



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0075569
(43) 공개일자 2011년07월06일

(51) Int. Cl.

H04L 12/28 (2006.01) H04L 12/26 (2006.01)

(21) 출원번호 10-2009-0132053

(22) 출원일자 2009년12월28일

심사청구일자 2009년12월28일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 서천동 1 경희대학교 국제 캠퍼스내

(72) 발명자

홍충선

경기 용인시 수지구 상현동 성원3차상떼빌아파트 233-101

사이드 오베이드 아민

경기도 용인시 기흥구 서천동 경희대학교 전자정보대학 352호

(뒷면에 계속)

(74) 대리인

서재승

전체 청구항 수 : 총 8 항

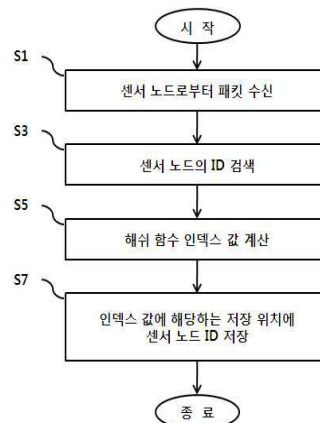
(54) 센서 네트워크에서 패킷의 송신 경로를 역추적하는 방법

(57) 요약

본 발명은 무선 센서 네트워크에서 패킷의 송신 경로를 역추적하는 방법에 관한 것으로, 보다 구체적으로 ब्ल록 필터를 사용하는 로깅 방식의 송신 경로 역추적 방법에서 역추적 오탐율을 줄일 수 있으며 역추적 정확성을 향상시킬 수 있는 패킷 송신 경로의 역추적 방법에 관한 것이다.

본 발명에 따른 패킷 송신 경로의 역추적 방법은 질의 메시지를 브로딩캐스팅 방식이 아닌 유니캐스팅 방식으로 송신하여 패킷의 송신 경로를 역추적함으로써, 패킷 송신 경로의 역추적 오탐율을 줄일 수 있으며, 패킷이 특정 센서 노드를 통과하였는지 여부뿐만 아니라 센서 노드의 ब्ल록 필터에 저장되어 있는 센서 노드 식별자를 통해 패킷의 이전 송신 센서 노드도 판단할 수 있다.

대표도 - 도4



(72) 발명자

조웅준

경기도 수원시 영통구 영통1동 1029-12번지 103호

김진호

경기도 고양시 일산동구 중산동 1800번지 하늘마을
510-806

이 발명을 지원한 국가연구개발사업

과제고유번호 NIPA-2009-(C1090-0902-0016)

부처명 지식경제부

연구관리전문기관

연구사업명 대학 IT 연구센터 지원사업

연구과제명 해킹-바이러스 대응기술 연구

기여율

주관기관 정보통신산업진흥원

연구기간 2009년1월 1일 ~ 2009년 12월 31일

특허청구의 범위

청구항 1

센서 네트워크에서 ब्लूम 필터를 사용하여 패킷의 송신 경로를 역추적하는 방법에 있어서,

- (a) 상기 패킷 송신 경로 상의 제1 센서 노드에서 제1 질의 메시지를 수신하는 단계;
- (b) 상기 제1 질의 메시지에 포함된 페이로드의 해쉬 함수 인덱스 값에 해당하는 상기 ब्लूम 필터의 저장 위치에 저장된 센서 노드 식별자를 검색하는 단계;
- (c) 상기 검색한 센서 노드 식별자들 중 가장 많은 동일 센서 노드 식별자의 센서 노드를 상기 패킷의 송신 경로 상의 제2 센서 노드로 판단하는 단계; 및
- (d) 판단한 상기 패킷의 송신 경로 상의 제2 센서 노드로 제2 질의 메시지를 유니캐스트 방식으로 송신하는 단계를 포함하는 것을 특징으로 하는 패킷 송신 경로의 역추적 방법.

청구항 2

제 1 항에 있어서,

상기 제2 질의 메시지를 유니캐스트 방식으로 수신한 상기 패킷 송신 경로상의 제2 센서 노드는 상기 (a) 단계 내지 상기 (c) 단계를 수행하는 것을 특징으로 하는 패킷 송신 경로의 역추적 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서, 상기 제1 센서 노드 또는 제2 센서 노드는

상기 제1 질의 메시지 또는 상기 제2 질의 메시지에 포함되어 있는 페이로드를 다수의 해쉬 함수에 각각 적용하여 다수의 인덱스 값을 계산하며,

상기 다수의 인덱스 값에 각각 해당하는 상기 ब्लूम 필터의 저장 위치에 저장된 센서 노드의 식별자를 검색하는 것을 특징으로 하는 패킷 송신 경로의 역추적 방법.

청구항 4

제 3 항에 있어서, 상기 센서 노드 식별자는

상기 패킷 송신 경로 상의 제1 센서 노드 또는 제2 센서 노드에서 주변 센서 노드에 할당하는 것을 특징으로 하는 패킷 송신 경로의 역추적 방법.

청구항 5

제 4 항에 있어서,

상기 센서 노드 식별자(IDT)의 크기는 아래의 수학식(1)에 따라 i 비트로 결정되며

[수학식 1]

$$i = \log_2(l_{IDT} + 1)$$

여기서 l_{IDT} 는 센서 노드 식별자(IDT)의 최대 값인 것을 특징으로 하는 패킷 송신 경로의 역추적 방법.

청구항 6

센서 네트워크에서 ब्लूम 필터를 사용하여 패킷의 송신 경로를 역추적하는 방법에 있어서,

- (a) 상기 패킷 송신 경로 상의 제1 센서 노드에서 패킷의 페이로드와 상기 패킷의 수신 시간 정보를 포함하는 제1 질의 메시지를 수신하는 단계;
- (b) 상기 수신한 패킷의 수신 시간 정보에 기초하여 상기 수신 시간에 저장된 ब्लूम 필터를 선택하는 단계;

- (c) 상기 페이로드를 해쉬 함수에 적용하여 해쉬 함수 인덱스 값을 계산하고, 계산한 상기 해쉬 함수 인덱스 값에 해당하는, 상기 선택한 블록 필터의 저장 위치에 저장되어 있는 센서 노드 식별자를 검색하는 단계; 및
- (d) 상기 검색한 센서 노드 식별자들 중 가장 많은 동일 센서 노드 식별자의 센서 노드를 상기 패킷 송신 경로의 제2 센서 노드로 판단하는 단계를 포함하는 패킷 송신 경로의 역추적 방법.

