006]에는 일반적인 IDS 에이전트 프레임워크 기술에 대해 개시하고 있다.

발명의 내용

해결하려는 과제

- [0006] 일 양상에 따라, 무선 센서 네트워크의 분산 환경에서 내부공격으로부터 센서노드의 침입을 탐지하고 침입을 차단하여 보안율을 높일 수 있는 침입 탐지 장치 및 그 방법을 제안한다.

과제의 해결 수단

- [0007] 일 양상에 따른 무선 센서 네트워크의 센서노드에 형성되어 내부공격으로부터 침입을 탐지하는 침입 탐지 장치는, 이벤트 발생시에 이웃노드 정보와 악성노드 정보를 이용하여, 미리 선언된 악성노드로부터 센서노드를 보호하는 온라인 침입 차단부와, 이벤트 발생 후 소정의 시간이 경과하면 탐지규칙을 규정한 명세에 기초하여 소정의 시간 동안의 침입을 탐지하고, 이웃노드와 연동하여 침입이 탐지된 대상노드의 악성 여부를 결정하며, 악성 여부 결정결과에 따라 악성노드를 선언하는 오프라인 침입 탐지부를 포함한다.
- [0008] 온라인 침입 차단부는, 이웃노드 정보와 악성노드 정보를 저장하는 데이터 저장부와, 노드 간 송수신되는 패킷을 감시하고, 저장된 이웃노드 정보와 악성노드 정보를 이용하여 소정의 노드에 대한 패킷 수신경로를 확인하여, 소정의 노드가 패킷을 악성노드로부터 수신하거나 이웃노드가 아닌 노드로부터 수신하거나 소정의 노드로 전송되는 패킷이 아니면 해당 패킷을 폐기하는 로컬 감시부를 포함한다.
- [0009] 오프라인 침입 탐지부는, 수집 패킷을 분석한 결과인 감시 데이터를 미리 설정된 기준 데이터와 비교하여 비교 결과에 따라 대상노드의 침입을 탐지하는 침입 탐지부와, 침입이 탐지된 대상노드의 악성등급을 결정하는 침입 결정부와, 악성등급 결정 결과 해당 등급이 중간등급인 경우 중간등급을 갖는 대상노드에 대한 상태를 이웃노드들에 요청하여 대상노드 상태정보를 수신하고 이를 반영하여 악성등급을 최종 결정하는 협력 처리부를 포함한다.
- [0010] 다른 양상에 따른 침입 탐지 방법은, 이벤트 발생시에 이웃노드 정보와 악성노드 정보를 이용하여, 미리 선언된 악성노드로부터 센서노드를 보호하는 온라인 침입 차단 단계와, 이벤트 발생 후 소정의 시간이 경과하면 탐지규칙을 규정한 명세에 기초하여 소정의 시간 동안의 침입을 탐지하고, 이웃노드와 연동하여 침입이 탐지된 대상노드의 악성 여부를 결정하며, 악성 여부 결정결과에 따라 악성노드를 선언하는 오프라인 침입 탐지 단계를 포함한다.

발명의 효과

[0011] 일 실시예에 따르면, 침입 탐지 장치는 무선 센서 네트워크의 분산 환경에서 내부공격으로부터 침입을 탐지하고 침입을 차단하여 보안율을 높일 수 있다. 즉, 이벤트가 발생하는 온라인 상태에서는 미리 선언된 악성노드로부터 센서노드를 보호하고, 이벤트 발생 후 소정의 시간이 경과한 오프라인 상태에서는 탐지규칙을 규정한 명세에 기초하여 소정의 시간 동안의 침입을 탐지할 수 있다.

[0012] 나아가, 침입 탐지 장치는 탐지방식(detection schema), 경고 발생, 탐지 결정 및 이웃노드와의 연동을 통한 협업 프로세스를 수행하여 보안율을 높일 수 있다. 나아가 헬스케어, 재해 복구, 환경 모니터링 등의 애플리케이션이 무선 네트워크에서의 처리량 증가를 위하여 메시지의 신뢰성 있는 전송을 처리할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일 실시예에 따른 침입 탐지 장치를 도시한 구성도,
 도 2는 본 발명의 일 실시예에 따른 온라인 침입 차단 방법을 도시한 흐름도,
 도 3은 본 발명의 일 실시예에 따른 오프라인 침입 탐지 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 이하에서는 첨부한 도면을 참조하여 본 발명의 실시예들을 상세히 설명한다. 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0015] 도 1은 본 발명의 일 실시예에 따른 침입 탐지 장치(1)를 도시한 구성도이다.

