



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년02월13일
(11) 등록번호 10-1232918
(24) 등록일자 2013년02월06일

(51) 국제특허분류(Int. Cl.)

H04L 12/22 (2006.01) H04L 12/26 (2006.01)

H04W 84/18 (2009.01) G06F 21/20 (2006.01)

(21) 출원번호 10-2011-0077051

(22) 출원일자 2011년08월02일

심사청구일자 2011년08월02일

(56) 선행기술조사문헌

KR1020090065306 A*

KR1020090102001 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스
내 (서천동, 경희대학교)

(72) 발명자

홍충선

경기도 용인시 수지구 상현로 30-10, 성원3차 상
페빌아파트 233동 101호 (상현동)

조웅준

경기도 수원시 영통구 청명로59번길 54, 103호 (영
통동)

(74) 대리인

서재승

전체 청구항 수 : 총 5 항

심사관 : 양찬호

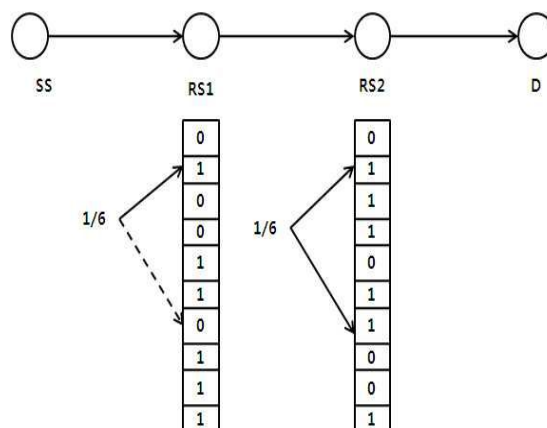
(54) 발명의 명칭 분산 공격 탐지 기능을 구비한 무선 센서 네트워크

(57) 요약

무선 센서 네트워크의 공격 탐지 시스템(Intrusion Detection System, IDS)에 관한 것으로, 보다 구체적으로 무선 센서 네트워크에 분포되어 있는 센서 노드들은 애드-혹(ad-hoc) 방식으로 데이터를 송수신하며 복수의 서로 다른 종류의 공격 유형 데이터 중 어느 하나를 저장하고 있어 공격 패턴을 탐지시 공격 유형을 확인하기 위하여 싱크 노드로 공격 패턴을 송수신할 필요가 없어 공격 패턴 송수신에 따른 에너지 소실을 줄이며 오탐(false positive) 공격을 방지할 수 있는 무선 센서 네트워크에 관한 것이다.

본 발명에 따른 무선 센서 네트워크는 센서 노드에 구비되어 있는 블룸필터부에서 공격 패턴으로 판단되는 서명 코드를 싱크 노드로 송신하지 않고 직접 센서 노드에서 오탐 패턴 또는 공격 유형을 판단함으로써, 서명 코드 송신에 따른 에너지 낭비를 방지할 수 있다. 또한 본 발명에 따른 무선 센서 네트워크는 센서 노드에서 공격 패턴으로 판단된 서명 코드가 오탐 패턴인지를 직접 공격 유형 데이터베이스부를 통해 센서 노드에서 판단함으로써, 오탐 패턴을 이용한 제3자의 악의적인 공격을 방지할 수 있다.

대표도 - 도4



이 발명을 지원한 국가연구개발사업

과제고유번호	NIPA-2011-C1090-1131-0005
부처명	지식경제부
연구사업명	대학 IT 연구센터 육성사업
연구과제명	해킹/바이러스 대응 기술 연구
주관기관	충남대학교
연구기간	2011.01.01 ~ 2011.12.31

특허청구의 범위

청구항 1

다수의 센서 노드가 분포되어 있는 무선 센서 네트워크에 있어서,

상기 센서 노드는

수신한 공격 데이터를 복수의 해쉬 함수에 적용하여 각 해쉬 함수에 상응하는 해쉬 함수값으로 서명 코드를 생성하는 서명 코드 생성부와, 공격 패턴 데이터를 저장하고 있는 블룸필터 저장부와, 상기 생성한 서명 코드와 상기 공격 패턴 데이터를 비교하여 상기 생성한 서명 코드가 공격 패턴인지 판단하는 공격 패턴 판단부를 구비하는 블룸 필터부;

공격 패턴의 서명 코드에 해당하는 공격 유형 데이터를 저장하고 있는 공격 유형 데이터베이스부; 및

상기 서명 코드가 공격 패턴으로 판단되는 경우 상기 공격 패턴의 서명 코드에 해당하는 공격 유형을 상기 공격 유형 데이터베이스부에서 검색하는 검색부를 포함하는 것을 특징으로 하는 무선 센서 네트워크.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

상기 무선 센서 네트워크에 분포되어 있는 상기 센서 노드의 블룸필터 저장부에는 복수의 서로 다른 유형의 공격 패턴 데이터 중 어느 하나가 저장되어 있으며,

상기 센서 노드의 공격 유형 데이터베이스에는 상기 센서 노드의 블룸필터 저장부에 저장되어 있는 공격 패턴 데이터를 통해 탐지할 수 있는 공격 패턴 서명 코드의 공격 유형 데이터베이스가 저장되어 있는 것을 특징으로 하는 무선 센서 네트워크.

청구항 4

제 3 항에 있어서,

상기 공격 패턴의 서명 코드는 서로 다른 등급으로 분류되어 있으며,

상위 등급으로 분류된 공격 패턴의 서명 코드는 하위 등급으로 분류된 공격 패턴의 서명 코드보다 상기 복수의 서로 다른 유형의 공격 패턴 데이터에 더 많이 중복되어 설정 저장되어 있는 것을 특징으로 하는 무선 센서 네트워크.

청구항 5

제 1 항, 제 3 항 및 제 4 항 중 어느 한 항에 있어서,

상기 무선 센서 네트워크에 분포되어 있는 다수의 센서 노드들은 애드-혹(ad-hoc) 방식으로 데이터를 송수신하는 것을 특징으로 하는 무선 센서 네트워크.

청구항 6

다수의 센서 노드가 분포되어 있는 애드-혹(ad-hoc) 무선 센서 네트워크의 상기 센서 노드에 있어서,

수신한 공격 데이터를 복수의 해쉬 함수에 적용하여 각 해쉬 함수에 상응하는 해쉬 함수값으로 서명 코드를 생성하는 서명 코드 생성부와, 공격 패턴 데이터를 저장하고 있는 블룸필터 저장부와, 상기 생성한 서명 코드와 상기 공격 패턴 데이터를 비교하여 상기 생성한 서명 코드가 공격 패턴인지 판단하는 공격 패턴 판단부를 구비하는 블룸 필터부;

공격 패턴의 서명 코드에 해당하는 공격 유형 데이터를 저장하고 있는 공격 유형 데이터베이스부; 및

상기 서명 코드가 공격 패턴으로 판단되는 경우 상기 공격 패턴의 서명 코드에 해당하는 공격 유형을 상기 공격 유형 데이터베이스부에서 검색하는 검색부를 포함하는 것을 특징으로 하는 센서 노드.