청구항 7

제 6 항에 있어서, 상기 패킷 송신 경로의 역추적 방법은

상기 제1 센서 노드에서 판단한 상기 제2 센서 노드로 제2 질의 메시지를 유니캐스트 방식으로 송신하며,

상기 제2 센서 노드는 상기 (a) 단계 내지 (d) 단계를 수행하는 것을 특징으로 하는 패킷 송신 경로의 역추적 방법.

청구항 8

제 6 항에 있어서, 상기 센서 네트워크에 존재하는 센서 노드들은 서로 동기화되어 있는 것을 특징으로 하는 패킷 송신 경로의 역추적 방법.

명세서

발명의 상세한 설명

기술 분야

- [0001] 본 발명은 무선 센서 네트워크에서 패킷의 송신 경로를 역추적하는 방법에 관한 것으로, 보다 구체적으로 블록 필터를 사용하는 로깅 방식의 송신 경로 역추적 방법에서 역추적 오탐율을 줄일 수 있으며 역추적 정확성을 향상시킬 수 있는 패킷 송신 경로의 역추적 방법에 관한 것이다.

배경 기술

- [0002] 인터넷은 우리의 삶에서 매우 중요한 부분이 되었다. IP 계층을 사용하는 인터넷은 IP를 이용하여 서로 다른 링크인 무선과 유선이 서로 통신 할 수 있도록 한다. 개발자들은 매일 같이 새로운 인터넷 액세스 기술을 개발하고 있기 때문에 인터넷을 기반으로 한 네트워크의 크기는 점차 증대되고 있다. IP 기반 센서 네트워크(IP-USN, IP-based Ubiquitous Sensor Network)은 센서 네트워크를 구성하는 센서 노드들에 IP를 할당하고, 센서 네트워크를 인터넷에 연결하여 외부 단말기와 통신할 수 있는 네트워크이다. IP 기반 센서 네트워크는 군사분야, 민간분야의 환경과 거주지 모니터링, 실시간 건강 관리, 지뢰 탐지, 지능적 운송 시스템 등 여러 곳에서 다양하게 사용되고 있으며, 센서 노드들에 IP를 할당하여 IP 네트워크 상에서 가능한 여러 기술들의 이점을 얻을 수 있다.
- [0003] 그러나 IP 기반 센서 네트워크에서 장소와 시간에 구분없이 센서 네트워크를 통해 다양한 정보를 획득하는 등 IP 기반 센서 네트워크의 순기능과 함께 분산 시스템들의 증가와 인터넷의 확산으로 인해 IP 기반 센서 네트워크를 통한 시스템의 해킹, 정보 유출, 불법 침입, 악성 바이러스 유포 등 역기능도 점차 확대되고 있다.
- [0004] IP 기반 센서 네트워크에서는 센서 노드가 전송하는 데이터를 단순히 암호화하는 것으로는 충분하지 않으며, 센서 네트워크 시스템 내에 비정상적인 행위를 탐지하는 것이 필요하다. DoS나 DDoS와 같은 공격과 침입은 센서 네트워크 시스템에 심각한 피해를 준다. 따라서 이러한 외부 공격 또는 침입으로부터 센서 네트워크 시스템을 보호하기 위하여, 방화벽이나 패킷 필터링, IDS와 같은 시스템을 사용하여 센서 네트워크의 피해를 줄이고 있다. 그러나 외부 공격 또는 침입이 탐지되더라도 외부 공격 또는 침입으로부터 센서 네트워크 시스템의 피해를 최소화하기 위해서는 공격 또는 침입 소스(source)를 찾아내어 원천적으로 공격 또는 침입 소스가 센서 네트워크에 접근하는 것을 차단하여 대응할 필요가 있다.
- [0005] 패킷 송신 경로의 역추적 기법은 공격 또는 침입 소스의 실제 위치를 탐색할 수 있는 기술로 패킷 마킹 방식, 메시징 방식, 패킷 다이제스팅으로 크게 나누어 볼 수 있다. 역추적 기법 중 패킷 다이제스팅 기법은 IP 네트워크에서 라우터가 송신하는 패킷의 트래픽 로그를 블록 필터에 확률적 또는 결정적으로 저장하고 있다가 센서 네트워크에서 공격 또는 침입이 탐지되는 경우 블록 필터에 저장되어 있는 패킷의 트래픽 로그를 이용하여 공격 소스를 역추적하는 방법이다. 즉 패킷 다이제스팅 기법은 블록 필터에 저장되어 있는 트래픽 로그를 이용하는

로깅 방식의 역추적 방법이다.

