(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0105425
(43) 공개일자 2008년12월04일

(51) Int. Cl.
H04L 12/56 (2006.01) *H04L 29/02* (2006.01)
H04L 9/00 (2006.01)
(21) 출원번호 10-2007-0052988
(22) 출원일자 2007년05월31일
심사청구일자 2008년05월19일

(71) 출원인
이형우
경기도 용인시 기흥구 중동 성산마을서해그랑블 3101동 501호
한신대학교 산학협력단
경기 오산시 양산동 한신대학교내
충남대학교산학협력단
대전광역시 유성구 궁동 220번지 충남대학교
(72) 발명자
이형우
경기도 용인시 기흥구 중동 성산마을서해그랑블 3101동 501호
(74) 대리인
특허법인태동

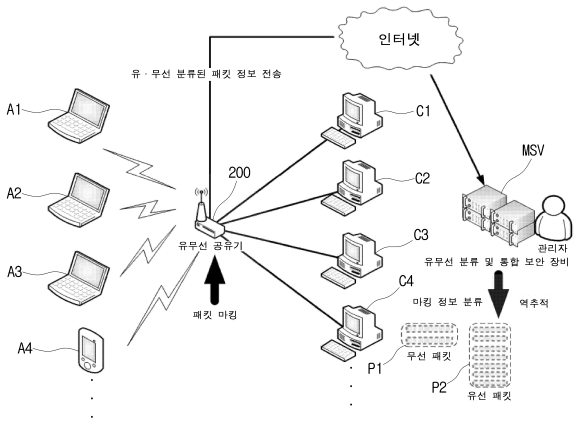
전체 청구항 수 : 총 14 항

(54) 패킷마킹을 통한 유/무선 패킷 분류 방법 및 시스템, 그를이용한 무선사용자 정보추출/역추적 방법 및 시스템

(57) 요 약

본 발명은 패킷마킹을 통한 유/무선 패킷 분류 시스템에 관한 것으로서, 유/무선인터페이스부를 통해 접근한 유/무선 단말기 혹은 컴퓨터 사용자의 유/무선 패킷을 접수하고 유/무선 패킷을 구분하여 전송하는 유/무선 리스너(Listener) 모듈; 상기 유/무선 리스너모듈을 통해 전송된 무선패킷의 특정필드에 마킹하는 패킷 마킹(Packet Marking) 모듈; 상기 패킷 마킹모듈로 부터 마킹된 무선 패킷을 외부연결인터페이스부를 통해 재전송하는 전송모듈;을 포함하여 이루어지는 유/무선 액세스포인트;와 상기 유/무선 액세스포인트로부터 전달된 유/무선 패킷을 분류하여 저장하는 관리자서버;를 포함하여 이루어진 것을 특징으로 한다.

대 표 도 - 도5



특허청구의 범위

청구항 1

패킷마킹을 통한 유/무선 패킷 분류 시스템에 있어서,

유/무선인터페이스부를 통해 접근한 유/무선 단말기 혹은 컴퓨터 사용자의 유/무선 패킷을 접수하고 유/무선 패킷을 구분하여 전송하는 유/무선 리스너(Listener) 모듈;

상기 유/무선 리스너모듈을 통해 전송된 무선패킷의 특정필드에 마킹하는 패킷 마킹(Packet Marking) 모듈;

상기 패킷 마킹모듈로 부터 마킹된 무선 패킷을 외부연결인터페이스부를 통해 재전송하는 전송모듈;을 포함하여 이루어지는 유/무선 액세스포인트;와

상기 유/무선 액세스포인트로부터 전달된 유/무선 패킷을 분류하여 저장하는 관리자서버;를 포함하여 이루어진 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 2

패킷마킹을 통한 유/무선 패킷 분류 시스템에 있어서,

유/무선인터페이스부를 통해 접근한 유/무선 단말기 혹은 컴퓨터 사용자의 유/무선 패킷을 접수하고 유/무선 패킷을 구분하여 전송하는 유/무선 리스너(Listener) 모듈;

상기 유/무선 리스너모듈을 통해 전송된 무선패킷의 특정필드에 무선 패킷임을 표시함과 동시에 역추적을 위한 마킹을 수행하는 패킷 마킹(Packet Marking) 모듈;

상기 패킷 마킹모듈로 부터 마킹된 무선 패킷을 외부연결인터페이스부를 통해 재전송하는 전송모듈;을 포함하여 이루어지는 유/무선 액세스포인트;와

상기 유/무선 액세스포인트로부터 전달된 유/무선 패킷을 분류하여 저장하는 관리자서버;를 포함하여 이루어진 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 패킷 마킹(Packet Marking) 모듈은

상기 유/무선 리스너모듈로부터 전송된 무선 패킷을 접수하는 무선패킷 접수부;

무선패킷을 구분하기 위하여 표시하는 무선패킷 표시부; 및

공격자 역추적을 위하여 상기 구분된 무선패킷에 마킹하는 역추적 마킹부를 포함하여 이루어진 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 4

제 1 항 또는 제 2 항에 있어서,

상기 무선패킷 표시부는 TOS필드(precedence 3bit, TOS 4bit)중, 마지막의 1bit와 Flags(second bit - Don't Fragment, third bit - More Fragment) 필드의 사용하지 않는 첫 번째 필드를 사용하여 표시하는 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 5

제 3 항에 있어서,

상기 역추적 마킹부는 무선패킷 마킹을 위한 특정비트를 특정비트로 만들어주며 추출하기 위한 비트추출부, 상기 비트추출부로부터 추출된 비트들을 연산하여 역추적을 위한 비트를 생성하는 역추적마킹정보 생성부, 상기 생성된 역추적을 위한 비트를 ID필드에 입력하는 역추적 정보입력부를 포함하여 이루어진 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 6

제 5 항에 있어서,

상기 역추적 마킹부의 비트추출부를 통해 추출된 비트들은 기존 16bit의 ID필드의 값, 32bit의 AP의 IP, 48bit의 클라이언트의 Mac Address로 구성된 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 7

제 5 항에 있어서,

상기 역추적마킹정보 생성부는 상기 비트추출부를 이용항 추출된 비트들을 통해 역추적마킹정보를 생성하되,

ID와 AP의 IP는 문자열을 합쳐주는 함수를 이용하여 48bit로 만들어주며 합쳐진 48bit는 클라이언트의 Mac Address와 함께 XOR를 통해 다시 새로운 48bit의 값을 만들고, 만들어진 48bit의 값은 16bit씩 3개의 값으로 나누어 다시 합하는 기능을, 즉, 폴딩(folding)을 수행하여 16bit를 생성하는 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 8

제 5 항에 있어서,

상기 역추적정보 입력부는 최종적으로 생성된 16bit의 값(ID'값)을 다시 기존 ID필드에 입력하는 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 9

제 1 항 또는 제 2 항에 있어서,

상기 전송(Transport) 모듈은 마킹된 패킷을 재전송하는 모듈로서 변환정보 접수부와 재전송부를 포함하여 이루어지며, 즉 상기 패킷마킹 모듈로부터 상기 변환정보접수부를 통해 전달받은 패킷을 재전송부에 의해 다시 AP의 외부연결인터페이스부를 통해 관리자서버로 재전송을 수행하는 것을 패킷마킹을 통한 유/무선 패킷 분류 시스템.