청구항 7

삭제

명세서

기술분야

[0001] 본 발명은 무선 센서 네트워크의 공격 탐지 시스템(Intrusion Detection System, IDS)에 관한 것으로, 보다 구체적으로 무선 센서 네트워크에 분포되어 있는 센서 노드들은 애드-혹(ad-hoc) 방식으로 데이터를 송수신하며 복수의 서로 다른 종류의 공격 유형 데이터 중 어느 하나를 저장하고 있으며 공격 패턴 서명 코드에 상응하는 공격 유형 데이터베이스를 구비하여 센서 노드에서 공격 패턴 서명 코드를 탐지시 공격 유형을 확인하기 위하여 싱크 노드로 공격 패턴 서명 코드를 송수신하지 않아 공격 패턴 서명 코드의 송수신에 따른 에너지 소실을 줄이며 오탐(false positive) 공격을 방지할 수 있는 무선 센서 네트워크에 관한 것이다.

배경기술

[0002] 무선 센서 네트워크는 센서 노드(Sensor Node)와 이를 수집하여 외부로 내보내는 싱크 노드(Sink Node)로 구성된 네트워크로, IEEE 802.15.4를 기반으로 하는 6LoWPAN은 센서 노드상에 IPv6를 할당하여 최근 유비쿼터스 컴퓨팅 환경을 구축하기 위한 핵심 기술로 많은 관심을 끌고 있다.

[0003] 무선 센서 네트워크는 야생환경 모니터링, 산업기계 계측, 건축구조물 안전 모니터링, 군사목적 계측 등 특수 응용 분야에서부터 교통 트래픽 모니터링, 공해 모니터링, 화재 감시 등 생활 응용 분야에 이르기까지 그 이용 분야가 방대하며 대부분 대상 정보에 대한 정확한 측정과 안전한 정보 수집 및 전달을 요구한다. 따라서 무선 센서 네트워크에서 공격 탐지를 포함한 보안 기능이 반드시 필수적으로 요구되고 있는데, 공격 탐지 시스템(IDS, Intrusion Detection System)은 무선 센서 네트워크를 공격으로부터 보호하는 기초적이면서 중요한 시스템이다.

[0004] 무선 센서 네트워크의 공격 탐지 시스템은 서명(signature) 기반으로 공격을 탐지하는 방식과 패킷 트래픽량을 관리자가 모니터링하여 공격을 탐지하는 행위 기반 방식으로 크게 분류할 수 있는데, 도 1 내지 도 3을 참고로 종래 무선 센서 네트워크에서 블룸필터를 이용하여 서명 기반으로 공격을 탐지하는 방식을 보다 구체적으로 살펴본다.

[0005] 도 1은 종래 무선 센서 네트워크에서 소스 노드(SS)로부터 목적지 노드(DS)로 데이터를 송신하는 과정을 설명하기 위한 도면이다.

[0006] 소스 노드(SS)가 위치하는 장소에서 수집한 데이터 또는 목적지 노드(DS)로 송신하고자 하는 데이터를 소스 노드(SS)는 애드-혹(ad-hoc) 방식으로 목적지 노드(DS)로 송신한다. 무선 센서 네트워크는 별도의 기반 통신 시설이 없기 때문에, 무선 센서 네트워크에서 무선 센서 네트워크를 구성하는 센서 노드들은 데이터를 송수신하는 기능 이외에 소스 노드의 데이터를 목적지 노드로 전달하는 릴레이 노드(Relay node)로도 동작한다.

[0007] 소스 노드(SS)로부터 목적지 노드(DS)로 데이터를 송수신하는 과정에서, 데이터 라우팅 경로 상에 위치하는 릴레이 노드들(RS1, RS2)과 목적지 노드(DS)는 각각 수신 데이터로부터 생성되는 서명 코드로부터 공격 패턴을 감지할 수 있는 블룸 필터부를 구비하고 있다. 예를 들어 데이터 라우팅 경로 상에 위치하는 릴레이 노드(RS1)에서 수신 데이터로부터 서명 코드를 생성하고 생성한 서명 코드가 공격 패턴으로 탐지되는 경우, 공격 패턴 서명 코드를 싱크 노드로 송신하여 공격 패턴 서명 코드에 해당하는 공격 유형을 확인하거나 공격 패턴 서명 코드에 해당하는 공격 패턴이 오탐(false positive) 패턴인지 여부를 확인하게 된다.

[0008] 도 2는 종래 센서 노드에 구비되어 있는 블룸 필터부를 보다 구체적으로 설명하기 위한 도면이다.

[0009] 도 2를 참고로 살펴보면, 센서 노드에서 공격 데이터가 수신되면 서명 코드 생성부(10)는 공격 데이터를 해쉬 함수(HF)에 적용하여 서명 코드를 생성한다. 서명 코드 생성부(10)는 서로 다른 복수의 해쉬 함수를 구비하고

있는데, 공격 데이터를 서로 다른 해쉬 함수에 각각 적용하여 서로 다른 해쉬 함수값을 생성하며 생성한 서로 다른 해쉬 함수값의 조합으로 서명 코드를 생성한다. 여기서 해쉬 함수는 입력되는 공격 데이터의 크기에 상관없이 항상 일정한 크기를 가지는 해쉬 함수값을 생성한다.

[0010] 공격 패턴 판단부(20)는 생성한 서명 코드와 블룸 필터 저장부(30)에 저장되어 있는 공격 패턴 데이터를 비교하여 생성한 서명 코드가 공격 패턴인지 판단한다. 블룸필터 저장부(30)에 저장되어 있는 공격 패턴 데이터는 0과 1의 배열로 구성되어 있는데, 탐지하고자 하는 공격 데이터를 복수의 해쉬 함수에 각각 적용하여 생성되는 해쉬 함수값에 해당하는 배열 위치는 1로 초기 설정되어 있으며 탐지하고자 하는 공격 데이터를 복수의 해쉬 함수에 각각 적용하여 생성되는 해쉬 함수값에 해당하지 않는 배열 위치는 0으로 초기 설정된다. 종래 무선 센서 네트워크에 분포되어 있는 센서 노드는 모두 동일한 공격 패턴의 서명 코드를 탐지하기 위한 공격 패턴 데이터가 저장되어 있는 블룸필터 저장부를 구비하고 있다.

[0011] 공격 패턴 판단부(20)는 서명 코드에 해당하는 블룸필터 저장부(30)의 배열 위치에 저장되어 있는 공격 패턴 데이터를 검색하여, 서명 코드에 해당하는 블룸필터 저장부(30)의 배열 위치에 저장되어 있는 공격 패턴 데이터가 모두 1로 설정되어 있는 경우, 생성한 서명 코드를 공격 패턴으로 판단한다. 예를 들어, 서명 코드 생성부(10)가 2개의 해쉬 함수(HF1, HF2)로 구성되어 있으며 공격 데이터를 해쉬 함수(HF1, HF2)에 적용하여 생성된 서명 코드가 (1/4)인 경우, 서명 코드(1/4)에 해당하는 블룸필터 저장부(30)의 배열 위치($i=1, i=4$, 첫번째 배열 위치는 $i=0$ 으로 시작)에 저장되어 있는 공격 패턴 데이터가 모두 1로 설정되어 있는 경우 생성한 서명 코드를 공격 패턴으로 판단한다.