- [0006] 도 1은 센서 네트워크의 일 예를 도시하고 있으며, 도 2는 센서 노드의 블록 필터에 저장되어 있는 트래픽 로그의 일 예를 도시하고 있다.
- [0007] 도 1을 참고로 살펴보면, 센서 네트워크를 구성하는 센서 노드(SN1)로부터 센서 노드(SN6)로 패킷을 송신하고자 하는 경우, 센서 노드(SN1)에서 생성된 패킷(M1)은 센서 노드들(SN2, SN3, SN4, SN5)을 차례로 통과하여 센서 노드(SN6)로 송신된다. 센서 노드(SN1)로부터 센서 노드(SN6)로 송신되는 패킷이 센서 노드(SN2, SN3, SN4, SN5)를 통과할 때, 각 센서 노드들(SN2, SN3, SN4, SN5)은 각 센서 노드(SN2, SN3, SN4, SN5)에 구비되어 있는 블록 필터에 패킷(M1)의 트래픽 로그를 저장한다.
- [0008] 도 2(a)에 도시되어 있는 센서 노드(SN5)의 블록 필터를 참고로 센서 노드(SN5)에 트래픽 로그가 저장되는 일 예를 살펴보면, 패킷(M1)이 센서 노드(SN5)를 통과할 때 센서 노드(SN5)는 패킷(M1)의 페이로드(P1)를 해쉬 함수에 적용하여 해쉬 함수 인덱스 값을 생성한다. 센서 노드(SN5)는 다수의 해쉬 함수(1, 2, 3, ..., n)에 각각 패킷(M1)의 페이로드(P1)를 적용하여 다수의 해쉬 함수 각각에 상응하는 해쉬 함수 인덱스 값을 생성한다. 해쉬 함수 인덱스 값은 단일 비트열로 구성되어 있는 블록 필터의 저장 위치, 즉 단일 비트열의 주소를 나타내는 값으로 블록 필터는 0의 값으로 초기 설정되어 있다. 해쉬 함수 인덱스 값이 생성되는 경우 해쉬 함수 인덱스 값(0, 3, 7)에 상응하는 블록 필터의 저장 위치의 저장값은 1로 설정된다. 이와 동일하게 패킷(M2)이 센서 노드(SN5)를 통과할 때 센서 노드(SN5)는 패킷(M2)의 페이로드(P2)를 다수의 해쉬 함수에 각각 적용하여 다수의 해쉬 함수 각각에 해당하는 해쉬 함수 인덱스 값을 생성한다. 해쉬 함수 인덱스 값이 생성되는 경우 해쉬 함수 인덱스 값(1, 4, 7, 8)에 상응하는 블록 필터의 저장 위치의 저장값은 1로 설정된다.
- [0009] 한편, 도 2(b)를 참고로 블록 필터에 저장되어 있는 저장값에 기초하여 송신 경로를 역추적하는 방법의 일 예를 살펴보면, 센서 노드(SN6)에서 공격이 감지되거나 잘못된 패킷이 송신되는 경우, 센서 노드(SN6)는 공격이 감지되거나 잘못된 패킷의 송신 경로를 역추적하기 위한 질의 메시지를 생성하고, 생성한 질의 메시지를 브로드캐스팅 방식으로 송신한다. 질의 메시지에는 센서 노드(SN6)가 공격을 감지하거나 잘못된 패킷으로 판단한 패킷의 페이로드가 포함되어 있다.
- [0010] 브로드캐스팅된 질의 메시지를 수신한 센서 노드(SN5)는 질의 메시지에 포함되어 있는 페이로드(P2)를 다수의 해쉬 함수(1, 2, 3, ..., n)에 각각 적용하여 다수의 해쉬 함수 각각에 해당하는 인덱스 값을 생성한다. 생성한 인덱스 값(1, 4, 7, 8)에 해당하는 저장 위치의 저장값은 1로 설정되어 있으며, 따라서 메시지(M2)는 센서 노드(SN5)를 통과하여 센서 노드(SN6)로 송신된 것으로 패킷(M2)의 송신 경로를 역추적한다.
- [0011] 반면, 브로드캐스팅된 질의 메시지를 수신한 센서 노드(SN5)는 질의 메시지에 포함되어 있는 페이로드(P4)를 다수의 해쉬 함수(1, 2, 3, ..., n)에 각각 적용하여 다수의 해쉬 함수 각각에 해당하는 인덱스 값을 생성한다. 생성한 인덱스 값(2, 3, 5)에 해당하는 저장 위치의 저장값 중 일부는 0으로 설정되어 있으며, 따라서 패킷(M4)은 센서 노드(SN5)를 통과하여 센서 노드(SN6)로 송신되지 않은 것으로 패킷(M4)의 송신 경로를 역추적한다.

발명의 내용

해결 하고자하는 과제

- [0012] 위에서 설명한 로깅 방식의 역추적 방법은 질의 메시지를 브로드캐스팅 방식으로 송신하기 때문에, 한정된 에너지원과 낮은 연산 능력을 가지는 센서 네트워크에서는 효율적이지 못한다. 더욱이 질의 메시지를 브로드캐스팅함으로써 인하여, 역추적한 패킷의 송신 경로가 다수개 생길 수 있어 패킷의 송신 경로 역추적에 오류가 발생할 수 있다. 이러한 역추적 오류는 많은 패킷을 송수신하는 싱크 노드 주변의 센서 노드에서 블록 필터의 트래픽 로그가 대부분 1로 설정되어 더욱 심한 역추적 오류를 일으키게 된다.
- [0013] 또한 위에서 설명한 로깅 방법으로 패킷의 송신 경로를 역추적하는 경우, 패킷이 특정 센서 노드를 통과하여 전송되었는지만을 확인할 수 있을 뿐, 패킷이 어떤 센서 노드로부터 송신되었는지를 확인할 수 없다는 문제점을 가진다.
- [0014] 따라서 본 발명이 이루고자 하는 목적은 IP 기반 센서 네트워크에서 질의 메시지를 브로드캐스팅 방식이 아닌 유니캐스팅 방식으로 송신하여 패킷의 송신 경로를 역추적하는 방법을 제공하는 것이다.
- [0015] 본 발명이 이루고자 하는 다른 목적은 패킷이 센서 노드를 통과하였는지 여부뿐만 아니라 센서 노드의 블록 필터에 저장되어 있는 센서 노드 식별자를 통해 패킷의 이전 송신 센서 노드를 판단할 수 있는 역추적 방법을 제

공하는 것이다.

[0016] 본 발명이 이루고자 하는 또 다른 목적은 센서 노드 식별자를 통해 판단한 이전 송신 센서 노드로만 질의 메시지를 유니캐스팅 방식으로 송신하여 패킷 송신 경로의 역추적 오탐율을 줄일 수 있으며, 센서 노드의 에너지 낭비를 줄이고 센서 노드에 가해지는 부하를 줄일 수 있는 역추적 방법을 제공하는 것이다.

[0017] 본 발명이 이루고자 하는 또 다른 목적은 싱크 노드로부터의 거리에 따라 센서 노드의 블룸 필터 수를 설정하여 패킷의 송신 경로 역추적 오탐율을 줄일 수 있는 역추적 방법을 제공하는 것이다.

과제 해결수단

[0018] 본 발명의 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 패킷 송신 경로의 역추적 방법은 패킷 송신 경로 상의 제1 센서 노드에서 제1 질의 메시지를 수신하는 단계와, 제1 질의 메시지에 포함된 페이로드의 해쉬 함수 인덱스 값에 해당하는 블룸 필터의 저장 위치에 저장된 센서 노드 식별자를 검색하는 단계와, 검색한 센서 노드 식별자들 중 동일 센서 노드 식별자를 가장 많이 가지는 센서 노드를 패킷의 송신 경로 상의 제2 센서 노드로 판단하는 단계 및 판단한 상기 패킷의 송신 경로 상의 제2 센서 노드로 제2 질의 메시지를 유니캐스트 방식으로 송신하는 단계를 포함하고 있다.

[0019] 제1 센서 노드 또는 제2 센서 노드는 제1 질의 메시지 또는 제2 질의 메시지에 포함되어 있는 페이로드를 다수의 해쉬 함수에 각각 적용하여 다수의 인덱스 값을 계산하며, 다수의 인덱스 값에 각각 해당하는 블룸 필터의 저장 위치에 저장된 센서 노드의 식별자를 검색하여 패킷의 송신 경로를 역추적한다. 여기서 센서 노드 식별자는 패킷의 송신 경로 상의 제1 센서 노드 또는 제2 센서 노드에서 주변 센서 노드에 할당한 식별 주소인 것을 특징으로 한다.