청구항 10

유/무선인터페이스부를 통해 접근한 유/무선 단말기 혹은 컴퓨터 사용자의 유/무선 패킷을 접수하고 유/무선 패킷을 구분하여 전송하는 유/무선 리스너(Listener) 모듈;

상기 유/무선 리스너모듈을 통해 전송된 무선패킷의 특정필드에 마킹하는 패킷 마킹(Packet Marking) 모듈;

상기 패킷 마킹모듈로 부터 마킹된 무선 패킷을 외부연결인터페이스부를 통해 재전송하는 전송모듈;을 포함하여 이루어지는 유/무선 액세스포인트;와

상기 유/무선 액세스포인트로부터 전달된 유/무선 패킷을 분류하여 저장하는 관리자서버;를 포함하여 이루어지되,

무선공격발생시, 해당 공격자(클라이언트)의 ID헤더 필드를 통해 해당 무선공격자를 추적하되, 전송된 IP 헤더의 ID' 값을 추출하고, 관리자서버(MSV)의 저장부에 저장된 무선패킷데이터 중에서 해당 ID'에 대응하는 클라이언트 MAC값을 비교하여, 해당 무선공격자 클라이언트의 MAC주소를 추출하는 것을 특징으로 하는 제 2 항의 패킷마킹을 통한 유/무선 패킷 분류 시스템을 이용한 무선사용자 정보추출/ 역추적 시스템.

청구항 11

패킷마킹을 통한 유/무선 패킷 분류 방법에 있어서,

유/무선 AP에서는 먼저 유/무선 단말기로부터 유/무선 네트워크 접속요청이 있는 경우, 유/무선 패킷을 캡처하는 제 1 단계;

상기 제 1 단계에서 캡처된 패킷이 유선 패킷인 경우에는 외부연결인터페이스부를 통해 관리자서버(MSV)로 패킷 전송을 수행하여 그냥 통과시키며, 무선 패킷인 경우에는, 무선패킷 표시부를 무선 패킷에 특정표시를 수행한

후 전송하는 제 2 단계;

상기 전송된 유선 및 무선 패킷을 분류하여 저장하는 제 3 단계;를 포함하여 이루어진 것을 특징으로 하는 패킷 마킹을 통한 유/무선 패킷 분류 방법.

청구항 12

패킷마킹을 통한 유/무선 패킷 분류 방법에 있어서,

유/무선 AP에서는 먼저 유/무선 단말기로부터 유/무선 네트워크 접속요청이 있는 경우, 유/무선 패킷을 캡처하는 제 1 단계;

상기 제 1 단계에서 캡처된 패킷이 유선 패킷인 경우에는 외부연결인터페이스부를 통해 관리자서버(MSV)로 패킷 전송을 수행하여 그냥 통과시키며, 무선 패킷인 경우에는, 무선패킷 표시부를 통해 무선패킷의 특정위치에 무선 패킷임을 나타내는 표시를 수행함과 동시에 역추적을 위한 마킹을 수행하여 전송하는 제 2 단계;

상기 전송된 유선 및 무선 패킷을 분류하여 저장하는 제 3 단계;를 포함하여 이루어진 패킷마킹을 통한 유/무선 패킷 분류 방법.

청구항 13

제 12 항에 있어서,

상기 제 2 단계에서의 역추적을 위한 마킹은

역추적 마킹부의 비트추출부를 통해 무선패킷 마킹을 위한 특정비트를 특정비트로 만들어주는 제 4 단계;

상기 비트추출부로부터 추출된 비트들을 역추적마킹정보 생성부를 통해 연산하여 역추적을 위한 비트를 생성하는 제 5 단계;

역추적 정보입력부를 통해 상기 생성된 역추적을 위한 비트(ID'값)를 ID 값 필드에 바꾸어 입력하는 제 6 단계;를 포함하여 이루어진 것을 특징으로 하는 패킷마킹을 통한 유/무선 패킷 분류 방법.

청구항 14

무선공격이 있는 경우, 전송된 IP 헤더의 ID 필드를 추출하는 제 7 단계;

관리자서버(MSV)의 저장부에 저장된 무선패킷데이터 중에서 ID'값에 대응하는 클라이언트 MAC값을 비교하는 제 8 단계; 및

해당 무선공격자 클라이언트의 MAC주소를 추출하는 제 9 단계를 포함하여 이루어진 것을 특징으로 하는 제 12 항의 패킷마킹을 통한 유/무선 패킷 분류 방법을 이용한 무선사용자 정보추출/역추적 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<27> 본 발명은 패킷 마킹을 이용한 유/무선 패킷 분류 방법, 시스템 및 그를 이용한 무선사용자 정보추출/역추적 방법 및 시스템에 관한 것으로, 더욱 상세하게는 유무선 액세스포인트에서 아이피 헤더의 패킷 마킹기법을 적용하여 유무선 트랙픽을 구분하는 패킷 마킹을 이용한 유/무선 패킷 분류 방법, 시스템 및 그를 이용한 무선사용자 정보추출/역추적 방법 및 시스템에 관한 것이다.

<28> 도 1은 티오에스 플래그 세부내역을 나타낸 도면이고, 도 2는 아이피 티오에스 관련 권고안을 나타낸 도면이고, 도 3은 각 프로토콜에 대한 티오에스 권고안을 나타낸 도면이다.

<29> 도 1 내지 도 3을 참조하면, 티오에스(Type of Servic: 이하 ToS라 함)는 패킷의 아이피(Internet Protocol:이하 IP라 함) 헤더(header) 내에 있는 8 비트 필드를 말하며, 이는 요구되는 서비스 유형을 나타내는데 사용된다. 주로 IP 데이터그램이 라우터에서 어떻게 처리되어야하는지를 정의하고 있다. 이하 설명한다.