[0016] 도 1을 참조하면, 침입 탐지 장치(1)는 온라인 침입 차단부(10)와 오프라인 침입 탐지부(12)를 포함한다. 온라인 침입 차단부(10)는 데이터 저장부(100)와 로컬 감시부(102)를 포함한다. 오프라인 침입 탐지부(12)는 패킷 수집부(120), 패킷 분석부(122), 침입 탐지부(124), 침입 결정부(126), 협력 처리부(128) 및 후처리부(129)를 포함한다.

[0017] 침입 탐지 장치(1)는 센서노드에 설치되어, 무선 센서 네트워크 상의 내부 공격(intrusion attack)으로부터 센서노드를 보호한다. 침입 탐지 장치(1)는 분산 환경에서 침입을 탐지하기 위한 탐지 규칙에 따른 명세를 사용하여 내부 공격을 탐지하는 명세 기반 분산 탐지 장치(a specification based distributed detection system : SpecDDS)이다.

[0018] 침입 탐지 장치(1)는 온라인 모드(Online mode)와 오프라인 모드(Offline mode)에서 동작한다. 온라인 모드는 무선 센서 네트워크에서 소정의 이벤트가 발생할 때 수행되는 모드이다. 오프라인 모드는 소정의 이벤트 발생 이후 소정의 시간(next epoch of time)이 경과되면 수행되는 모드이다. 온라인 모드에 있어서 침입 탐지 장치(1)는 이벤트가 발생하면 이웃노드 정보와 악성노드 정보를 이용하여 미리 선언된 악성노드(malicious node declared already)로부터 센서노드를 보호한다. 오프라인 모드에 있어서 침입 탐지 장치(1)는 이벤트 발생 이후 소정의 시간이 경과하면 탐지규칙을 규정한 명세에 기초하여 소정의 시간 동안의 침입을 탐지하고, 이웃노드와 연동하여 침입이 탐지된 대상노드의 악성 여부를 결정하며 악성 여부 결정결과에 따라 악성노드를 선언한다. 침입 탐지 장치(1)는 탐지방식(detection schema), 경고 발생, 탐지 결정 및 이웃노드와의 연동을 통한 협업 프로세스를 수행한다.

[0019] 본 발명에 따르면, 센서노드는 몇 가지 전제조건을 갖는 무선 센서 네트워크에서 동작한다고 가정한다. 우선, 센서 네트워크는 정적(static)이어야만 한다. 둘째, 센서노드는 초기화 단계(initialization phase)인 일정 시간 이후에는 센서 네트워크에 참여할 수 없다. 초기화 단계에서 센서노드는 이웃노드들과 통신하여 토폴로지를 구성하고 싱크노드 또는 베이스스테이션과의 연결경로를 탐색한다. 셋째, 센서노드는 일정 시간 이후에는 경로 탐색을 초기화해야만 한다. 초기화 단계의 일정 시간은 침입 탐지 장치(1)가 동작하는 데 필요한 시간보다 크거나 같아야만 한다.

[0020] 이하 도 1을 참조로 하여, 침입 탐지 장치(1)의 세부 구성에 대해 상세히 후술한다.

[0021] 데이터 저장부(data repository)(100)에는 이웃노드 정보(a list of neighboring node: N_list)와 악성노드 정보(a list of malicious nodes: N_list)가 저장된다. 이웃노드 정보는 이웃노드가 악성노드인지 여부를 나타내

는 노드 상태정보를 포함한다. 악성노드 정보는 악성노드의 악성정도를 나타내는 악성등급 정보를 포함한다.

[0022] 모든 센서노드는 네트워크에 참여하거나 탈퇴한다. 따라서, 참여 또는 탈퇴시마다 이웃노드 정보(N_list)는 갱신되어야 한다. 이웃노드 정보(N_list)는 이웃노드 식별자인 neighbor node ID 필드와, 대상노드로부터 마지막으로 수신한 패킷의 타임스탬프 값인 Time_Stamp 필드와, 대상노드가 악성노드(M)인지 정상노드(N)인지 여부를 표시하는 Status 필드를 포함한다 (표 1 참조).

표 1

[0023]

Node_ID	Time Stamp	Status (Normal or Mal.)
X	X_New	N or M

[0024] 악성노드 정보(N_list)는 악성노드 식별자인 malicious node ID 필드와 악성노드 등급(maliciousness level) 필드를 포함한다 (표 2 참조).