[0020] 본 발명의 목적을 달성하기 위하여, 본 발명의 다른 실시예에 따른 패킷 송신 경로의 역추적 방법은 패킷 송신 경로 상의 제1 센서 노드에서 수신한 패킷의 페이로드와 패킷의 수신 시간 정보를 포함하는 제1 질의 메시지를 수신하는 단계와, 수신한 패킷의 수신 시간 정보에 기초하여 수신 시간에 저장된 블룸 필터를 검색하는 단계와, 페이로드를 해쉬 함수에 적용하여 해쉬 함수 인덱스 값을 계산하고, 계산한 해쉬 함수 인덱스 값에 해당하는, 검색한 블룸 필터의 저장 위치에 저장되어 있는 센서 노드 식별자를 검색하는 단계 및 검색한 센서 노드 식별자들 중 동일 식별자를 가장 많이 가지는 센서 노드를 패킷의 송신 경로 상의 제2 센서 노드로 판단하는 단계를 포함한다.

[0021] 여기서 센서 네트워크에 존재하는 센서 노드들은 서로 동기화되어 있는 것을 특징으로 한다.

효과

[0022] 본 발명에 따른 패킷 송신 경로의 역추적 방법은 종래 패킷 송신 경로의 역추적 방법과 비교하여 다음과 같은 다양한 효과들을 가진다.

[0023] 첫째, 본 발명에 따른 패킷 송신 경로의 역추적 방법은 질의 메시지를 브로딩캐스팅 방식이 아닌 유니캐스팅 방식으로 송신하여 패킷의 송신 경로를 역추적함으로써, 패킷 송신 경로의 역추적 오탐율을 줄일 수 있다.

[0024] 둘째, 본 발명에 따른 패킷 송신 경로의 역추적 방법은 패킷이 특정 센서 노드를 통과하였는지 여부뿐만 아니라 센서 노드의 블룸 필터에 저장되어 있는 센서 노드 식별자를 통해 패킷의 이전 송신 센서 노드도 판단할 수 있다.

[0025] 셋째, 본 발명에 따른 패킷 송신 경로의 역추적 방법은 센서 노드 식별자를 통해 판단한 이전 송신 센서 노드로만 질의 메시지를 유니캐스팅 방식으로 송신함으로써, 센서 노드에서 소비되는 에너지 낭비를 줄일 수 있으며 센서 노드에 가해지는 부하를 줄일 수 있다.

[0026] 넷째, 본 발명에 따른 패킷 송신 경로의 역추적 방법은 싱크 노드와 싱크 노드 주변에 위치하는 센서 노드 사이의 거리에 따라 주변 센서 노드의 블룸 필터 수를 서로 다르게 설정함으로써, 패킷의 송신 경로 역추적 오탐율을 줄일 수 있다.

발명의 실시를 위한 구체적인 내용

[0027] 이하 첨부한 도면을 참고로 본 발명에 따른 패킷 송신 경로의 역추적 방법에 대해 보다 구체적으로 살펴본다.

[0028] 도 3은 본 발명의 일 실시예에 따른 센서 노드의 기능 블록도를 도시하고 있다.

- [0029] 도 3을 참고로 살펴보면, 센서 노드(1)는 송수신부(10)를 통해 센서 네트워크의 주변 센서 노드로부터 패킷을 수신하거나 센서 네트워크의 주변 센서 노드로 패킷을 송신한다. 또한, 송수신부(10)는 주변 센서 노드로부터 질의 메시지를 수신하거나 생성한 질의 메시지를 주변 센서 노드로 송신한다.
- [0030] 송수신부(10)를 통해 패킷을 수신하는 경우, 저장 제어부(20)는 패킷의 헤더에 저장되어 있는, 패킷을 송신한 주변 센서 노드의 주소를 판단하고, 판단한 주소에 해당하는 센서 노드의 식별자가 식별자 저장부(40)에 저장되어 있는지 판단한다. 식별자 저장부(40)에는 주변 센서 노드의 실제 IP 주소와 주변 센서 노드에 할당된 식별자가 저장되어 있다. 해쉬 함수부(30)는 다수의 해쉬 함수를 구비하고 있으며, 수신한 패킷의 페이로드를 다수의 해쉬 함수 각각에 적용하여 해쉬 함수 인덱스 값을 계산한다. 저장 제어부(20)는 해쉬 함수부(30)에서 계산한 해쉬 함수 인덱스 값에 해당하는 블록 필터의 저장 위치에 판단한 센서 노드의 식별자를 저장 제어한다.
- [0031] 한편, 송수신부(10)를 통해 주변 센서 노드로부터 질의 메시지를 수신하는 경우, 해쉬 함수부(30)는 질의 메시지에 포함되어 있는 페이로드를 해쉬 함수부(30)에 적용하여 해쉬 함수 인덱스 값을 계산하고, 계산한 해쉬 함수 인덱스 값을 센서 노드 판단부(60)로 제공한다. 센서 노드 판단부(60)는 제공된 해쉬 함수 인덱스 값에 해당하는 블록 필터의 저장 위치에 저장되어 있는 센서 노드의 식별자를 추출하고, 추출한 센서 노드의 식별자에 기초하여 질의 메시지에 포함되어 있는 페이로드를 송신한 이전 송신 센서 노드의 주소를 식별자 저장부(40)에서 판단한다. 센서 노드 판단부(60)는 질의 메시지를 생성하고, 생성한 질의 메시지를 판단한 이전 송신 노드로만 유니캐스팅 방식으로 송수신부(10)를 통해 송신한다.
- [0032] 도 4는 본 발명에 따라 블록 필터에 트래픽 로그를 저장하는 방법의 일 예를 설명하기 위한 흐름도이다.
- [0033] 도 3과 도 4를 참고로 보다 구체적으로 살펴보면, 주변 센서 노드로부터 패킷을 수신하는 경우(S1), 패킷의 헤더 정보를 이용하여 패킷을 송신한 주변 센서 노드의 주소를 판단하고 판단한 주소에 해당하는 센서 노드 식별자가 식별자 저장부(40)에 저장되어 있는 식별자인지 검색한다(S3). 이 때, 식별자 저장부(40)에 저장되어 있지 않은 센서 노드의 식별자인 경우, 패킷을 송신한 주변 센서 노드에 식별자를 할당하고 할당한 식별자와 IP 주소를 식별자 저장부에 갱신 등록한다.
- [0034] 식별자 저장부(40)에는 패킷을 수신한 센서 노드가 주변에 위치하는 센서 노드들에 할당한 식별자가 저장되어 있다.
- [0035] 바람직하게, 식별자 저장부(40)에 저장되는 주변 센서 노드들의 식별자는 아래의 수학식(1)에 따라 i 비트로 결정된다.
- [0036] [수학식 1]
- $$i = \log_2(I_{IDT} + 1)$$
- [0037]
- [0038] 여기서 I_{IDT} 는 센서 노드 식별자(IDT)의 최대 값으로, 센서 노드 주변에는 통상적으로 10개 이하의 센서 노드들이 존재하며 주변 센서 노드들의 식별자를 위해 4비트 이하가 사용된다.
- [0039] 한편, 수신한 패킷의 페이로드를 다수의 해쉬 함수에 각각 적용하여 각 해쉬 함수에 대한 해쉬 함수 인덱스 값을 계산하고(S5), 계산한 해쉬 함수 인덱스 값에 해당하는 블록 필터의 저장 위치에 검색한 센서 노드의 식별자를 저장한다(S7).
- [0040] 도 5는 본 발명의 일 실시예에 따른 패킷 송신 경로의 역추적하는 방법을 설명하기 위한 흐름도이다.
- [0041] 도 3과 도 5를 참고로 보다 구체적으로 살펴보면, 패킷의 송신 경로 상의 센서 노드들 중 제1 센서 노드에서 주변 센서 노드로부터 제1 질의 메시지를 수신하는 경우(S11), 제1 질의 메시지에 포함되어 있는 페이로드(P)를 추출하고 해쉬 함수부(30)는 추출한 페이로드를 다수의 해쉬 함수($H_1, H_2, H_3, \dots, H_k$)에 적용하여 각 해쉬 함수에 대한 다수의 인덱스 값을 계산한다(S13). 센서 노드 판단부(60)는 계산한 다수의 인덱스 값에 상응하는 블록 필터의 저장 위치에 저장되어 있는 센서 노드의 식별자(ID)에 기초하여 제1 센서 노드로 페이로드를 포함한 패킷을 송신한 패킷 송신 경로 상의 이전 센서 노드, 즉 제2 센서 노드(D)를 아래의 수학식(2)와 같이 판단한다(S15).
- [0042] [수학식 2]
- [0043] $D = \text{Mode}(\text{ID}[H_1(P)], \text{ID}[H_2(P)], \text{ID}[H_3(P)], \text{ID}[H_4(P)], \dots, \text{ID}[H_k(P)])$