<30> * 우선순위 설정용(3bit) (※오늘날에는 드물게 사용되고 있음)

<31> - Bit 0-2 : Precedence (우선순위 8단계)

<32> 000 : Routine (Normal)

<33> 001 : Priority

<34> 010 : Immediate

<35> 011 : Flash

<36> 100 : Flash Override

<37> 101 : Critical

<38> 110 : Internetwork Control (OSPF에서 셋팅됨)

<39> 111 : Network Control

<40> *TOS 설정용(4bit)

<41> - Bit 3 : Delay (지연) (0 보통의 지연, 1 높은 지연)

<42> - Bit 4 : Throughput (처리율) (0 보통, 1 높음)

<43> - Bit 5 : Reliability (신뢰성) (0 보통, 1 높음)

<44> - Bit 6 : Minimum Cost (최소비용)

<45> *사용안함(1bit)

<46> - Bit 7 : 항상 0으로 셋팅됨

<47> 도 4는 종래 기술에 따른 유/무선 패킷을 통한 유/무선 통신접속과정을 나타낸 시스템 구성도이다.

<48> 도 4를 참조하면, 현재까지 개발된 기존의 무선 액세스포인터(Access Pointer:이하 AP라 함) 및 유/무선 공유기의 경우 유/무선의 구분없이 디에이치씨피(Dynamic Host Configuration Protocol:이하 DHCP라 함) 서버를 이용한 사설 IP를 할당해 관리했다. 그러나, 무선 네트워크의 트래픽은 무선 사용자 컴퓨터 혹은 단말기(A1~A4, C1~C4는 유선사용카 컴퓨터를 나타냄)들이 AP 혹은 유/무선 공유기(2)를 통과한 뒷단에서는 무선 맥(MAC)헤더의 삭제로 관리자(서버 혹은 컴퓨터)(MSV)의 입장에서는 어떤 패킷이 무선으로부터 온 것인지 즉, 유/무선 트래픽의 구분이 불가능한 문제점이 있었다. 최근 무선 네트워크 특성을 이용한 특화된 공격의 증가로 인하여 유/무선 트래픽의 분류 과정이 선행되지 않고서는 효과적인 공격 탐지가 어려운 실정이다.

<49> 현재 무선 네트워크 침입의 형태와 기술의 다양성이 점차 증가되고 있고 그에 따른 공격 시도 및 침입으로 인한 피해가 증가하고 있다. 그러나 무선 네트워크 침입에 특화된 침임 탐지 기술은 미흡한 실정이다.

<50> 즉, 기존의 AP에서는 패킷마킹 기술을 제공하지 않기 때문에 서버에서 공격이 발생시 이 공격이 유선을 통한 공격인지 무선을 통한 공격인지 판단이 불가능한 문제점이 있었고 더군다나 무선공격자의 위치를 파악하기는 현실적으로 불가능한 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

<51> 본 발명의 목적은 AP 혹은 유/무선 공유기 장비에 유/무선 패킷 중 무선패킷의 티오에스(ToS)필드에 무선 패킷을 구분할 수 있는 마킹을 통하여 무선네트워크를 통한 사용자 단말기의 무선패킷을 분류하고 이를 통해 무선네트워크를 이용한 공격자를 쉽게 파악하여 역추적할 수 있는 패킷마킹을 통한 유/무선 패킷 분류 방법 및 그를 이용한 무선사용자 정보추출/역추적 방법을 제공함에 있다.

<52> 본 발명의 또 다른 목적은 AP 혹은 유/무선 공유기 장비에 유/무선 패킷 중 무선패킷의 티오에스(ToS)필드에 무선 패킷을 구분할 수 있는 마킹을 통하여 무선네트워크를 통한 사용자 단말기의 무선패킷을 분류하고 이를 통해 무선네트워크를 이용한 공격자를 쉽게 파악하여 역추적할 수 있는 패킷마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템을 제공함에 있다.

발명의 구성 및 작용

<53> 상기한 바와 같은 목적을 달성하기 위하여, 본 발명에 따른 패킷마킹을 통한 유/무선 패킷 분류 시스템은, 유/무선인터페이스부를 통해 접근한 유/무선 단말기 혹은 컴퓨터 사용자의 유/무선 패킷을 접수하고 유/무선 패킷을 구분하여 전송하는 유/무선 리스너(Listener) 모듈; 상기 유/무선 리스너모듈을 통해 전송된 무선패킷의 특정필드에 마킹하는 패킷 마킹(Packet Marking) 모듈; 상기 패킷 마킹모듈로 부터 마킹된 무선 패킷을 외부연결인터페이스부를 통해 재전송하는 전송모듈;을 포함하여 이루어지는 유/무선 액세스포인트;와 상기 유/무선 액세스포인트로부터 전달된 유/무선 패킷을 분류하여 저장하는 관리자서버;를 포함하여 이루어진 것을 특징으로 한다.

<54> 본 발명의 또 다른 측면에 있어서, 패킷마킹을 통한 유/무선 패킷 분류 시스템은, 유/무선인터페이스부를 통해 접근한 유/무선 단말기 혹은 컴퓨터 사용자의 유/무선 패킷을 접수하고 유/무선 패킷을 구분하여 전송하는 유/무선 리스너(Listener) 모듈; 상기 유/무선 리스너모듈을 통해 전송된 무선패킷의 특정필드에 무선 패킷임을 표시함과 동시에 역추적을 위한 마킹을 수행하는 패킷 마킹(Packet Marking) 모듈; 상기 패킷 마킹모듈로 부터 마킹된 무선 패킷을 외부연결인터페이스부를 통해 재전송하는 전송모듈;을 포함하여 이루어지는 유/무선 액세스포인트;와 상기 유/무선 액세스포인트로부터 전달된 유/무선 패킷을 분류하여 저장하는 관리자서버;를 포함하여 이루어진 것을 특징으로 한다.

<55> 본 발명의 또 다른 측면에 있어서, 패킷마킹을 통한 유/무선 패킷 분류 시스템을 이용한 무선공격자 정보추출 및 역추적 시스템은 유/무선인터페이스부를 통해 접근한 유/무선 단말기 혹은 컴퓨터 사용자의 유/무선 패킷을 접수하고 유/무선 패킷을 구분하여 전송하는 유/무선 리스너(Listener) 모듈; 상기 유/무선 리스너모듈을 통해 전송된 무선패킷의 특정필드에 마킹하는 패킷 마킹(Packet Marking) 모듈; 상기 패킷 마킹모듈로 부터 마킹된 무선 패킷을 외부연결인터페이스부를 통해 재전송하는 전송모듈;을 포함하여 이루어지는 유/무선 액세스포인트;와 상기 유/무선 액세스포인트로부터 전달된 유/무선 패킷을 분류하여 저장하는 관리자서버;를 포함하여 이루어지되, 무선공격발생시, 해당 공격자(클라이언트)의 ID헤더 필드(ID'값)를 통해 해당 무선공격자를 추적하되, 전송된 IP 헤더의 ID 필드(ID'값)를 추출하고, 관리자서버(MSV)의 저장부에 저장된 무선패킷데이터 중에서 해당 ID'값에 대응하는 클라이언트 MAC값을 비교하고, 해당 무선공격자 클라이언트의 MAC주소를 추출하는 것을 특징으로 하는 것을 특징으로 한다.