표 2

[0025]

Node_ID	Status
Y	Mal_Level

[0026] 로컬 감시부(Local Auditing Unit)(102)는 노드 간 전송되는 패킷을 감시하고, 데이터 저장부(100)에 저장된 이웃노드 정보와 악성노드 정보를 이용하여 소정의 노드에 대한 패킷 수신경로를 확인한다. 그리고, 소정의 노드가 패킷을 악성노드로부터 수신하거나 이웃노드가 아닌 노드로부터 수신하거나 소정의 노드로 전송되는 패킷이 아니면 해당 패킷을 폐기한다. 이에 비해, 소정의 노드가 패킷을 악성노드가 아닌 이웃노드로부터 수신한 경우 패킷 관련 정상적인 동작을 수행하도록 한다. 정상적인 동작 수행은 센서노드의 구성과 애플리케이션에 따라 결정된다. 전술한 로컬 감시 동작에 대한 프로그램 알고리즘은 표 3과 같다.

표 3

[0027]

Algorithm : Local Auditing at node X

Input: Packets from other nodes

Output: Validation of packet (discard or accepted)

begin

if received packet is destined for node X

if it is from neighbor (Tally N_List)

if neighbor is not malicious

 accept it for further processing

else

 discard it

end if

else

 discard it

end if

else

 discard it

end if

end

[0028] 로컬 감시부(102)는 프로미스큐어스 모드(promiscuous listening mode)에서 동작한다. 프로미스큐어스 모드는 노드 간 전송되는 모든 패킷을 인터셉트하여 이를 관측하는 모드이며, 로컬 감시부(102)는 관측 결과에 따라 해당 패킷이 안전한 이웃노드로부터 전송된 것인지를 확인한다.

[0029] 한편, 오프라인 침입 탐지부(12)는 패킷 수집부(120), 패킷 분석부(122), 침입 탐지부(124), 침입 결정부(126), 협력 처리부(128) 및 후처리부(129)를 포함한다.

[0030] 패킷 수집부(120)는 노드 간 전송되는 패킷을 수집한다. 패킷 수집부(120) 역시 로컬 감시부(102)처럼 프로미스큐어스 모드에서 동작한다. 패킷 수집부(120)는 수집한 패킷을 패킷 분석부(122)에 제공한다.

[0031] 패킷 분석부(122)는 패킷 수집부(120)로부터 제공받은 수집 패킷의 헤더를 관측하여 감시 데이터(Audit Data List:A_list)를 생성한다. 감시 데이터는 패킷 송신 필드, 패킷 수신 필드, 패킷 포워딩 필드 및 패킷 재전송 필드를 포함하는 패킷 처리에 정보를 포함한다 (표 4 참조). 감시 데이터(A_list)는 후술할 침입 탐지부(124)의 침입 탐지 결정을 위해 사용된다.

표 4

Node_ID	Packet Sent (A_snt)	Packet Received (A_rec)	Packet Forward (A_fwd)	Packet Retransmit (A_rtm)
X	X1	X2	X3	X4
Y	Y1	Y2	Y3	Y4

[0033] 표 4를 참조하여 감시 데이터(A_list)의 예를 들면, node A가 node X에서 node Y로 전송되는 패킷을 수집한 경우라고 가정할 때, node A는 수집 패킷의 헤더를 관측하여, A_list에서 node X와 node Y의 송신 필드(A_snt) 및 수신 필드(A_rec)를 갱신한다. node Y가 일정시간 동안 해당 패킷을 포워딩하지 않는다면, node X는 동일한 패킷을 재전송할 수 있다. 이때, node A는 A_list에서 node X의 재전송 필드(A_rtm)와 node Y의 수신 필드(A_rec)를 갱신한다. node Y가 node X로부터 수신한 패킷을 포워딩하는 경우라면, node A는 A_list에서 node Y의 포워딩 필드(A_fwd)를 갱신한다.

[0034] 침입 탐지부(124)는 감시 데이터(A_list)를 기준 데이터(Threshold list:T_list)와 비교하여 비교 결과에 따라 대상노드의 침입을 탐지한다. 결과값은 플래그 리스트(Flag list:F_list) 형태로 출력된다. 플래그 리스트(F_list)의 구조는 감시 데이터(A_list)와 유사하되, 각 플래그 필드가 포함된다 (표 5 참조).