[0012] 공격 패턴 송신부(40)는 생성한 서명 코드가 공격 패턴 서명 코드로 판단되는 경우, 공격 패턴 서명 코드를 센서 노드의 싱크 노드로 송신하며, 싱크 노드는 수신한 공격 패턴 서명 코드가 오탐(false positive) 패턴인지 여부를 판단하거나 공격 패턴 서명 코드에 해당하는 공격 유형을 판단하여 무선 센서 네트워크에서 공격 노드를 차단 제어하기 위한 후속 조치를 취한다. 싱크 노드는 공격 패턴 서명 코드가 오탐 패턴인지 여부를 판단하거나 공격 패턴 서명 코드에 해당하는 공격 유형을 판단하기 위하여 각 공격 패턴 서명 코드에 해당하는 공격 유형과 대응 방안을 저장하고 있는 공격 유형 데이터베이스를 구비하고 있다. 도 3은 종래 싱크 노드에 저장되어 있는 공격 유형 데이터베이스의 일 예를 도시하고 있다.

발명의 내용

해결하려는 과제

[0013] 위에서 설명한 블룸 필터를 이용한 서명 기반의 공격 탐지 시스템은 수신한 데이터가 공격 데이터인지를 판단하기 위하여 공격 데이터를 블룸필터에 적용하여 생성되는 서명 코드의 크기를 획기적으로 줄일 수 있으며, 이로 인하여 자원 제한적인 무선 센서 네트워크에서 유용하게 사용될 수 있다.

[0014] 그러나 많은 수의 공격 패턴을 감지하기 위해서는 블룸필터 저장부(30)의 저장 용량을 증가시켜 많은 수의 공격 패턴에 해당하는 서명 코드를 저장하고 있어야 한다. 그러나 자원 제한적인 무선 센서 네트워크의 특성상 공격 패턴에 해당하는 서명 코드를 모두 블룸필터 저장부(30)에 저장하기 곤란하다. 이러한 블룸필터 저장부(30)의 저장 공간의 제한으로 인하여 블룸 필터부는 실제 공격 패턴에 해당하지 않는 서명 코드를 공격 패턴으로 판단하는 경우가 발생하는데, 이를 오탐(false positive) 패턴이라 언급한다. 예를 들어, 도 2에서 공격 패턴에 해당하는 서명 코드의 조합은 각각 1/4, 5/7, 8/9, 12/13, 16/17, 18/19이며 생성한 서명 코드가 1/4, 5/7, 8/9, 12/13, 16/17, 18/19 중 어느 하나에 해당하는 경우에만 공격 패턴 서명 코드로 인식되어야 하는데 서명 코드가 4/5의 경우에도 블룸 필터부는 공격 패턴 서명 코드로 판단하여 공격 패턴 서명 코드의 공격 유형을 확인하기 위하여 공격 패턴 서명 코드를 싱크 노드로 송신하게 된다. 센서 노드는 에너지가 제한되어 이러한 오탐 패턴을 싱크 노드로 송신한데 에너지를 낭비하게 되며, 보안에 취약한 제3자가 오탐 패턴을 악용하여 주기적으로 오탐 패턴을 싱크 노드로 송신하는 경우 무선 센서 네트워크가 제대로 동작하지 못한다는 문제점을 가진다.

[0015] 본 발명은 종래 무선 센서 네트워크에서 블룸필터를 이용한 서명 코드기반의 공격 탐지 시스템이 가지는 문제점을 해결하기 위한 것으로, 본 발명이 이루고자 하는 목적은 센서 노드에 구비되어 있는 블룸필터부에서 공격 패턴으로 판단되는 오탐 패턴의 서명 코드를 싱크노드로 송신함에 따른 에너지 낭비를 방지할 수 있는 무선 센서 네트워크를 제공하는 것이다.

[0016] 본 발명이 이루고자 하는 다른 목적은 센서 노드에서 공격 패턴으로 판단된 서명 코드의 공격 유형을 센서 노드에서 직접 판단할 수 있는 무선 센서 네트워크를 제공하는 것이다.

[0017] 본 발명이 이루고자 하는 또 다른 목적은 애드-혹 방식의 무선 센서 네트워크에 분포되어 있는 센서 노드들에 서로 다른 공격 패턴을 탐지할 수 있는 서로 다른 유형의 공격 패턴 데이터를 저장하여 소스 노드에서 목적지 노드까지의 홉 수가 증가할수록 공격 데이터를 더욱 정확하게 탐지할 수 있는 무선 센서 네트워크를 제공하는 것이다.

[0018] 본 발명이 이루고자 하는 또 다른 목적은 무선 센서 네트워크에 분포되어 있는 센서 노드들에 서로 다른 공격 패턴을 탐지할 수 있는 서로 다른 유형의 공격 패턴 데이터와 공격 유형을 판단할 수 있는 공격 유형 데이터베이스를 분배 저장하여 한정된 자원을 이용하는 센서 노드의 메모리 공간을 줄이면서 공격 데이터를 정확하게 탐지할 수 있는 무선 센서 네트워크를 제공하는 것이다.

과제의 해결 수단

[0019] 본 발명의 목적을 달성하기 위하여 본 발명에 따른 무선 센서 네트워크는 다수의 센서 노드가 분포되어 있으며, 센서 노드는 복수의 해쉬 함수에 각각 공격 데이터를 적용하여 생성된 해쉬 함수값으로 서명 코드를 생성하며 생성한 서명 코드가 공격 패턴인지 판단하는 블룸필터부와, 공격 패턴의 서명 코드에 해당하는 공격 유형 데이터를 저장하고 있는 공격 유형 데이터베이스와, 서명 코드가 공격 패턴으로 판단되는 경우 공격 패턴의 서명 코드에 해당하는 공격 유형을 공격 유형 데이터에서 검색하는 검색부를 포함하는 것을 특징으로 한다.

[0020] 여기서 블룸 필터는 수신한 공격 데이터를 복수의 해쉬 함수에 적용하여 각 해쉬 함수에 상응하는 해쉬 함수값으로 서명 코드를 생성하는 서명 코드 생성부와, 공격 패턴 데이터를 저장하고 있는 블룸필터 저장부와, 생성한 서명 코드와 공격 패턴 데이터를 비교하여 생성한 서명 코드가 공격 패턴인지 판단하는 공격 패턴 판단부를 포함한다.

[0021] 바람직하게, 무선 센서 네트워크에 분포되어 있는 센서 노드의 블룸필터 저장부에는 서로 다른 공격 패턴을 탐지하기 위한 복수의 공격 패턴 데이터 중 어느 하나가 저장되어 있으며, 센서 노드의 공격 유형 데이터베이스에는 센서 노드의 블룸필터 저장부에 저장되어 있는 공격 패턴 데이터를 통해 탐지할 수 있는 공격 패턴 서명 코드의 공격 유형 데이터베이스가 저장되어 있는 것을 특징으로 한다.

[0022] 바람직하게 공격 패턴의 서명 코드는 서로 다른 등급으로 분류되어 있으며, 상위 등급으로 분류된 공격 패턴의 서명 코드는 하위 등급으로 분류된 공격 패턴의 서명 코드보다 복수의 서로 다른 유형의 공격 패턴 데이터베이스부에 더 많이 중복되어 저장되어 있는 것을 특징으로 한다.