<56> 본 발명의 또 다른 측면에 있어서, 패킷마킹을 통한 유/무선 패킷 분류 방법은, 유/무선 AP에서는 먼저 유/무선 단말기로부터 유/무선 네트워크 접속요청이 있는 경우, 유/무선 패킷을 캡처하는 제 1 단계; 상기 제 1 단계에서 캡처된 패킷이 유선 패킷인 경우에는 외부연결인터페이스부를 통해 관리자서버(MSV)로 패킷 전송을 수행하여 그냥 통과시키며, 무선 패킷인 경우에는, 무선패킷 표시부를 무선 패킷에 특정표시를 수행한 후 전송하는 제 2 단계; 상기 전송된 유선 및 무선 패킷을 분류하여 저장하는 제 3 단계;를 포함하여 이루어진 것을 특징으로 한다.

<57> 본 발명의 또 다른 측면에 있어서, 패킷마킹을 통한 유/무선 패킷 분류 방법은, 유/무선 AP에서는 먼저 유/무선 단말기로부터 유/무선 네트워크 접속요청이 있는 경우, 유/무선 패킷을 캡처하는 제 1 단계; 상기 제 1 단계에서 캡처된 패킷이 유선 패킷인 경우에는 외부연결인터페이스부를 통해 관리자서버(MSV)로 패킷 전송을 수행하여 그냥 통과시키며, 무선 패킷인 경우에는, 무선패킷 표시부를 통해 무선패킷의 특정위치에 무선패킷임을 나타내는 표시를 수행함과 동시에 역추적을 위한 마킹을 수행하여 전송하는 제 2 단계; 상기 전송된 유선 및 무선 패킷을 분류하여 저장하는 제 3 단계;를 포함하여 이루어진 것을 특징으로 한다.

<58> 본 발명의 또 다른 측면에 있어서, 패킷마킹을 통한 유/무선 패킷 분류 방법을 이용한 무선사용자 정보추출/역추적 방법은 무선공격이 있는 경우, 전송된 IP 헤더의 ID 필드를 추출(ID'값획득)하는 제 7 단계; 관리자서버(MSV)의 저장부에 저장된 무선패킷데이터 중에서 해당 ID'값에 대응하는 클라이언트 MAC값을 비교하는 제 8 단계; 및 해당 무선공격자 클라이언트의 MAC주소를 추출하는 제 9 단계를 포함하여 이루어진 것을 특징으로 한다.

<59> 이하, 본 발명에 따른 패킷마킹을 통한 유/무선 패킷 분류 방법 및 시스템, 그를 이용한 무선사용자 정보추출/역추적 방법 및 시스템에 대하여 첨부도면을 참조로 상세히 설명한다.

<60> 본 발명에서는 AP 및 유/무선 공유기와 같이 무선 통신을 제공하는 시스템에서 유/무선 트래픽을 판별할 수 있도록 도와주는 모듈을 추가하여 유무선 통신에 대한 판별을 향상시킨다.

<61> 공격으로 판단된 패킷의 경우 정보추출 및 역추적을 통하여 공격 패킷에 마킹된 데이터와 공격의 중간지점이 된 유무선 통합장비의 정보를 비교하여 공격에 대한 증거 및 자료로 사용한다.

<62> 유/무선 트래픽 분류 기술은 유/무선 네트워크에 특화된 침입탐지 기술 개발을 위해 선행되어야 하는 기술이다.

<63> 유/선 트래픽 구분을 위한 패킷마킹에서는 무선트래픽을 제공하는 AP 혹은 유무선 공유기(이하 유/무선 AP라 함)에서 시스템을 통과하는 모든 패킷에 마킹을 하게 된다.

<64> 유/무선 AP(200)를 통해 전송되는 무선 트래픽에 마킹을 함으로써 유·무선을 판별한다.

<65> 네트워크 침해가 발생 시 유/무선 망에 특화된 참고 데이터 분류 역할을 한다.

<66> 무선 액세스포인트 기능에 패킷마킹을 적용한 임베디드 리눅스 기반 무선 액세스포인트를 개발하였다.

<67> 본 발명에서는 공개된 여러 펌웨어(firmware) 중 최소 기능만 포함하는 openWRT를 포팅하고 패킷마킹 기능을 소프트웨어적으로 추가한다.

<68> 도 5는 본 발명에 따른 패킷마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적을 위한 시스템 구성도이다.

<69> 도 5를 참조하면, 무선 네트워크의 트래픽은 무선 사용자 컴퓨터 혹은 단말기(A1~A4)들이 AP 혹은 유/무선 공유기(200)에서 무선 패킷마킹되고 이후 관리자(서버 혹은 컴퓨터)(MSV)에 전달되어, 관리자는 무선 패킷(P1)과 유선 패킷(P2)를 분류하여 저장하므로 어떤 패킷이 무선으로부터 온 것인지 즉, 유/무선 트래픽의 구분이 가능하다.

<70> 도 6은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 과정을 개략적으로 나타낸 시스템 구성도이다.

<71> 도 6을 참조하면, 유/무선 AP(200)를 지나는 유선 및 무선 패킷 중 무선패킷에 패캣 마킹과정을 수행하여 관리자(서버)(MSV)에는 특정 유선 단말기 및 무선 단말기의 패킷을 분류하여 저장한다.

<72> 도 7은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 과정을 순차적으로 나타낸 개념도이고, 도 8은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 유/무선 공유기의 내부구성을 개략적으로 나타낸 블록도이고, 도 9는 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 네트워크별 패킷 마킹 규칙의 예를 나타낸 도표이고, 도 10a는 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 역추적을 위한 마킹정보생성과정의 예를 나타낸 도면이고, 도 10b는 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 역추적을 위한 마킹정보생성과정 중 폴딩과정의 예를 나타낸 도면이고, 도 11은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서의 아이피헤더의 구조를 나타낸 도면이다.

<73> 도 7 내지 도 11을 참조하면, 먼저 리스너(Listener)부분은 802.11 b/g 채널 호핑 프로토콜을 가지며, Level 2 무선 트래픽 모니터링을 실시하되, 프로브 요청(probe request), 프로브 응답(probe respose) 및 비콘 프레임(beacon frame)등을 모니터링하며, 환경정보 설정을 동기화한다. 여기서 사용될 툴 체인 구성 및 모니터링 모듈이 개발된다. MIPSEL 아키텍처 기반으로 하며, 크로스 컴파일 환경으로 리눅스 페도라(fedora) 코어3 환경이다.