표 5

Node_ID	F_snt	F_rec	F_fwd	F_rtm
XY	N X L	N X L	N X L	N X L

[0036] 표 5를 참조하면, 침입 탐지부(124)는 대상노드 별로 감시 데이터와 기준 데이터의 비교 결과, 감시 데이터 값이 기준 데이터의 최소값(minimum threshold value)보다 작고 대상노드의 침입이 탐지되면 해당 플래그 필드를 'N:min'으로 설정하고, 감시 데이터 값이 기준 데이터의 최대값(maximum threshold value)보다 크고 대상노드의 침입이 탐지되면 해당 플래그 필드를 'X:max'로 설정한다. 이에 비해, 감시 데이터 값이 N과 X 사이에 있거나, 최소값보다 작거나 최대값보다 크지만 대상노드의 침입이 탐지되지 않으면 해당 플래그 필드를 L:normal로 설정한다 (표 6 참조).

표 6

[0037]

A. N:min:
if value is less than the minimum threshold value and shows any attack pattern

B. X:max:
if value is greater than the maximum threshold value and shows any attack pattern

C. L:normal:
if value is between N and X or less/ greater than threshold value but does not show any attack pattern

[0038]

기준 데이터(T_list)는 패킷 송신률, 패킷 수신률, 패킷 포워딩률, 패킷 재전송률을 포함하는 패킷 처리율에 대한 스트레스홀드 값을 포함한다. 스트레스홀드 값은 네트워크 상의 모든 노드들의 평균값 또는 시뮬레이션 결과값으로부터 도출될 수 있으나 이에 한정되지는 않는다(표 7 참조).

표 7

[0039]

Node_ID	N_Snt	X_Snt	N_Rec	X_Rec	N_Fwd	X_Fwd	N_Rtm	X_Rtm
X	X_nSnt	X_xSnt	X_nRec	X_xRec	X_nFwd	X_xFwd	X_nRtm	X_xRtm

[0040]

침입 탐지부(124)가 대상노드의 침입 탐지 동작에 대한 프로그램 알고리즘은 표 8과 같다. 이때, 입력값은 A_list와 T_list이고, 출력값은 F_list이다.

표 8

[0041]

```

Algorithm : Detection Policy

Input: Audit Data List (A_List), Threshold List (T_List)
Output: Flag List (F_List)
begin
  Case I: (Packet Sent)
    If Node_ID.A_snt < Node_ID.N_Snt
      Node_ID.F_snt == N
    Else If Node_ID.A_snt > Node_ID.X_Snt
      Node_ID.F_snt == X
    Else
      Node_ID.F_snt == L
    End If
  Case II: (Packet Receive)
    If Node_ID.A_rec < Node_ID.N_Rec
      Node_ID.F_rec == L
    Else If Node_ID.A_rec > Node_ID.X_Rec
      Node_ID.F_rec == X
    Else
      Node_ID.F_rec == L
    End If
  Case III: (Packet Forward)
    If Node_ID.A_fwd < Node_ID.N_Fwd
      Node_ID.F_fwd == N
    Else If Node_ID.A_fwd > Node_ID.X_Fwd
      Node_ID.F_fwd == L
    Else
      Node_ID.F_fwd == L
    End If
  Case IV: (Packet Retransmit)
    If Node_ID.A_rtm < Node_ID.N_Rtm
      Node_ID.F_rtm == L
    Else If Node_ID.A_rtm > Node_ID.X_Rtm
      Node_ID.F_rtm == X
    Else
      Node_ID.F_rtm == L
    End If
end

```

[0042]

일 실시예에 따르면, 침입 탐지부(124)는 감시 데이터와 기준 데이터의 패킷 송신률 비교 결과, 대상노드로부터의 송신 패킷의 감시 데이터 값이 기준 데이터의 최대값보다 크면 플로딩 공격 또는 라우팅 공격에 의해 훼손된 노드로부터 송신된 패킷으로 판단한다(표 9 참조).

표 9

[0043]

Case I (Sending rate analysis)

- A. Less than miN : Node might be damaged or exhausted.
- B. More than maX : Flooding attack or any other routing attack that compromises the node to send many packets.

[0044]

일 실시예에 따르면, 침입 탐지부(124)는 감시 데이터와 기준 데이터의 패킷 수신률 비교 결과, 대상노드로의 수신 패킷의 감시 데이터 값이 기준 데이터의 최대값보다 크면 트랜스포트 공격 또는 라우팅 공격에 의해 훼손된 노드로부터 수신된 패킷으로 판단한다(표 10 참조).