[0023] 여기서 무선 센서 네트워크에 분포되어 있는 다수의 센서 노드들은 애드-혹(ad-hoc) 방식으로 데이터를 송수신하는 것을 특징으로 한다.

발명의 효과

[0024] 본 발명에 따른 무선 센서 네트워크는 종래 무선 센서 네트워크와 비교하여 공격 탐지에 있어 다음과 같은 다양한 효과를 가진다.

[0025] 첫째, 본 발명에 따른 무선 센서 네트워크는 센서 노드에 구비되어 있는 블룸필터부에서 공격 패턴으로 판단되는 서명 코드를 싱크 노드로 송신하지 않고 직접 센서 노드에서 오탐 패턴 또는 공격 유형을 판단함으로써, 서명 코드 송신에 따른 에너지 낭비를 방지할 수 있다.

[0026] 둘째, 본 발명에 따른 무선 센서 네트워크는 센서 노드에서 공격 패턴으로 판단된 서명 코드가 오탐 패턴인지를 직접 공격 유형 데이터베이스부를 통해 센서 노드에서 판단함으로써, 오탐 패턴을 이용한 제3자의 악의적인 공격을 방지할 수 있다.

[0027] 셋째, 본 발명에 따른 무선 센서 네트워크는 센서 노드들에 서로 다른 공격 패턴을 탐지할 수 있는 서로 다른 유형의 공격 패턴 데이터를 저장함으로써, 소스 노드에서 목적지 노드까지의 홉 수가 증가할수록 공격 데이터를 더욱 정확하게 탐지할 수 있다.

[0028] 넷째, 본 발명에 따른 무선 센서 네트워크는 센서 노드들에 서로 다른 공격 패턴을 탐지할 수 있는 서로 다른 유형의 공격 패턴 데이터가 저장되며, 저장된 공격 패턴 데이터에 따른 공격 패턴 서명 코드의 공격 유형을 판단할 수 있는 공격 유형 데이터베이스를 분배 저장함으로써, 한정된 자원을 이용하는 센서 노드의 메모리 공간을 줄이면서 공격 데이터를 정확하게 탐지할 수 있다.

도면의 간단한 설명

- [0029] 도 1은 종래 무선 센서 네트워크에서 소스 노드로부터 목적지 노드로 데이터를 송신하는 과정을 설명하기 위한 도면이다.
- 도 2는 종래 센서 노드에 구비되어 있는 블룸 필터부를 보다 구체적으로 설명하기 위한 도면이다.
- 도 3은 종래 싱크 노드에 저장되어 있는 공격 유형 데이터베이스의 일 예를 도시하고 있다.
- 도 4는 본 발명에 따른 무선 센서 네트워크에서 소스 노드로부터 목적지 노드로 데이터를 송신하는 과정을 설명하기 위한 도면이다.
- 도 5는 본 발명에 따른 무선 센서 네트워크에 분포되어 있는 센서 노드의 일 예를 설명하기 위한 도면이다.
- 도 6은 본 발명에 따른 무선 센서 네트워크에 분포되어 있는 센서 노드의 다른 예를 설명하기 위한 도면이다.
- 도 7은 도 5에서 설명한 센서 노드의 공격 유형 데이터베이스부와 도 6에서 설명한 센서 노드의 공격 유형 데이터베이스부의 일 예를 도시하고 있다.
- 도 8은 공격 패턴 서명 코드의 공격 등급과 공격 등급에 따라 공격 패턴 데이터의 설정 저장 예를 설명하기 위한 도면이다.
- 도 9는 본 발명에 따른 무선 센서 네트워크에서 소스 노드에서 목적지 노드 또는 싱크 노드로 공격 데이터 송신에 따른 평균 홉수 및 공격 데이터 탐지율을 도시하고 있다.
- 도 10은 본 발명에 따른 무선 센서 네트워크에서 사용되는 공격 패턴 데이터의 종류와 그에 따른 블룸 필터 저장부 및 공격 유형 데이터베이스의 필요 메모리 크기를 도시하고 있다.

발명을 실시하기 위한 구체적인 내용

- [0030] 이하 첨부한 도면을 참고로 본 발명에 따른, 공격 탐지가 가능한 무선 센서 네트워크에 대해 보다 구체적으로 설명한다.
- [0031] 도 4는 본 발명에 따른 무선 센서 네트워크에서 소스 노드(SS)로부터 목적지 노드(DS)로 데이터를 송신하는 과정을 설명하기 위한 도면이다.
- [0032] 무선 센서 네트워크에는 다수의 센서 노드들이 분포되어 있으며, 센서 노드들은 수신 데이터로부터 생성되는 서명 코드로부터 공격 패턴을 감지할 수 있는 블룸 필터부와 감지한 공격 패턴 서명 코드의 공격 유형을 판단할 수 있는 공격 유형 데이터베이스부를 구비하고 있다. 무선 센서 네트워크에 분포된 센서 노드에 구비되어 있는 블룸 필터부에는 서로 다른 공격 패턴을 탐지할 수 있는, 복수의 서로 다른 유형의 공격 패턴 데이터 중 어느 하나가 저장되어 있으며, 공격 유형 데이터베이스부에는 센서 노드의 블룸필터부에 저장되어 있는 공격 패턴 데이터를 통해 탐지할 수 있는 공격 패턴의 공격 유형 데이터베이스가 저장되어 있다.
- [0033] 무선 센서 네트워크에 분포되어 있는 다수의 센서 노드들 중 소스 노드(SS)가 위치하는 장소에서 수집한 데이터 또는 목적지 노드(DS)로 송신하고자 하는 데이터는 애드-혹(ad-hoc) 방식으로 소스 노드(SS)에서 목적지 노드(DS)로 송신된다. 소스 노드(SS)로부터 목적지 노드(DS)로 데이터를 송신하는 과정에서 데이터 라우팅 경로 상에 위치하는 릴레이 노드들(RS1, RS2)과 목적지 노드(DS)는 수신 데이터가 공격 패턴인지 그리고 공격 패턴으로 판단되는 경우 공격 유형을 각 릴레이 노드와 목적지 노드에 구비되어 있는 블룸 필터부와 공격 유형 데이터베이스부를 이용하여 판단한다.
- [0034] 예를 들어, 데이터 라우팅 경로 상에 위치하는 릴레이 노드(RS1)는 수신 데이터로부터 서명 코드(1/6)를 생성한다. 릴레이 노드(RS1)는 생성한 서명 코드와 공격 패턴 데이터를 비교하여 생성한 서명 코드가 공격 패턴의 서명 코드인지 판단한다. 릴레이 노드(RS1)에서 생성한 서명 코드가 공격 패턴의 서명 코드가 아닌 경우, 릴레이 노드(RS1)는 데이터를 다시 릴레이 노드(RS2)로 송신하며 릴레이 노드(RS2)는 수신 데이터로부터 서명 코드(1/6)를 생성한다. 릴레이 노드(RS2)는 생성한 서명 코드와 공격 패턴 데이터를 비교하여 생성한 서명 코드가 공격 패턴의 서명 코드인지 판단한다. 릴레이 노드(RS2)에서 생성한 서명 코드가 공격 패턴의 서명 코드인 경우, 릴레이 노드(RS2)는 릴레이 노드(RS2)에 구비되어 있는 공격 유형 데이터베이스부에 기초하여 공격 패턴 서명 코드가 오탐 패턴인지를 판단하거나 공격 패턴 서명 코드의 공격 유형 또는 대응 방안을 판단한다.
- [0035] 릴레이 노드(RS2)는 공격 패턴 서명 코드가 오탐 패턴인 경우, 데이터를 목적지 노드(DS)로 송신한다. 그러나

공격 패턴 서명 코드가 오탐 패턴이 아니며 공격 패턴 서명 코드에 해당하는 공격 유형과 대응 방안이 공격 유형 데이터베이스부에서 검색되는 경우, 검색된 공격 유형에 따른 대응 방안에 따라 데이터 송수신을 제어한다.