<74> 또한, 패킷 마킹 부분은 패킷을 분석하고 무선트래픽 탐지/마킹기능을 수행하며, 이를 위하여 무선트래픽 마킹 모듈이 개발되었다. 또한 맥 헤더의 정보를 로드/변경하는 기능과, 유/무선 네트워크 특징을 추출하며, 분류에 따른 마킹을 수행한다. 또한 역추적을 위한 마킹모듈이 개발되었다. 역추적을 위한 마킹모듈이 또한 개발되었으며, ToS와 Flag필드의 마킹을 수행하며 동시에 ID필드와 마킹을 수행한다.

<75> 또한, 전송(transport) 부분은 마킹된 패킷 전송모듈이 개발되었고, 마킹된 유/무선 네트워크패킷을 전달한다.

<76> 본 발명의 패킷마킹을 통한 유/무선 패킷 분류 시스템 및 무선 사용자 정보추출/역추적 시스템에서 유/무선 AP(200)는 크게 세가지 모듈로 구성한다.

<77> * 유/무선 리스너(Listener) 모듈(240): 유/무선 단말기 혹은 컴퓨터(A1,C1) 사용자가 유/무선인터페이스부(210,220)를 통해 접근한 경우, 유/무선 패킷 캡처부(242)가 해당 유/무선 트래픽을 캡처하는 기능을 수행한다. 기본적으로는, 네트워크 기반 프로그래밍 중 네트워크 리스닝(Listening)모드가 있으며 그 기능을 통해 무선네트워크를 이용하는 모든 패킷을 캡처 할 수가 있다. 유선의 경우 그냥 AP의 외부연결인터페이스부(230)를 통해 통과시키며 무선 패킷의 경우 차단을 시키고 무선/패킷 필터/전송부(244)를 통해 패킷마킹모듈(250)로 전달하게 된다.

<78> * 패킷 마킹(Packet Marking) 모듈(250): 유/무선 트래픽의 구분 및 역추적을 위한 패킷마킹 기능을

수행하는데, 유무선통합장비에서는 유선통신과 무선통신을 분류하기 위한 패킷마킹과 역추적을 위한 패킷마킹 과정을 거치게 된다.

<79> 무선패킷 접수부(252)는 상기 유/무선 리스너모듈(140)로부터 전송된 무선 패킷을 접수한다.

<80> 무선패킷 표시부(254)는 무선패킷을 구분하기 위하여 표시하는 과정을 수행하는데, 즉, 유선통신과 무선통신을 분류하기 위한 패킷마킹으로서, TOS필드(precedence 3bit, TOS 4bit)중 현재 사용하고 있지 않은 마지막의 1bit와 Flags(second bit - Don't Fragment, third bit - More Fragment) 필드의 사용하지 않는 첫 번째 필드를 사용하여 표시하게 된다.

<81> TOS필드의 사용하지 않는 마지막 필드는 기본적으로 0bit가 구성되며 여기서 1의 값을 가질 경우 패킹마킹 기술이 적용된 패킷이라는 것으로 판단한다. 그리고 Flags의 필드에서의 첫 번째 1bit가 1일때 무선으로 판단하게 된다. TOS의 필드와 Flags의 필드를 합쳐서 볼 경우 00이거나 01, 10일 경우에는 일반적인 패킷으로 간주하며 11일 경우 무선패킷으로 간주한다.

<82> 실제로 사용하지 않는 패킷이기 때문에 두 필드 모두 1의 값을 가질 경우는 매우 적으며 단순히 경우의 수만으로도 25%의 확률을 가진다. 그렇기에 11의 경우에는 본 특허의 기술이 적용된 된 패킷으로 판단할 수 있는 것이다.

<83> 또한, 역추적 마킹부(256)는 무선패킷 마킹을 위한 특정비트를 특정비트로 만들어주며 추출하기 위한 비트추출부(256a), 상기 비트추출부(256a)로부터 추출된 비트들을 연산하여 역추적을 위한 비트를 생성하는 역추적마킹정보 생성부(256b), 상기 생성된 역추적을 위한 비트를 ID필드에 입력하는 역추적 정보입력부(256c)를 포함하여 이루어진다. 즉, 역추적을 위한 기술에서는 ID필드의 내용을 바꾸어 넣는다.

<84> 구체적으로, 기존의 ID값에 따라 통신이 이루어지기 때문에 ID필드의 값을 기본적으로 이용하며 AP의 IP, 클라이언트의 Mac Address를 이용한다. ID필드는 16bit로 구성되어 있으며 AP의 IP는 32bit, 클라이언트의 Mac Address는 48bit로 구성되어 있는데 이를 역추적 마킹부(256)의 비트추출부(256a)를 통해 추출한다.

<85> 이후, 역추적마킹정보 생성부(256b)를 이용하여 추출된 비트들을 통해 역추적마킹정보를 생성한다. 그 과정은 다음과 같다. 즉, ID와 AP의 IP는 문자열을 합쳐주는 함수를 이용하여 48bit로 만들어주며 합쳐진 48bit는 클라이언트의 Mac Address와 함께 XOR를 통해 다시 새로운 48bit의 값으로 만들어진다. 그렇게 만들어진 48bit의 값은 16bit씩 3개의 값으로 나누어 다시 합하는 기능을 수행한다(도 10참조). 즉, 폴딩(folding)을 수행하여 16bit를 생성한다(도 10b참조). 최종적으로 만들어진 16bit의 값은 역추적마킹부(256)의 역추적정보 입력부(256c)를 통해 다시 ID필드에 입력한다. 이렇게 만들어진 ID필드 값은 기존의 ID필드의 값(ID')에 따라 달라지기 때문에 실제 통신에도 영향을 미치지 않는다.

<86> * 전송(Transport) 모듈(260): 마킹된 패킷을 재전송하는 모듈로서 변환정보 접수부(262)와 재전송부(264)를 포함하여 이루어진다. 즉, 패킷마킹 모듈(250)로부터 전달받은 패킷을 다시 AP의 외부연결인터페이스부(230)를 통해 재전송을 수행한다.

<87> 도 12는 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 패킷 마킹과정을 구체적으로 나타낸 순서도이다.

<88> 도 12를 참조하면, 유/무선 AP(200)에서는 먼저 유/무선 단말기(A1~A4, C1~C4)로부터 유/무선 네트워크 접속요청이 있는 경우(ST-2), 유/무선 패킷을 캡처한다(ST-4). 상기 단계 ST-4의 판단결과, 유선 패킷인 경우에는 외부연결인터페이스부(230)를 통해 관리자서버(MSV)로 패킷 전송(ST-10)을 수행하여 그냥 통과시키며, 무선 패킷인 경우에는, 무선 신호 판별(혹은 분류) 및 역추적을 위한 마킹단계를 수행한 후(ST-8) 패킷 전송을 수행한다.