표 10

[0045]

Case II (Receiving rate analysis)

- A. Less than miN : Not affected. It might be due to other compromise node.
- B. More than maX : Transport or routing attack; collision, flooding, worm-hole, sink-hole, black-hole, selective forwarding attack

[0046]

일 실시예에 따르면, 침입 탐지부(124)는 감시 데이터와 기준 데이터의 패킷 포워딩률 비교 결과, 대상노드로의 포워딩 패킷의 감시 데이터 값이 기준 데이터의 최소값보다 작으면 라우팅 공격에 의해 훼손된 노드로부터 포워딩된 패킷으로 판단한다(표 11 참조).

표 11

[0047]

Case III (Forward rate analysis)

- A. Less than miN : routing attack (node compromised with homing, selective forwarding or black-hole attack)
- B. More than maX : Not affected. It might be due to other compromise node.

[0048]

일 실시예에 따르면, 침입 탐지부(124)는 감시 데이터와 기준 데이터의 패킷 재전송률 비교 결과, 대상노드로의 재전송 패킷의 감시 데이터값이 기준 데이터의 최대값보다 크면 충돌 공격에 의해 훼손된 노드로부터 재전송된 패킷으로 판단한다(표 12 참조).

표 12

[0049]

Case IV (Retransmission rate analysis)

- A. Less than miN : Not affected. It might be due to other compromise node.
- B. More than maX : Collision attack.

[0050]

침입 결정부(126)는 침입이 탐지된 대상노드의 악성등급을 결정한다. 침입 결정부(126)는 악성등급(Maliciousness Level) 결정을 위해 침입 탐지부(124)에서 출력된 F_list를 이용할 수 있다. 일 실시예에 따르면, F_list의 플래그별 L의 총 갯수를 미리 설정된 값과 비교하여 비교결과에 따라 악성등급을

HIGH(상위등급), MEDIUM(중간등급) 또는 LOW(하위등급)로 결정한다. 예를 들면, 비교결과 L의 총갯수가 2보다 적거나 같으면 악성등급을 HIGH로 결정하고, L의 총갯수가 3이면 악성등급을 MEDIUM으로 결정한다. 그리고, 전술한 조건에 해당하지 않는 경우는 악성등급을 LOW로 설정한다. 대상노드별 악성등급 리스트(Maliciousness Level List:ML_list)는 표 13과 같다.

표 13

[0051]

Node_ID	Maliciousness Level
X	HIG
Y	MED
Z	LOW

[0052]

협력 처리부(128)는 침입 결정부(126)를 통한 악성등급 결정 결과 해당등급이 중간등급(MEDIUM)인 경우, 중간등급을 갖는 대상노드에 대한 상태를 이웃노드에 요청(inquiry)하여 대상노드 상태정보를 수신하고 이를 반영하여 악성등급을 최종 결정한다.

[0053]

이상적으로는 센서노드가 이웃노드의 도움없이 스스로 악성등급을 결정하는 것이 바람직하겠지만, 이는 현실적으로 불가능하다. 따라서, 본 발명의 협력 처리부(128)는 센서노드의 이웃노드들과 협업하여 대상노드의 악성등급을 최종 결정한다. 이를 위해 협력 처리부(128)는 의견합의 단계(Consensus Phase)와 인증단계(validation Phase)를 수행한다.

[0054]

의견합의 단계(Consensus Phase)에서, 협력 처리부(128)는 중간등급을 갖는 대상노드 리스트(Claim list:C_list)를 적어도 하나의 이웃노드들에 제공한다. 일 실시예에 따르면, 모든 이웃노드들(n)에게 제공하는 것이 아니라, n/2에 해당하는 이웃노드들에게만 C_list를 제공한다. 그리고, 협력 처리부(128)는 n/2에 해당하는 이웃노드들로부터 중간등급을 갖는 대상노드 각각에 대한 상태 리스트(Intital Status List:S_list)를 수신한다. 상태 리스트(S_list)는 표 14와 같다.

표 14

[0055]

Malicious Node Node_ID	Number of Claims N_Claim
D	1
M	1

[0056]

표 14를 참조하면, 상태 리스트(S_list)는 악성노드의 식별자인 Malicious Node_ID 필드와 악성노드의 상태정보인 N_Claim 필드를 포함한다. N_Claim 필드는 1로 설정된다. 전술한 의견 합의 단계(Consensus Phase)에 대한 프로그램 알고리즘은 표 15와 같다.