- [0036] 도 5와 도 6은 본 발명에 따른 무선 센서 네트워크에 분포되어 있는 센서 노드를 설명하기 위한 도면이다.
- [0037] 먼저, 도 5를 참고로 본 발명에 따른 무선 센서 네트워크에 분포되어 있는 센서 노드의 일 예를 살펴보면 블루 필터부(100-1)는 공격 데이터로부터 서명 코드를 생성하고, 생성한 서명 코드가 공격 패턴의 서명 코드인지 판단한다. 센서 노드의 블루 필터부(100-1)를 보다 구체적으로 살펴보면, 서명 코드 생성부(110-1)는 공격 데이터를 해쉬 함수(HF)에 적용하여 서명 코드를 생성한다. 서명 코드 생성부(110-1)는 서로 다른 복수의 해쉬 함수를 구비하고 있는데, 공격 데이터를 서로 다른 해쉬 함수에 각각 적용하여 일정한 크기를 가지는 서로 다른 해쉬 함수값을 생성하며 생성한 서로 다른 해쉬 함수값의 조합으로 서명 코드를 생성한다. 여기서 해쉬 함수는 입력되는 공격 데이터의 크기에 상관없이 항상 일정한 크기를 가지는 해쉬 함수값을 생성한다. 무선 센서 네트워크에 분포되어 있는 센서 노드의 서명 코드 생성부는 모두 동일한 복수의 해쉬 함수를 구비하고 있는 것을 특징으로 한다.
- [0038] 공격 패턴 판단부(120-1)는 생성한 서명 코드와 블루 필터 저장부(130-1)에 저장되어 있는 공격 패턴 데이터를 비교하여 생성한 서명 코드가 공격 패턴인지 판단한다. 블루 필터 저장부(130-1)에 저장되어 있는 공격 패턴 데이터는 0과 1의 배열로 구성되어 있는데, 탐지하고자 하는 공격 데이터를 복수의 해쉬 함수에 각각 적용하여 생성되는 해쉬 함수값에 해당하는 배열 위치는 1로 초기 설정되어 있으며 탐지하고자 하는 공격 데이터를 복수의 해쉬 함수에 각각 적용하여 생성되는 해쉬 함수값에 해당하지 않는 배열 위치는 0으로 초기 설정된다.
- [0039] 공격 패턴 판단부(120-1)는 서명 코드에 해당하는 블루 필터 저장부(130-1)의 배열 위치에 저장되어 있는 공격 패턴 데이터를 검색하여, 서명 코드에 해당하는 블루 필터 저장부(30)의 배열 위치에 저장되어 있는 공격 패턴 데이터가 모두 1로 설정되어 있는 경우, 생성한 서명 코드를 공격 패턴으로 판단한다.
- [0040] 검색부(200-1)는 공격 패턴 판단부(120-1)에서 생성된 서명 코드가 공격 패턴 서명 코드로 판단되는 경우, 공격 패턴 서명 코드에 해당하는 공격 유형을 공격 유형 데이터베이스부(300-1)에서 검색하고, 검색 결과에 기초하여 공격 패턴 서명 코드가 오탐 패턴인지 여부를 판단한다. 공격 패턴 서명 코드가 공격 유형 데이터베이스에서 검색되지 않는 경우 오탐 패턴으로 판단된다. 공격 유형 데이터베이스부(300-1)에는 공격 패턴 서명 코드, 공격 패턴 서명 코드에 매핑되어 있는 공격 유형, 공격 유형에 매핑되어 있는 대응 방안이 저장되어 있다.
- [0041] 제어부(400-1)는 검색부(200-1)에서 검색한 공격 패턴 서명 코드에 매핑되어 있는 공격 유형과 대응 방안에 따라 자체적으로 수신 데이터를 제거하거나 수신 데이터가 공격 데이터임을 주변 센서 노드와 싱크 노드로 송신하여 공격 노드를 무선 센서 네트워크에서 차단 제어한다.
- [0042] 한편, 도 6을 참고로 본 발명에 따른 무선 센서 네트워크에 분포되어 있는 센서 노드의 다른 예를 살펴보면, 블루 필터부(100-2)의 서명 코드 생성부(110-2), 공격 패턴 판단부(120-2)는 도 5를 참고로 설명한 블루 필터부(100-1)의 서명 코드 생성부(110-1), 공격 패턴 판단부(120-1)와 동일하며 이하 이에 대한 자세한 설명은 생략한다. 또한 검색부(200-2), 제어부(400-2)는 도 5를 참고로 설명한 검색부(200-1), 제어부(400-1)와 동일하며 이하 이에 대한 자세한 설명은 생략한다.
- [0043] 블루 필터부(100-2)에 구비되어 있는 블루 필터 저장부(130-2)에 저장되어 있는 공격 패턴 데이터는 0과 1의 배열로 구성되어 있는데, 탐지하고자 하는 공격 데이터를 복수의 해쉬 함수에 각각 적용하여 생성되는 해쉬 함수값에 해당하는 배열 위치는 1로 초기 설정되어 있으며 탐지하고자 하는 공격 데이터를 복수의 해쉬 함수에 각각 적용하여 생성되는 해쉬 함수값에 해당하지 않는 배열 위치는 0으로 초기 설정된다. 블루 필터 저장부(120-2)에는 블루 필터부(100-1)를 통해 탐지하고자 하는 공격 데이터와 다른 공격 데이터를 탐지하기 위하여 블루 필터 저장부(120-1)와 다른 공격 패턴 데이터가 저장되어 있다. 공격 패턴 판단부(120-2)는 서명 코드에 해당하는 블루 필터 저장부(130-2)의 배열 위치에 저장되어 있는 공격 패턴 데이터를 검색하여, 서명 코드에 해당하는 블루 필터 저장부(130-2)의 배열 위치에 저장되어 있는 공격 패턴 데이터가 모두 1로 설정되어 있는 경우, 생성한 서명 코드를 공격 패턴으로 판단한다.
- [0044] 또한, 공격 유형 데이터베이스부(300-2)는 블루 필터 저장부(120-2)에 저장되어 있는 공격 패턴 데이터를 통해 탐지할 수 있는 공격 패턴 서명 코드에 해당하는 공격 패턴 서명 코드, 공격 패턴 서명 코드에 매핑되어 있는

공격 유형 및 공격 유형에 매핑되어 있는 대응 방안이 저장되어 있다.