- [0044] 여기서 $ID[H_i(P)]$ 는 다수의 해쉬 함수들($H_1, H_2, H_3, \dots, H_k$) 중 제 i 해쉬 함수에 페이로드(P)를 적용하여 계산한 해쉬 함수 인덱스 값에 상응하는 블록 필터의 저장 위치에 저장되어 있는 센서 노드의 식별자를 의미하며, $Mode()$ 는 구성 식별자들 중 동일한 식별자가 가장 많은 식별자를 선택하는 함수를 의미한다.
- [0045] 수학식(2)에 따라 패킷 송신 경로 상의 제2 센서 노드(D)가 판단되면, 센서 노드 판단부(60)는 제2 질의 메시지를 생성하고 생성한 제2 질의 메시지를 송수신부(10)를 통해 판단한 제2 센서 노드로만 유니캐스팅 방식으로 송신한다(S17). 본 발명에 따른 패킷 송신 경로의 역추적 방법은 질의 메시지를 판단한 패킷 송신 경로 상의 센서 노드로만 유니캐스팅 방식으로 송신함으로써, 질의 메시지를 브로드캐스팅 방식으로 송신하여 발생하는 역추적 오답율을 줄이고 센서 노드의 에너지 소비를 줄일 수 있다.
- [0046] 도 6은 본 발명의 일 실시예에 따라 블록 필터에 저장되어 있는 센서 노드 식별자에 기초하여 패킷 송신 경로를 역추적하는 일 예를 설명하기 위한 도면이다.
- [0047] 도 6을 참고로 살펴보면, 제1 센서 노드가 제1 질의 메시지를 수신하는 경우, 제1 질의 메시지에 포함되어 있는 페이로드를 다수의 해쉬 함수들($H_1, H_2, H_3, \dots, H_k$)에 각각 적용하여 해쉬 함수 인덱스 값을 계산하고, 계산한 인덱스 값에 상응하는 블록 필터의 저장 위치에 저장되어 있는 i 비트의 센서 노드 식별자(ID)를 인식한다.
- [0048] 예를 들어, 제1 해쉬 함수 내지 제6 해쉬 함수, 총 6개의 해쉬 함수를 사용하며 제1 해쉬 함수 내지 제6 해쉬 함수에 페이로드를 적용하여 계산한 제1 해쉬 함수 내지 제6 해쉬 함수의 인덱스 값이 각각 1, 4, 3, 8, 10, 6 인 경우, 블록 필터의 저장 위치 중 제1 해쉬 함수 내지 제6 해쉬 함수의 인덱스 값에 상응하는 저장 위치에 저장되어 있는 센서 노드 식별자들(010, 010, 010, 011, 010, 100)에 기초하여 동일한 식별자가 가장 많은 식별자(010)를 제2 센서 노드의 식별자로 판단한다.
- [0049] 다른 주변 센서 노드로부터 패킷이 송신되어 블록 필터의 특정 저장 위치에 저장되어 있던 센서 노드의 식별자가 다른 주변 센서 노드로부터 송신된 패킷에 의해 갱신되더라도, 다수의 해쉬 함수 인덱스 값을 사용하여 해쉬 함수 인덱스 값에 상응하는 블록 필터의 저장 위치에 센서 노드의 식별자를 저장함으로써, 패킷 송신 경로의 역추적 오답율을 줄일 수 있다.
- [0050] 도 7은 본 발명의 다른 실시예에 따른 패킷 송신 경로의 역추적 방법을 설명하기 위한 흐름도이다.
- [0051] 도 3과 도 7을 참고로 보다 구체적으로 살펴보면, 패킷의 송신 경로 상의 센서 노드들 중 제1 센서 노드에서 주변 센서 노드로부터 제1 질의 메시지를 수신하는 경우(S31), 센서 노드 판단부(60)는 제1 질의 메시지에 포함되어 있는 패킷의 수신 시각에 기초하여 다수의 블록 필터들을 구비하는 블록 필터부(50)에서 패킷 수신 시각에 패킷의 트래픽 로그를 저장하고 있는 블록 필터를 선택한다(S33). 싱크 노드 주변에 가깝게 위치하고 있는 센서 노드들은 싱크 노드로부터 멀리 떨어져 위치하고 있는 센서 노드에 비하여 더 많은 패킷을 전달하며 따라서 싱크 노드와 센서 노드 사이의 위치에 기초하여 싱크 노드로부터 가까이 위치하는 센서 노드들은 전달되는 다수 패킷의 트래픽 로그를 저장하기 위하여 싱크 노드로부터 멀리 떨어져 위치하는 센서 노드보다 더 많은 수의 블록 필터를 구비하고 있다. 저장 제어부(20)는 블록 필터의 용량이 채워진 경우, 각 블록 필터의 용량이 채워진 시각과 블록 필터 식별자를 블록 필터 식별자 테이블에 저장한다.
- [0052] 실제 제1 질의 메시지에 저장되어 있는 패킷의 수신 시각은 공격을 감지한 센서 노드에서 패킷을 수신한 시각으로, 제1 센서 노드에서 동일 패킷을 수신한 시각과는 서로 상이하다. 그러나 제1 센서 노드에서 패킷을 수신한 시각과 공격을 감지한 센서 노드에서 패킷을 수신한 시각의 차이는 미비하므로, 제1 질의 메시지에 저장되어 있는 패킷의 수신 시각과 가장 근접하여 블록 필터 용량이 채워진 블록 필터를 선택한다. 바람직하게, 센서 네트워크를 구성하는 다수의 센서 노드들은 서로 수신 시각을 파악하기 위하여 동기화되어 있다.
- [0053] 블록 필터를 선택한 경우, 센서 노드 판단부(60)는 제1 질의 메시지에 포함되어 있는 페이로드(P)를 해쉬 함수부(30)로 제공하며, 해쉬 함수부(30)는 다수의 해쉬 함수($H_1, H_2, H_3, \dots, H_k$)에 페이로드를 적용하여 각 해쉬 함수에 대한 다수의 인덱스 값을 계산한다(S35). 계산한 다수의 인덱스 값에 상응하는, 선택한 블록 필터의 저장 위치에 저장되어 있는 센서 노드의 식별자(ID)에 기초하여 제1 센서 노드로 페이로드를 포함한 패킷을 송신한 패킷 송신 경로 상의 이전 센서 노드, 즉 제2 센서 노드(D)를 위의 수학식(2)와 같이 판단한다(S37).
- [0054] 패킷 송신 경로 상의 제2 센서 노드(D)가 판단되면, 제2 질의 메시지를 생성하고 생성한 제2 질의 메시지를 판단한 제2 센서 노드로만 유니캐스팅 방식으로 송신한다(S39).