<89> 상기 단계 ST-8은, 무선패킷 표시부를 통해 무선패킷을 표시하는 단계와, 역추적 마킹부(256)의 비트추출부(256a)를 통해 무선패킷 마킹을 위한 특정비트를 특정비트로 만들어주는 과정과, 상기 비트추출부(256a)로부터 추출된 비트들을 역추적마킹정보 생성부(256b)를 통해 연산하여 역추적을 위한 비트를 생성하는 과정과, 역추적 정보입력부(256c)를 통해 상기 생성된 역추적을 위한 비트(ID')를 ID 값 필드에 입력하는 과정을 수행함으로써, 역추적을 위한 기술에서는 ID필드의 내용을 바꾸어 넣는 단계를 수행한다.

<90> 이후 전송된 상기 변경된 ID 값 필드는 관리자서버(MSV)에서 별도로 저장되는데(즉, ID'), 즉 해당 ID' 값과 대응되는 클라이언트 맥(MAC)이 함께 분류 저장되어(도 14참조) ID' 값에 대응되는 클라이언트 맥을 통해 이후 비교과정을 진행하여 공격자 클라이언트의 MAC주소를 추출할 수 있다.

<91> 상기 ID'은 본 발명에서 역추적을 위해 생성된 변형된 ID 비트값이다.

<92> 도 13은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 무선사용자 정보추출/역추적을 위한 과정을 나타낸 순서도이다.

<93> 도 13을 참조하면, 무선사용자 정보추출/역추적을 위한 과정에서, 먼저 IP 헤더의 ID 필드를 추출한다(ST-20). 이후 관리자서버(MSV)의 저장부(도시안됨)에 저장된 무선패킷데이터 중에서 해당 ID'에 대응하는 클라이언트 MAC값을 비교한다(ST-22). 이후 해당 무선공격자 클라이언트의 MAC주소를 추출할 수 있다(ST-24).

발명의 효과

<94> 상기 설명한 바와 같이, 본 발명에 따른 패킷마킹을 통한 유/무선 패킷 분류 방법 및 시스템, 그를 이용한 무선사용자 정보추출/역추적 방법 및 시스템에 의하면, IP 헤더(Header) 마킹기법을 이용하여 보안침해사고를 일으키는 공격을 유선과 무선으로 빠르게 분류하며 각기 다른 트래픽(유·무선 트래픽)에 특화된 침입 탐지 기술 효율적으로 분류할 수 있는 효과가 있으며 이를 통해 공격 탐지 성능을 향상시킬 수 있는 효과가 있고 및 역추적 기술에 효과적으로 적용할 수 있는 효과가 있다.

<95> 또한, 내부정보의 유출시 로그를 통해 쉽게 누출이 될 수 있는 무선네트워크를 통한 접속이었는지 판단을 할 수 있는 효과가 있다.

<96> 또한, 네트워크 침해 발생 시 유·무선 네트워크에 적합한 대응책을 수립 할 수 있으며 수사에 증거자료로 사용할 수 있는 효과가 있다.

도면의 간단한 설명

<1> 도 1은 티오에스 플래그 세부내역을 나타낸 도면이다.

<2> 도 2는 아이피 티오에스 관련 권고안을 나타낸 도면이다.

<3> 도 3은 각 프로토콜에 대한 티오에스 권고안을 나타낸 도면이다.

<4> 도 4는 종래 기술에 따른 유/무선 패킷을 통한 유/무선 통신접속과정을 나타낸 시스템 구성도이다.

<5> 도 5는 본 발명에 따른 패킷마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적을 위한 시스템 구성도이다.

<6> 도 6은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 과정을 개략적으로 나타낸 시스템 구성도이다.

<7> 도 7은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 과정을 순서적으로 나타낸 개념도이다.

<8> 도 8은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 유/무선 공유기의 내부구성을 개략적으로 나타낸 블록도이다.

<9> 도 9는 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 네트워크별 패킷 마킹 규칙의 예를 나타낸 도표이다.

<10> 도 10a는 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 역추적을 위한 마킹정보생성과정의 예를 나타낸 도면이다.

<11> 도 10b는 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 정보추출/역추적을 위한 마킹정보생성과정 중 폴딩과정의 예를 나타낸 도면이다.

<12> 도 11은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서의 아이피헤더의 구조를 나타낸 도면이다.

<13> 도 12는 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 패킷 마킹과정을 구체적으로 나타낸 순서도이다.

<14> 도 13은 본 발명에 따른 패킷 마킹을 통한 유/무선 패킷 분류 시스템 및 그를 이용한 무선사용자 정보추출/역추적 시스템에서 무선사용자 역추적을 위한 과정을 나타낸 순서도이다.

<15> 도 14는 전송된 무선 패킷 중에서 관리자서버가 저장하고 있는 테이블을 나타낸 것으로서, 변경된 ID 필드값 및

대응되는 클라이언트 MAC에 관한 데이터를 저장하는 테이블을 나타낸 도면이다.