- [0045] 본 발명이 적용되는 분야에 따라 무선 센서 네트워크에 분포되어 있는 센서 노드의 블룸필터 저장부에는 2개 이상의 서로 다른 유형의 공격 패턴 데이터 중 어느 하나가 저장되어 있으며, 센서 노드의 공격 유형 데이터베이스에는 센서 노드의 블룸필터 저장부에 저장되어 있는 공격 패턴 데이터를 통해 탐지할 수 있는 공격 패턴 서명 코드의 공격 유형 데이터베이스가 저장되어 있다.
- [0046] 도 7은 도 5에서 설명한 센서 노드의 공격 유형 데이터베이스부(300-1)와 도 6에서 설명한 센서 노드의 공격 유형 데이터베이스부(300-2)의 일 예를 도시하고 있다.
- [0047] 먼저, 도 7(a)를 참고로 살펴보면 도 5에서 설명한 센서 노드의 공격 유형 데이터베이스부(300-1)에는 센서 노드에서 탐지 가능한 공격 패턴 서명 코드의 종류(1/4, 5/7, 8/9), 각 공격 패턴 서명 코드의 공격 유형(A 타입, B 타입, C 타입) 및 각 공격 유형에 대한 대응 방안이 저장되어 있다.
- [0048] 한편, 도 7(b)를 참고로 살펴보면 도 6에서 설명한 센서 노드의 공격 유형 데이터베이스부(300-2)에는 센서 노드에서 탐지 가능한 공격 패턴 서명 코드의 종류(1/2, 3/5, 6/9), 각 공격 패턴 서명 코드의 공격 유형(D 타입, E타입, F 타입) 및 각 공격 유형에 대한 대응 방안이 저장되어 있다.
- [0049] 도 5 내지 도 7을 참고로 설명한 것과 같이, 본 발명에 따른 무선 센서 네트워크에서는 모든 공격 패턴 서명 코드가 각 센서 노드에서 탐지되는 대신, 각 센서 노드에서 탐지하고자 하는 공격 패턴 서명 코드가 분할되어 있으며 각 센서 노드에서는 저장된 공격 패턴 데이터를 통해 탐지할 수 있는 공격 패턴 서명 코드의 공격 유형 데이터베이스만 필요하므로 이에 따라 적은 메모리 공간을 사용하여 공격 패턴 서명 코드를 탐지하고 센서 노드에서 공격 유형 데이터베이스를 통해 탐지한 공격 패턴 서명 코드의 공격 유형을 판단할 수 있다. 따라서 센서 노드에서 공격 패턴 서명 코드를 싱크 노드로 송신하는데 소비되는 에너지 낭비를 막을 수 있으며, 제3자가 악의적으로 오탐 패턴을 싱크 노드로 반복하여 송신하는 공격을 막을 수 있다.
- [0050] 도 8은 공격 패턴 서명 코드의 공격 등급과 공격 등급에 따라 공격 패턴 데이터의 설정 저장 예를 설명하기 위한 도면이다.
- [0051] 도 8(a)를 참고로 살펴보면, 공격 패턴 서명 코드에 따라 공격 등급이 서로 다르게 설정되어 있다. 예를 들어, 공격 피해성이 크거나 즉각적인 대응이 필요한 공격 패턴의 서명 코드에 대해서는 상위 등급(예를 들어, 1등급)으로 공격 등급이 설정되며, 공격 피해성이 적거나 즉각적인 대응이 필요하지 않은 공격 패턴의 서명 코드에 대해서는 하위 등급(예를 들어, 3등급)으로 공격 등급이 설정된다.
- [0052] 도 8(b)를 참고로 총 3종류의 공격 패턴 데이터 중 1개의 공격 패턴 데이터가 무선 센서 네트워크에 분포된 센서 노드의 블룸 필터 저장부에 저장되어 있는 경우 공격 등급에 따라 무선 센서 네트워크에 분포된 센서 노드의 블룸 필터 저장부에 저장되어 있는 공격 패턴 데이터를 살펴보면, 1등급(0/1, 4/5)으로 설정되어 있는 공격 패턴 서명 코드는 3종류 공격 패턴 데이터에 모두 설정 저장되며, 2등급(1/3, 5/7)으로 설정되어 있는 공격 패턴 서명 코드는 3종류의 공격 패턴 데이터 중 2개에 설정 저장되며, 3등급(0/2, 6/9)으로 설정되어 있는 공격 패턴 서명 코드는 3종류의 공격 패턴 데이터 중 1개에만 설정 저장된다.
- [0053] 이와 같이 공격 등급에 따라 무선 센서 네트워크에 분포된 센서 노드의 블룸 필터 저장부에 저장되는 공격 패턴 데이터를 달리함으로써, 무선 센서 네트워크의 라우팅 경로 상에 위치하는 센서 노드를 통해 상위 등급의 공격 패턴 서명 코드는 더욱 정확하게 탐지될 수 있도록 제어할 수 있다.
- [0054] 도 9는 본 발명에 따른 무선 센서 네트워크에서 소스 노드에서 목적지 노드 또는 싱크 노드로 공격 데이터 송신에 따른 평균 흡수 및 공격 데이터 탐지율을 도시하고 있다. 도 9에 도시되어 있는 바와 같이 2 종류의 공격 패턴 데이터를 사용하는 무선 센서 네트워크에서는 4번째 흡수에서 90% 이상의 탐지율을 보이고 있으며 3종류의 공격 패턴 데이터를 사용하는 무선 센서 네트워크에서는 6번째 흡수에서 90% 이상의 탐지율을 보이고 있으며, 4

종류의 공격 패턴 데이터를 사용하는 무선 센서 네트워크에서는 8번째 함수에서 90% 이상의 탐지율을 보이고 있다.

[0055] 도 10은 본 발명에 따른 무선 센서 네트워크에서 사용되는 공격 패턴 데이터의 종류와 그에 따른 블룸 필터 저장부 및 공격 유형 데이터베이스의 필요 메모리 크기를 도시하고 있다.

[0056] 통상적으로 무선 센서 네트워크에는 무수히 많은 센서 노드들이 분포되어 있으며 많은 수의 릴레이 노드가 데이터를 송수신하기 때문에, 4 종류 이상의 공격 패턴 데이터를 사용하는 경우 1종류의 공격 패턴 데이터를 저장하는데 필요한 메모리 크기보다 작은 메모리로 높은 탐지율을 보인다는 것을 알 수 있다.