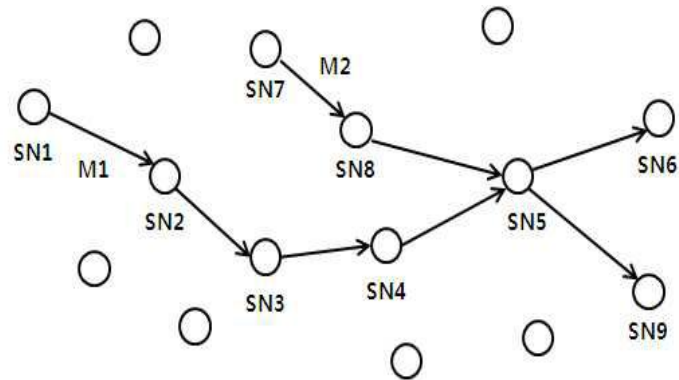
- [0055] 도 8은 본 발명의 다른 실시예에 따른 블룸 필터부의 일 예를 도시하고 있으며, 도 9는 본 발명의 다른 실시예에 따른 블룸 필터 식별자 테이블의 일 예를 도시하고 있다.
- [0056] 도 8을 참고로 살펴보면, 블룸 필터부(50)에 제1 내지 제3 블룸 필터들이 구비되어 있으며, 제1 블룸 필터, 제2 블룸 필터, 제3 블룸 필터에 차례로 패킷의 트래픽 로그가 저장된다. 즉, 제1 블룸 필터의 용량이 채워질 때까지 해쉬 함수 인덱스 값에 상응하는 제1 블룸 필터의 저장 위치에 센서 노드의 식별자를 저장하며, 제1 블룸 필터의 용량이 채워진 경우 제2 블룸 필터에 해쉬 함수 인덱스 값에 상응하는 제2 블룸 필터의 저장 위치에 센서 노드의 식별자를 저장하며, 제2 블룸 필터의 용량이 채워진 경우 해쉬 함수 인덱스 값에 상응하는 제2 블룸 필터의 저장 위치에 센서 노드의 식별자를 저장한다.
- [0057] 도 9를 참고로 살펴보면, 제1 블룸 필터의 용량이 채워진 경우 제1 블룸 필터의 용량이 채워진 시각(t_1)과 제1 블룸 필터의 식별자(01)가 블룸 필터 식별자 테이블에 저장되며, 제2 블룸 필터의 용량이 채워진 경우 제2 블룸 필터의 용량이 채워진 시각(t_2)과 제2 블룸 필터의 식별자(10)가 블룸 필터 식별자 테이블에 저장된다.
- [0058] 한편, 상술한 본 발명의 실시 예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.
- [0059] 상기 컴퓨터로 읽을 수 있는 기록 매체는 전기 또는 자기식 저장 매체(예를 들어, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.
- [0060] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면의 간단한 설명