표 15

[0057]

```

Algorithm : Consensus Phase

Input: Maliciousness level list (ML_List) => Claim List (C_List)
Output: Status List (S_List)
begin
  for i=1 to (n.N_List) / 2
    // n.N_List = Total number of Neighbors
    if rand(Node_ID.N_List) is Normal
      F1 →send C_List (rand(Node_ID.N_List))
    else
      decrement i
    end if
  end for
  F2 →receive S_List
  F3 →update S_List
end

```

[0058] 표 15를 참조하면, F1, F2 및 F3는 각각 함수(function)를 의미한다. 의견합의 단계(Consensus Phase) 동안에, 협력 처리부(128)는 다른 이웃노드들로부터 S_list를 수신하면 자신의 S_list를 갱신한다. 그리고, 이웃노드들에게 제공한 C_list에 대한 응답으로 S_list를 포함하는 메시지를 수신할 때마다 해당 노드들에 대한 악성노드 카운트 수(N_Claim)를 증가시킨다.

[0059] 이어서, 인증단계(validation Phase)에서 협력 처리부(128)는 이웃노드들로부터 수신된 상태 리스트(S_list)에 포함된 악성노드 카운트 수(N_Claim)를 미리 설정된 기준값과 비교하여 비교 결과에 따라 악성 등급을 상향 또는 하향 조정한다. 예를 들면, N_Claim이 기준값보다 크면 악성등급을 HIGH로 설정하고 대상노드를 악성노드로 선언한다. 이에 비해 N_Claim이 기준값보다 작으면 악성등급을 LOW로 설정한다.

[0060] 후처리부(129)는 협력 처리부(128)에서 최종 결정된 악성등급에 따라 데이터 저장부(100)의 이웃노드 정보와 악성노드 정보를 갱신한다. 일 실시예에 따르면, 대상노드가 악성등급이 HIGH이고 이웃노드인 경우는 데이터 저장부(100)의 이웃노드 정보와 악성노드 정보가 모두 갱신되고, 대상노드는 악성노드에 해당된다. 이에 비해, 대상노드의 악성등급이 HIGH이지만 이웃노드가 아닌 경우는 악성노드 정보가 갱신되고, 대상노드는 경계해야 할 노드에 해당된다. 또한, 후처리부(129)는 악성노드를 우회하는 새로운 경로를 탐색하며 갱신된 악성노드 정보를 상위단인 싱크노드 또는 베이스스테이션에 통지한다. 싱크노드는 센서노드를 통해 감지된 정보를 전송받아 이를 라우팅하고, 베이스스테이션을 통하여 광대역 통신 네트워크로 전송하는 역할을 한다.

[0061] 도 2는 본 발명의 일 실시예에 따른 온라인 침입 차단 방법을 도시한 흐름도이다.

[0062] 도 1 및 도 2를 참조하면, 침입 탐지 장치(1)는 온라인 상태에서 이벤트 발생시에 이웃노드 정보와 악성노드 정보를 이용하여, 미리 선언된 악성노드로부터 센서노드를 보호한다.

[0063] 구체적으로, 침입 탐지 장치(1)는 이웃노드 정보와 악성노드 정보를 저장한다(200). 이웃노드 정보는 이웃노드가 악성노드인지 여부를 나타내는 노드 상태정보를 포함한다. 악성노드 정보는 악성노드에 대한 악성등급 정보를 포함한다.

[0064] 이어서, 침입 탐지 장치(1)는 노드 간 송수신되는 패킷을 감시(210)하고, 저장된 이웃노드 정보와 악성노드 정보를 이용하여 소정의 노드에 대한 패킷 수신경로를 확인한다(220).

[0065] 확인 결과(230), 패킷이 소정의 노드가 패킷을 악성노드로부터 수신하거나 이웃노드가 아닌 노드로부터 수신하거나 소정의 노드로 전송되는 패킷이 아니면 해당 패킷을 폐기한다(240). 이에 비해, 소정의 노드가 패킷을 악성노드가 아닌 이웃노드로부터 수신한 경우 패킷 관련 정상적인 동작을 수행하도록 한다(250). 정상적인 동작 수행은 센서노드의 구성과 애플리케이션에 따라 결정된다.