[0057] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

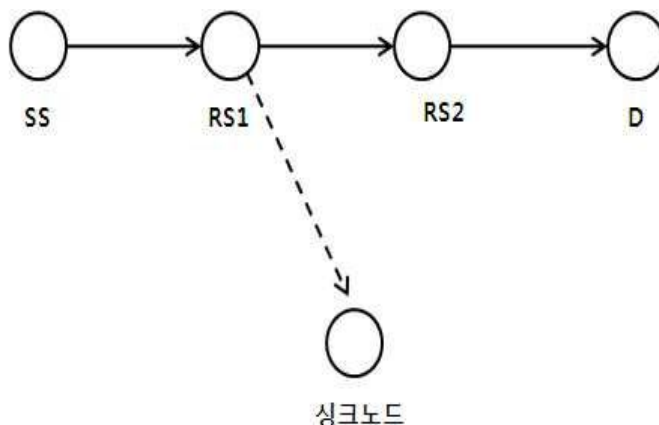
부호의 설명

[0058]

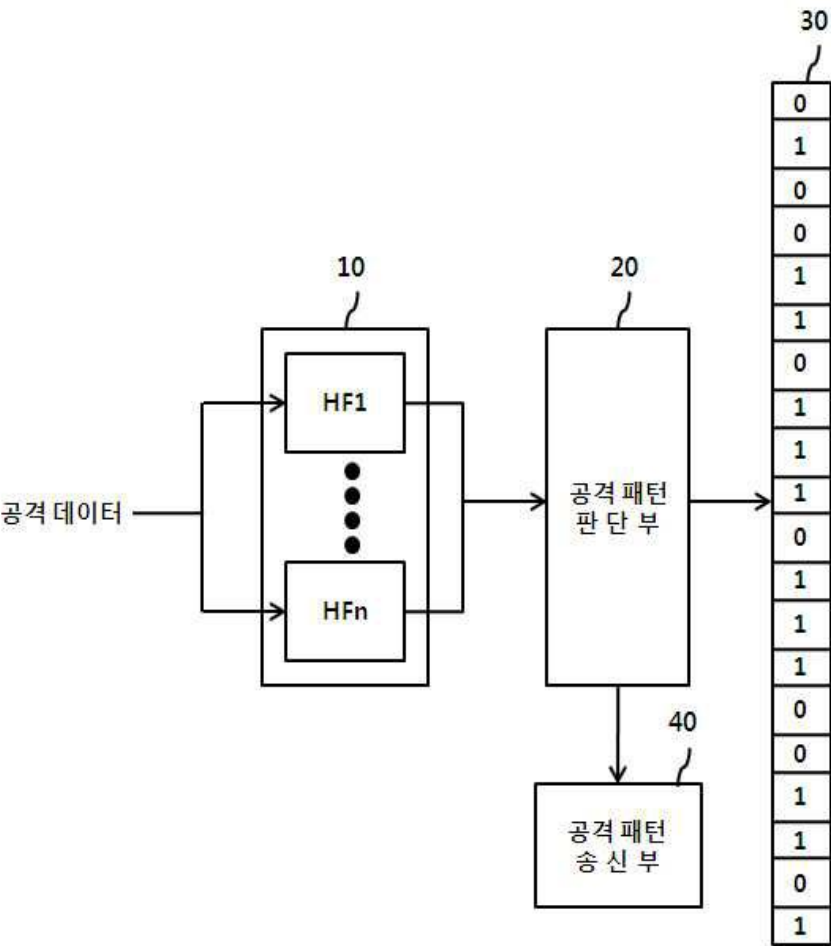
10: 110: 서명 코드 생성부	20, 120: 공격 패턴 판단부
30, 130: 블룸 필터 저장부	40: 공격 패턴 송신부
200: 검색부	300: 공격 유형 데이터베이스부
400: 제어부	

도면

도면1



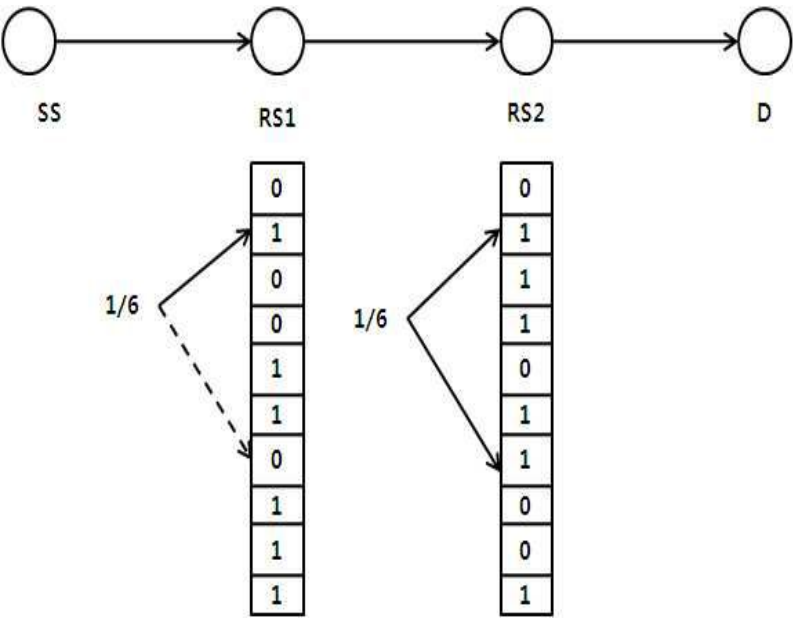
도면2



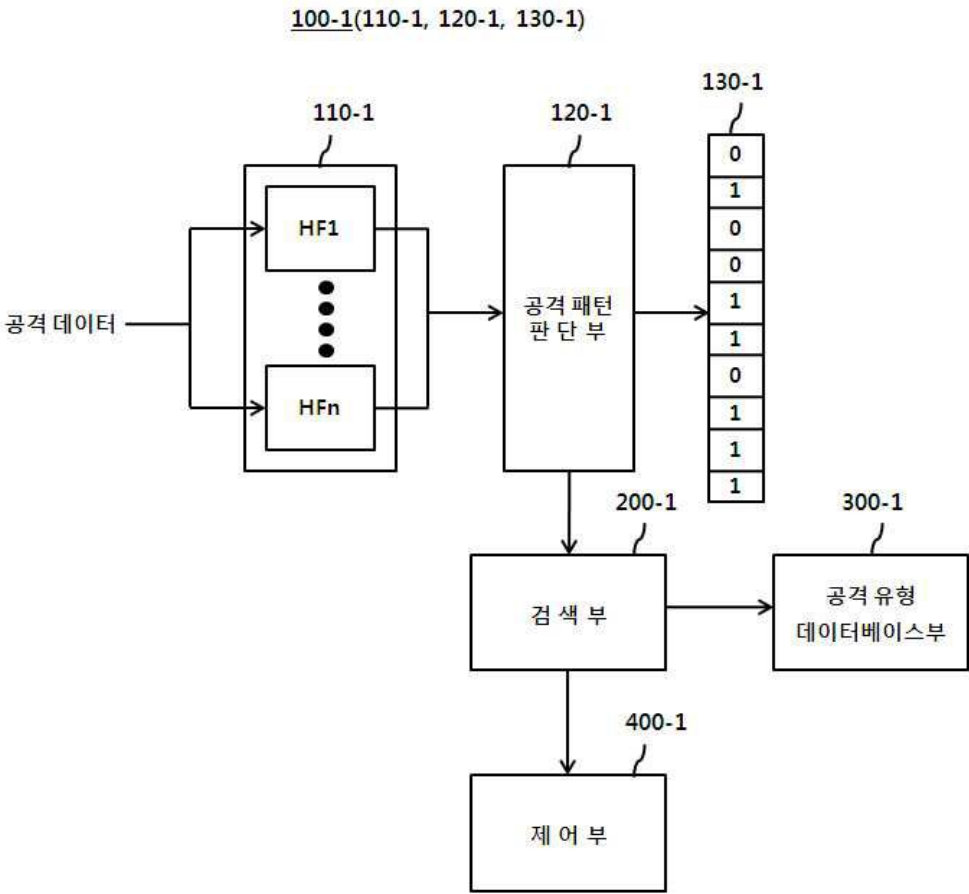
도면3

공격 패턴	공격유형	대응방안
1/4	A타입	차단
5/7	B타입	경고
8/9	C타입	차단
12/13	D타입	차단
16/17	E타입	경고
18/19	F타입	경고