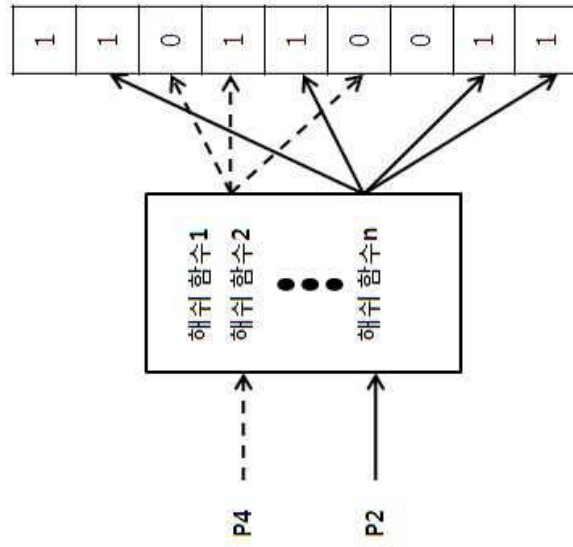
- [0061] 도 1은 센서 네트워크의 일 예를 도시하고 있다.
- [0062] 도 2는 센서 노드의 블룸 필터에 저장되어 있는 트래픽 로그의 일 예를 도시하고 있다.
- [0063] 도 3은 본 발명의 일 실시예에 따른 센서 노드의 기능 블록도를 도시하고 있다.
- [0064] 도 4는 본 발명에 따라 블룸 필터에 트래픽 로그를 저장하는 방법의 일 예를 설명하기 위한 흐름도이다.
- [0065] 도 5는 본 발명에 따른 패킷의 송신 경로를 역추적하는 방법의 일 예를 설명하기 위한 흐름도이다.
- [0066] 도 6은 본 발명에 따라 블룸 필터에 저장되어 있는 센서 노드 식별자에 기초하여 제2 송신 노드를 판단하는 방법의 일 예를 설명하기 위한 도면이다.
- [0067] 도 7은 본 발명의 다른 실시예에 따른 패킷 송신 경로의 역추적 방법을 설명하기 위한 흐름도이다.
- [0068] 도 8은 블룸 필터부와 블룸 필터 식별자 테이블의 일 예를 도시하고 있다.
- [0069] <도면의 주요 부분에 대한 설명>
- [0070] 10: 송수신부 20: 저장 제어부
- [0071] 30: 해쉬 함수부 40: 식별자 저장부
- [0072] 50: 블룸 필터부 60: 센서 노드 판단부

도면

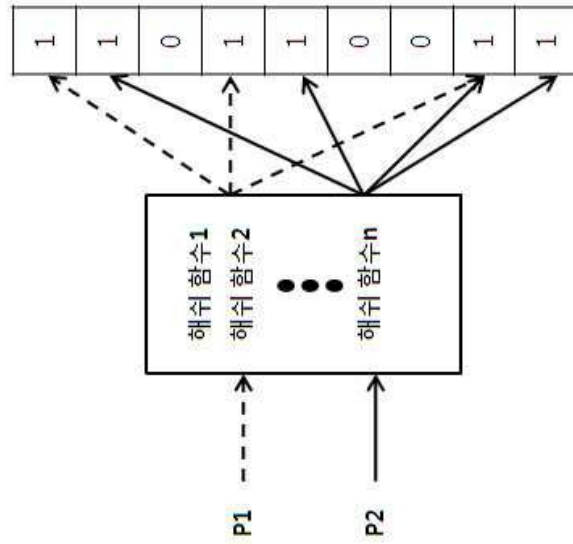
도면1



도면2

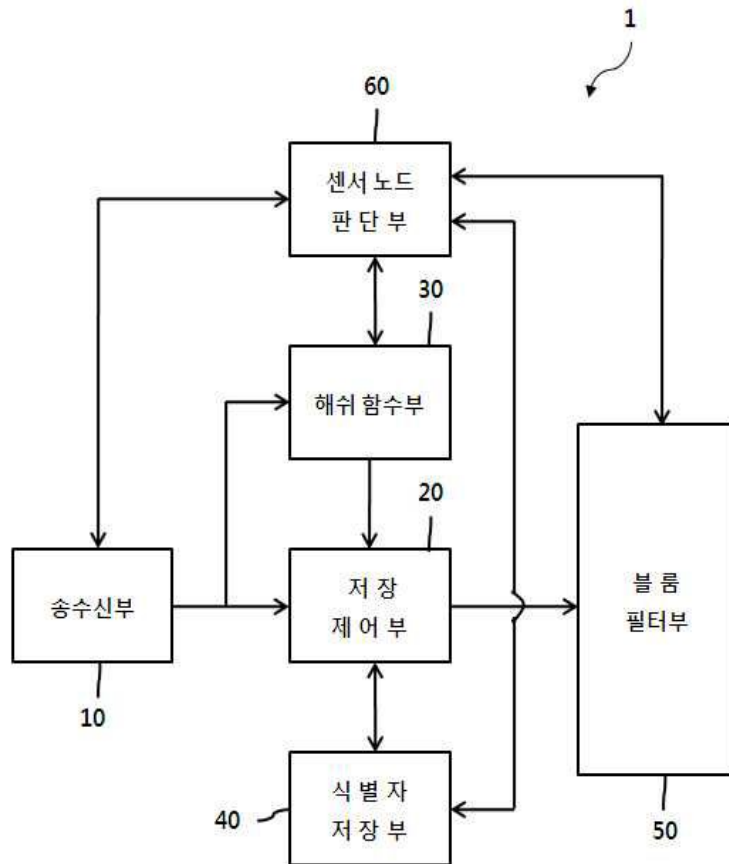


(b)

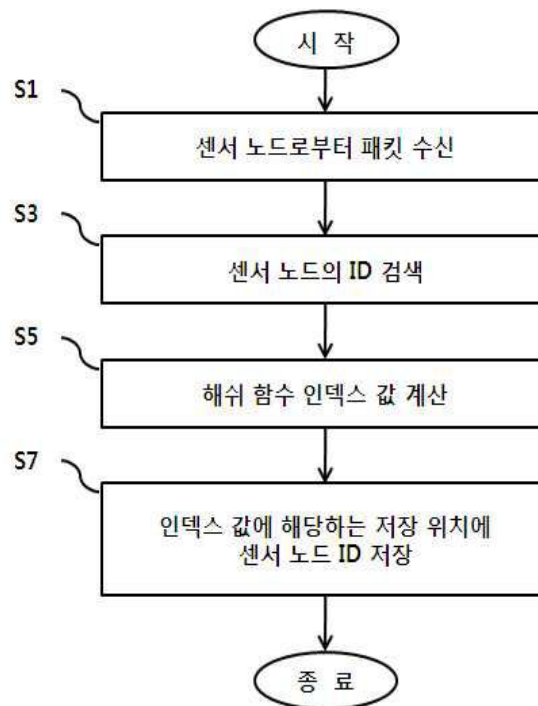


(a)