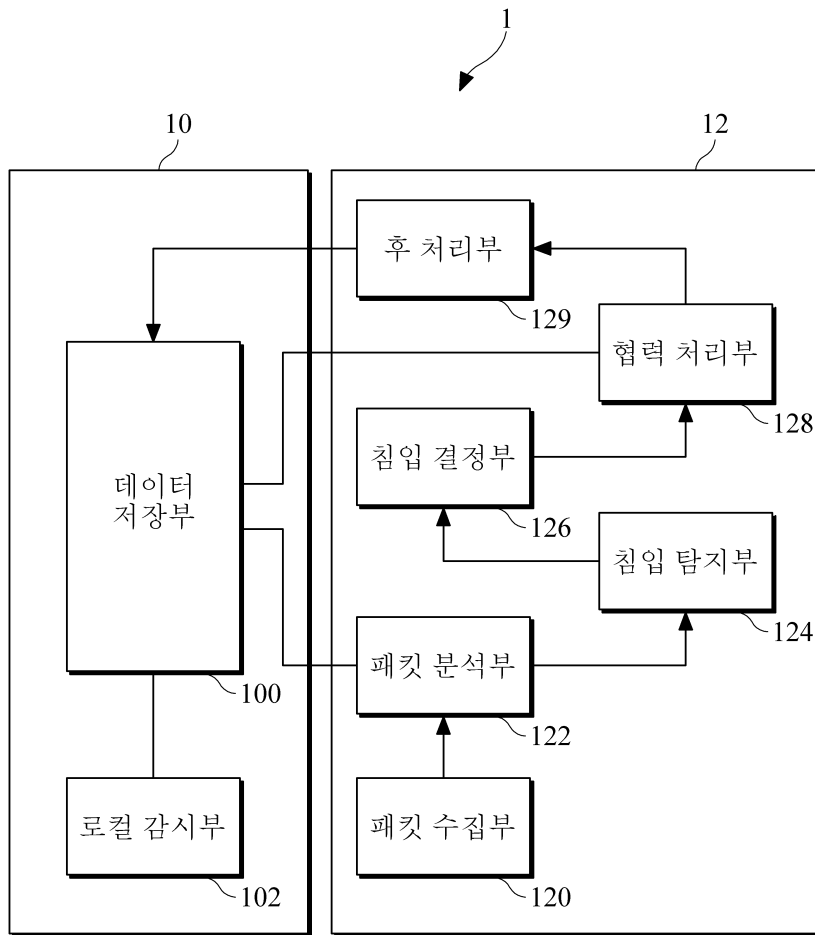
- [0066] 도 3은 본 발명의 일 실시예에 따른 오프라인 침입 탐지 방법을 도시한 흐름도이다.
- [0067] 도 1 및 도 3을 참조하면, 침입 탐지 장치(1)는 온라인 상태의 이벤트 발생 후 소정의 시간이 경과하면 탐지규칙을 규정한 명세에 기초하여 소정의 시간 동안의 침입을 탐지하고, 이웃노드와 연동하여 침입이 탐지된 대상노드의 악성 여부를 결정한다. 그리고, 악성 여부 결정결과에 따라 악성노드를 선언한다.
- [0068] 구체적으로, 오프라인 침입 탐지 단계에서 침입 탐지 장치(1)는 노드 간 전송되는 패킷을 수집한다(300). 이때, 침입 탐지 장치(1)는 프로미스큐어스 모드에서 동작한다. 이어서, 침입 탐지 장치(1)는 수집 패킷의 헤더를 판독하여 감시 데이터(Audit Data List:A_list)를 생성한다(310). 감시 데이터는 패킷 송신률 필드, 패킷 수신률 필드, 패킷 포워딩률 필드 및 패킷 재전송률 필드를 포함하는 패킷 처리율 정보를 포함한다. 기준 데이터는 패킷 송신률, 패킷 수신률, 패킷 포워딩률, 패킷 재전송률을 포함하는 패킷 처리율에 대한 스트레스홀드 값을 포함한다.
- [0069] 이어서, 침입 탐지 장치(1)는 감시 데이터를 기준 데이터와 비교하여 비교 결과에 따라 대상노드의 침입을 탐지한다(320). 일 실시예에 따르면, 침입을 탐지하는 단계(320)에서, 침입 탐지 장치(1)는 감시 데이터와 기준 데이터를 비교하고, 비교 결과값인 플래그 데이터를 출력한다.
- [0070] 침입 탐지 장치(1)는 플래그 데이터를 출력하는 단계에서, 감시 데이터 값이 기준 데이터의 최소값(minimum threshold value)보다 작고 대상노드의 침입이 탐지되면 해당 플래그 필드를 N:minN으로 설정한다. 감시 데이터 값이 기준 데이터의 최대값(maximum threshold value)보다 크고 대상노드의 침입이 탐지되면 해당 플래그 필드를 X:maxX로 설정한다. 감시 데이터 값이 N과 X 사이에 있거나, 최소값보다 작거나 최대값보다 크지만 대상노드의 침입이 탐지되지 않으면 해당 플래그 필드를 L:normal로 설정한다.
- [0071] 이어서, 침입 탐지 장치(1)는 침입이 탐지된 대상노드의 악성등급을 결정한다(330). 일 실시예에 따르면, 대상노드 침입 탐지 단계(320)에서 출력된 플래그 리스트의 플래그 필드별 L의 개수 합이 소정의 수보다 적으면 대상노드의 악성등급을 HIGH(상위등급)로 결정한다. 소정의 수에 해당하면 MED(중간등급)으로 결정한다. 이에 비해 소정의 수보다 크면 LOW(하위등급)으로 결정한다.
- [0072] 이어서, 침입 탐지 장치(1)는 악성등급 결정 결과, 해당 등급이 중간등급인 경우 중간등급을 갖는 대상노드에 대한 상태를 이웃노드들에 요청하여 대상노드 상태정보를 수신하고 이를 반영하여 악성등급을 최종 결정한다(340). 일 실시예에 따르면, 침입 탐지 장치(1)는 악성등급이 중간등급에 해당하는 대상노드 리스트를 적어도 하나의 이웃노드들에 제공하고, 이웃노드들로부터 중간등급을 갖는 대상노드 각각에 대한 상태 리스트를 수신한다. 그리고, 수신된 상태 리스트에 포함된 악성노드 카운트 수를 미리 설정된 기준값과 비교하여 비교 결과에 따라 악성 등급을 상향 또는 하향 조정한다.
- [0073] 추가 양상에 따르면, 오프라인 침입 탐지 단계는 후처리 단계(350)를 포함한다. 후처리 단계(350)에서 침입 탐지 장치(1)는 최종 결정된 악성등급에 따라 이웃노드 정보와 악성노드 정보를 갱신하고 악성노드를 우회하는 새로운 경로를 탐색하며 갱신된 악성노드 정보를 상위단에 통지한다.
- [0074] 이제까지 본 발명에 대하여 그 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