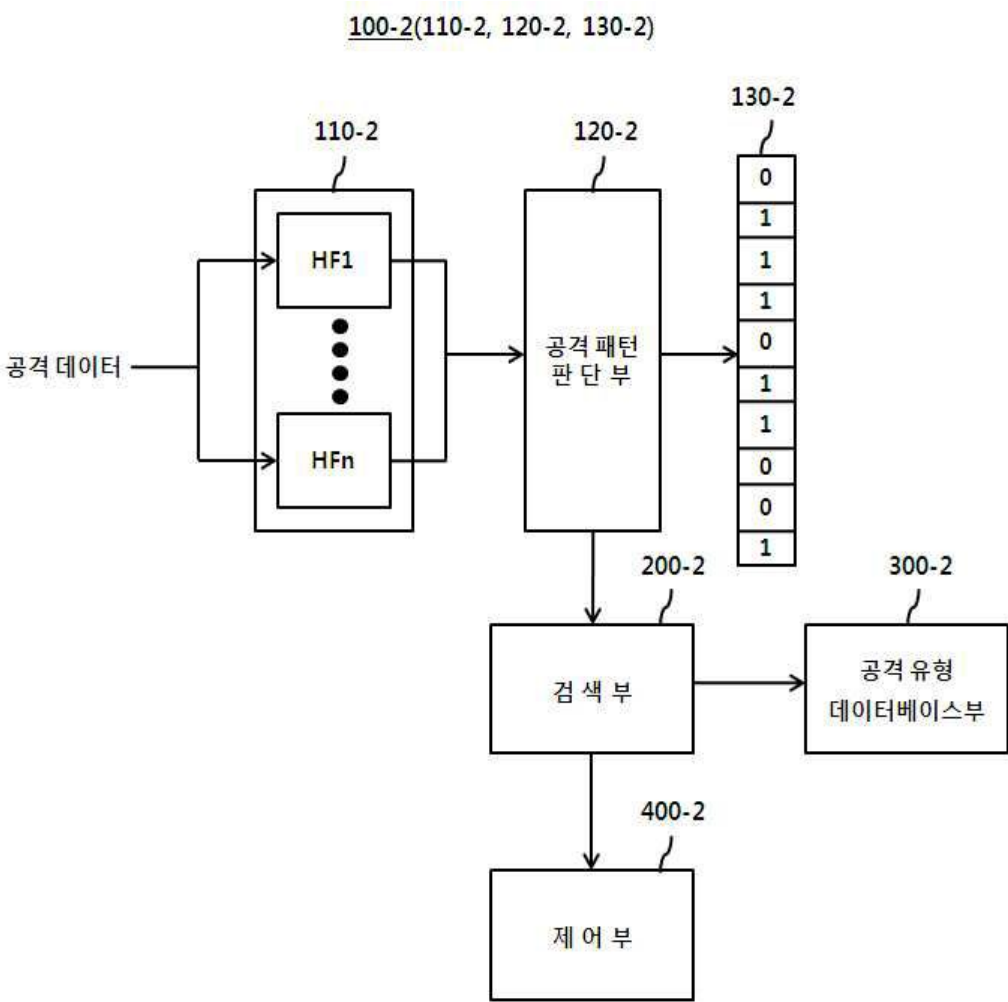
도면4



도면5



도면6



도면7

공격 패턴	공격유형	대응방안
1/4	1등급	차단
5/7	3등급	경고
8/9	2등급	차단

(a)

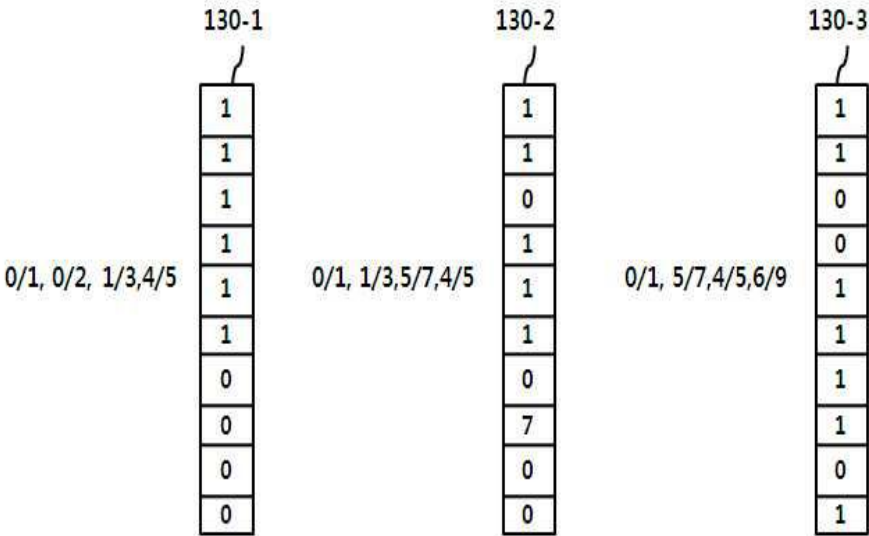
공격 패턴	공격유형	대응방안
1/2	1등급	차단
3/5	2등급	경고
6/9	3등급	경단

(b)

도면8

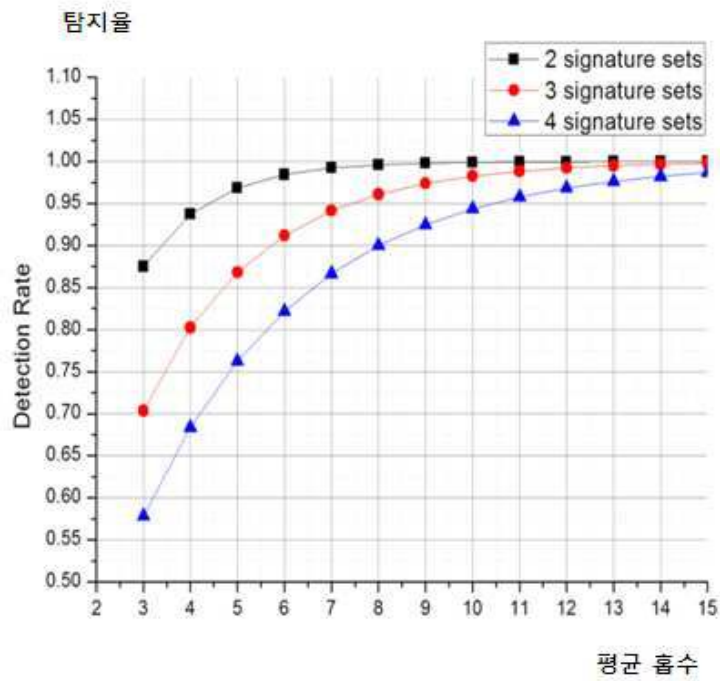
공격 패턴	공격등급
0/1	1등급
0/2	3등급
1/3	2등급
4/5	1등급
5/7	2등급
6/9	3등급

(a)



(b)

도면9



도면10