<16> * 도면의 주요부분에 대한 부호의 설명 *

<17> 200: 유/무선 액세스포인트

<18> 210: 무선 인터페이스부

<19> 220: 유선 인터페이스부

<20> 230: 외부 연결 인터페이스부

<21> 240: 유/무선 리스너 모듈

<22> 250: 패킷마킹 모듈

<23> 252: 무선패킷 접수부

<24> 254: 유선패킷 접수부

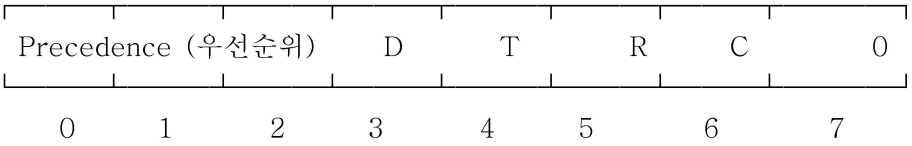
<25> 256: 역추적마킹부

<26> 260: 패킷전송 모듈

도면

도면1

◆ Type Of Service (TOS) Flag (8 bits) 세부내역



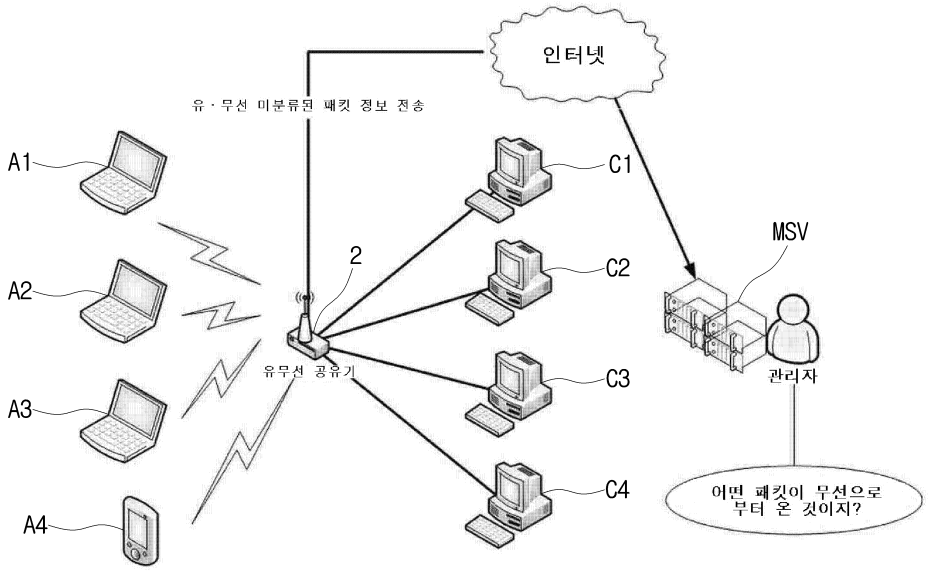
도면2

ToS Value	Description	Reference
0000	Default	[RFC1349]
0001	Minimize Monetary Cost	[RFC1349]
0010	Maximize Reliability	[RFC1349]
0100	Maximize Throughput	[RFC1349]
1000	Minimize Delay	[RFC1349]
1111	Maximize Security	[RFC1349]

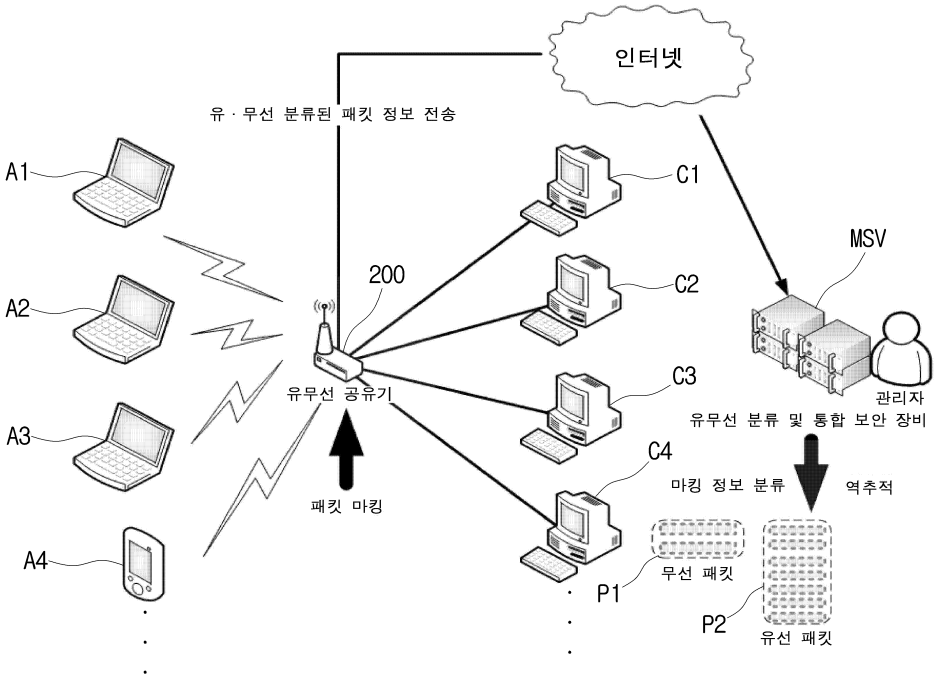
도면3

Protocol		ToS Value	서비스 유형
TELNET		1000	minimize delay
FTP Contro		1000	minimize delay
FTP Data		0100	maximize throughput
TFTP		1000	minimize delay
SMTP Command phase		1000	minimize delay
SMTP DATA phase		0100	maximize throughput
Domain Name Service	UDP Query	1000	minimize delay
	TCP Query	0000	
	Zone Transfer	0100	maximize throughput
NNTP		0001	minimize monetary cost
ICMP Errors		0000	
ICMP Requests		0000	
ICMP Responses			
Any IGP		0010	maximize reliability
EGP		0000	
SNMP		0010	maximize reliability
BOOTP		0000	