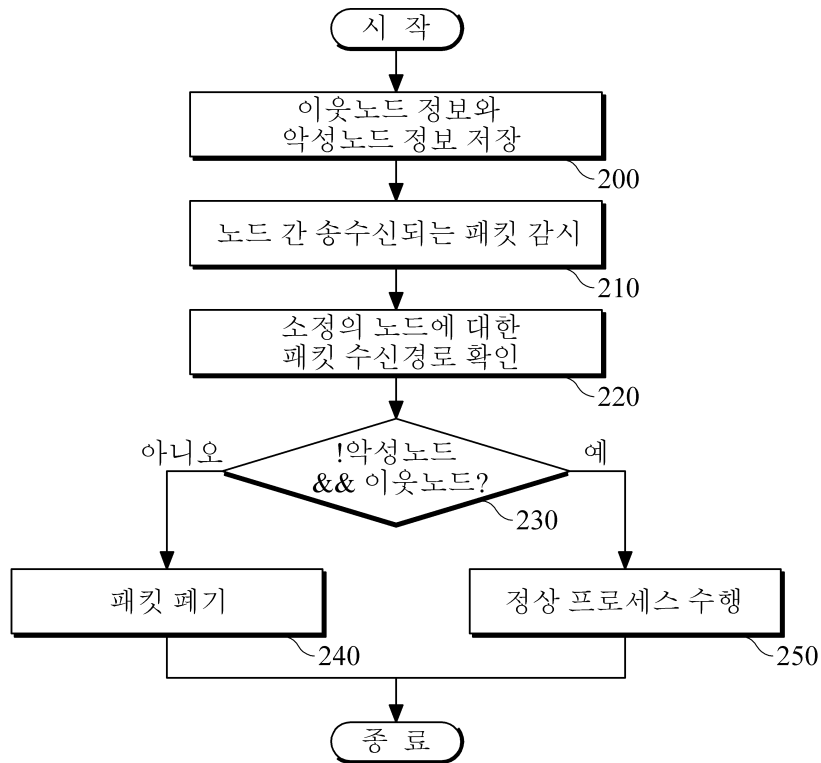
- | | | |
|--------|------------------|-----------------|
| [0075] | 1 : 침입 탐지 장치 | 10 : 온라인 침입 차단부 |
| | 12 : 오프라인 침입 탐지부 | 100 : 데이터 저장부 |
| | 102 : 로컬 감시부 | 120 : 패킷 수집부 |
| | 122 : 패킷 분석부 | 124 : 침입 탐지부 |
| | 126 : 침입 결정부 | 128 : 협력 처리부 |
| | 129 : 후처리부 | |

도면

도면1



도면2



도면3