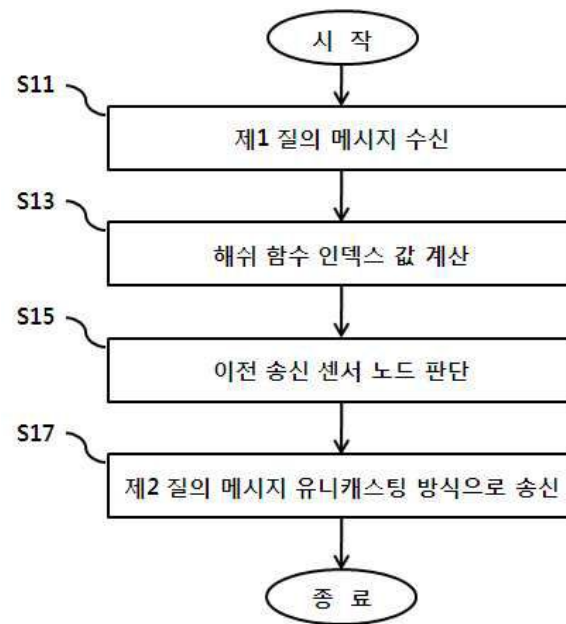
도면3



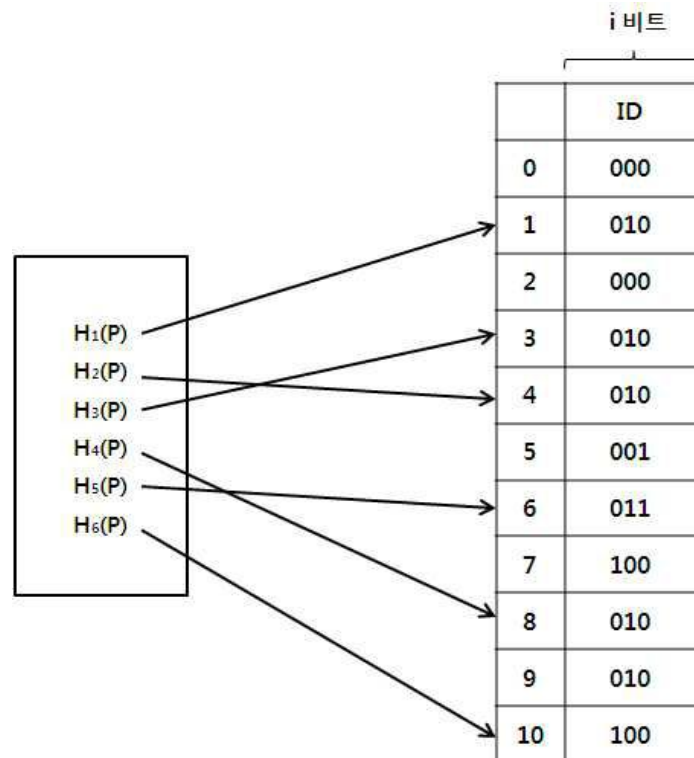
도면4



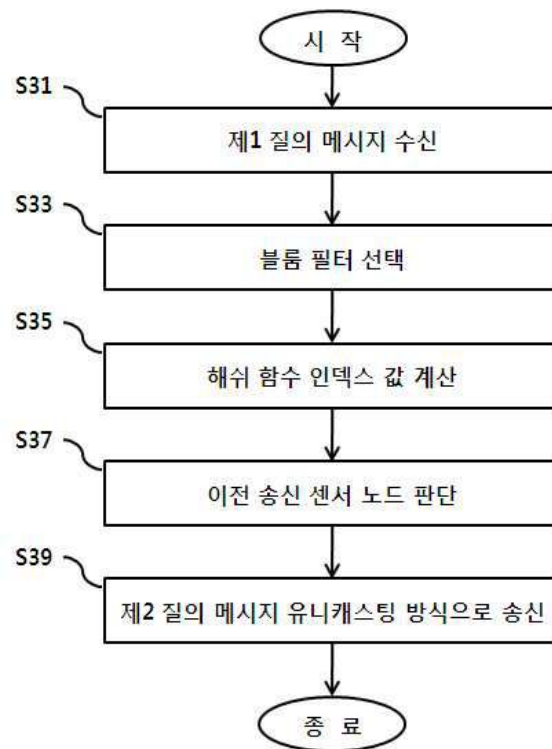
도면5



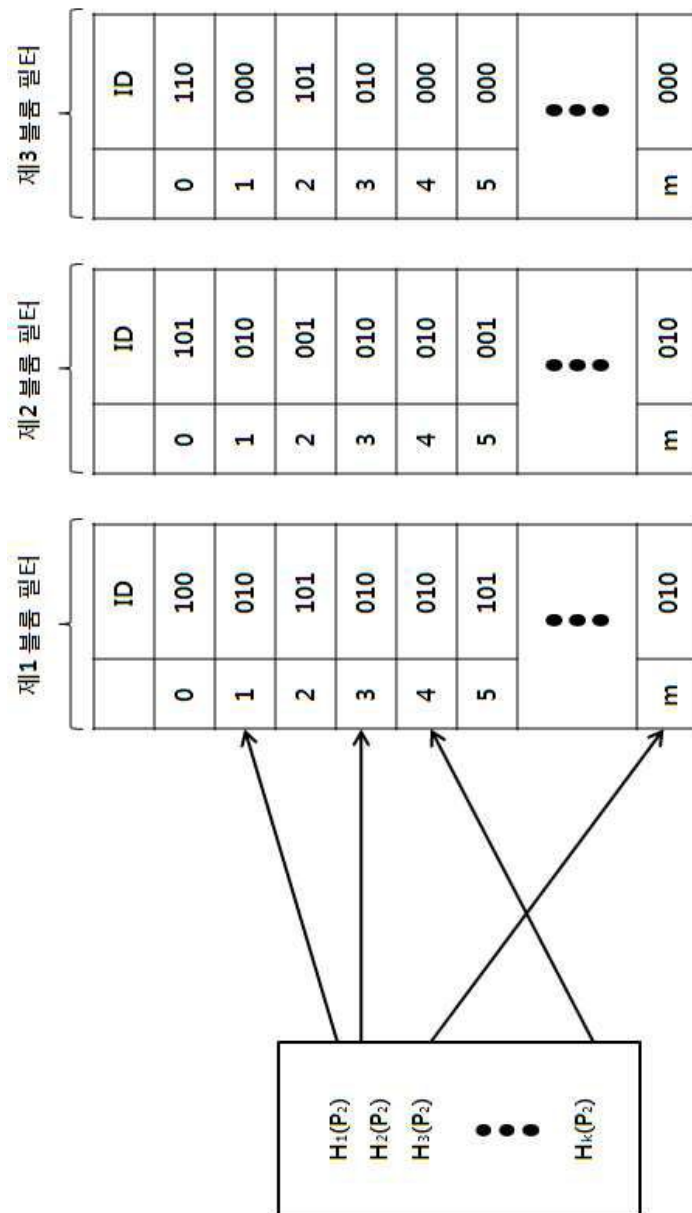
도면6



도면7



도면8



도면9

time	블룸필터 ID
t1	01
t2	10
	11