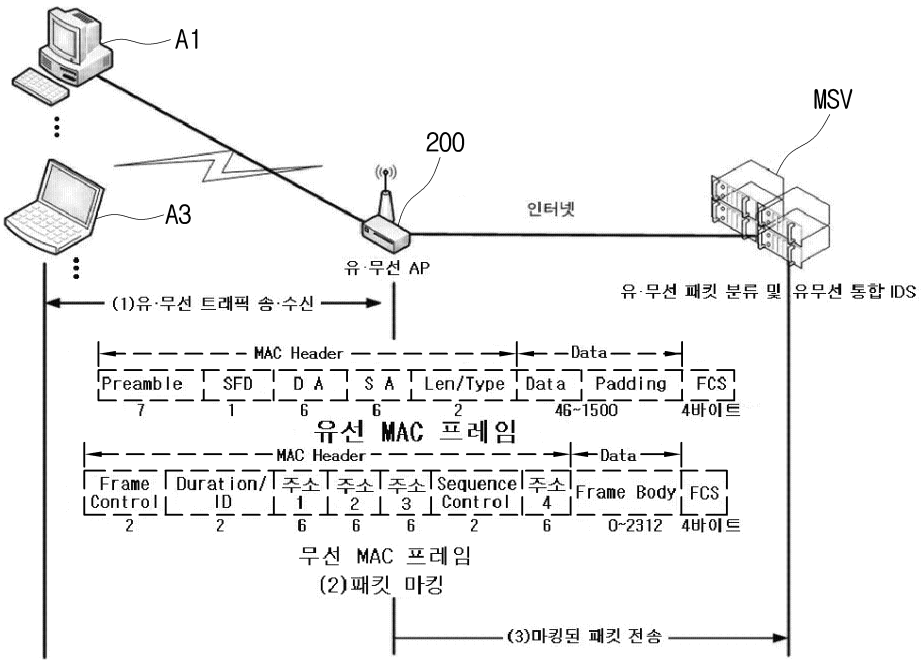
도면4



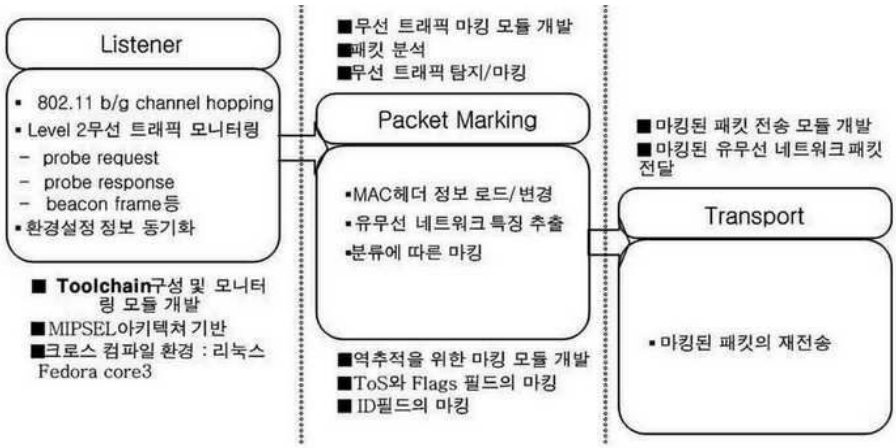
도면5


인터넷
유·무선 분류된 패킷 정보 전송
A1
A2
A3
A4
200
유무선 공유기
패킷 마킹
C1
C2
C3
C4
P1
MSV
관리자
유무선 분류 및 통합 보안 장비
마킹 정보 분류
역추적
무선 패킷
유선 패킷
P2

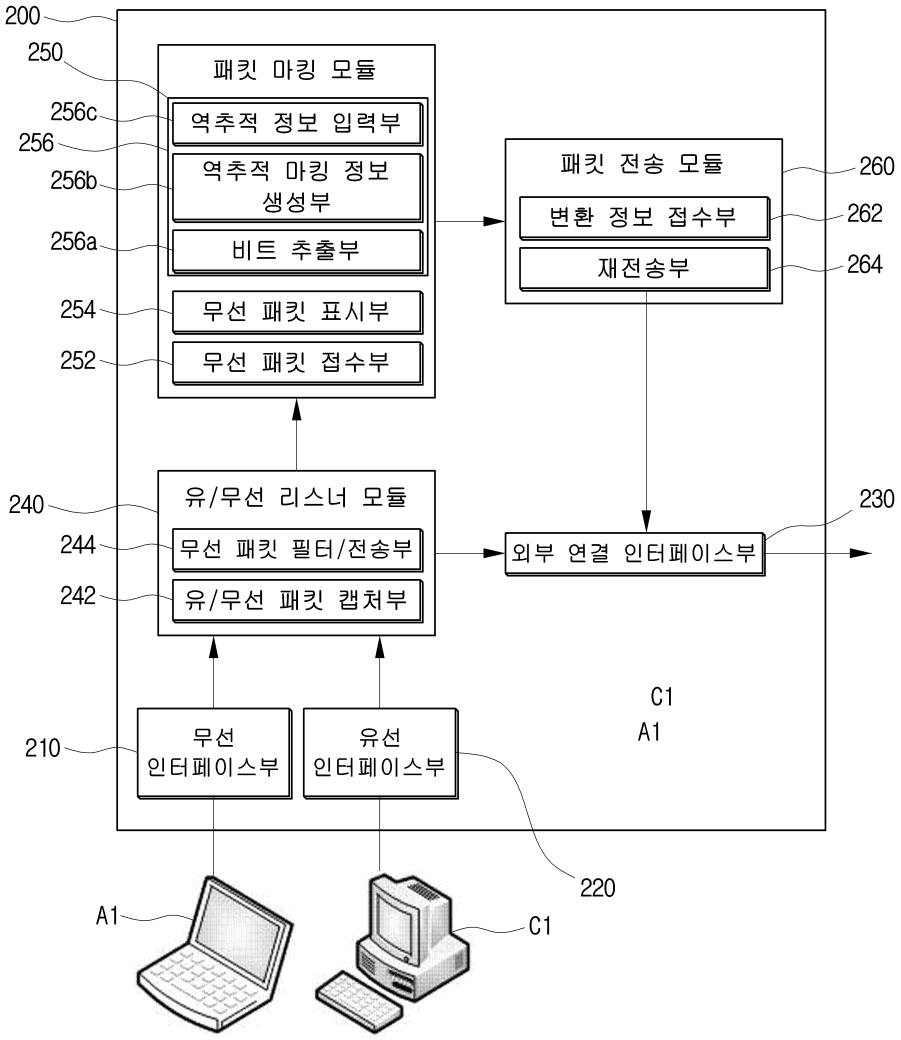
도면6


A1
A3
200
MSV
인터넷
유·무선 AP
유·무선 패킷 분류 및 유무선 통합 IDS
(1)유·무선 트래픽 송·수신
MAC Header
Data
Preamble
SFD
D A
S A
Len/Type
Data
Padding
FCS
7
1
6
6
2
46~1500
4바이트
유선 MAC 프레임
MAC Header
Data
Frame Control
Duration/ ID
주소 1
주소 2
주소 3
Sequence Control
주소 4
Frame Body
FCS
2
2
6
6
6
2
6
0~2312
4바이트
무선 MAC 프레임
(2)패킷 마킹
(3)마킹된 패킷 전송

도면7


Listener
▪ 802.11 b/g channel hopping
▪ Level 2무선 트래픽 모니터링
– probe request
– probe response
– beacon frame등
▪ 환경설정 정보 동기화
■ Toolchain구성 및 모니터링 모듈 개발
■MIPSEL아키텍처 기반
■크로스 컴파일 환경 : 리눅스 Fedora core3
■무선 트래픽 마킹 모듈 개발
■패킷 분석
■무선 트래픽 탐지/마킹
Packet Marking
▪MAC헤더 정보 로드/변경
▪유무선 네트워크 특징 추출
▪분류에 따른 마킹
■역추적을 위한 마킹 모듈 개발
■ToS와 Flags 필드의 마킹
■ ID필드의 마킹
■마킹된 패킷 전송 모듈 개발
■마킹된 유무선 네트워크패킷 전달
Transport
▪ 마킹된 패킷의 재전송

도면8


200
250
패킷 마킹 모듈
256c
역추적 정보 입력부
256
256b
역추적 마킹 정보 생성부
256a
비트 추출부
254
무선 패킷 표시부
252
무선 패킷 접수부
패킷 전송 모듈
260
변환 정보 접수부
262
재전송부
264
240
유/무선 리스너 모듈
244
무선 패킷 필터/전송부
242
유/무선 패킷 캡처부
230
외부 연결 인터페이스부
C1
A1
210
무선 인터페이스부
유선 인터페이스부
220
A1
C1

도면9

네트워크 분류	ToS	Flags
일반네트워크	0	0
일반네트워크	0	1
일반네트워크	1	0
무선네트워크(802.11)	1	1

도면10a

ID필드 16bit

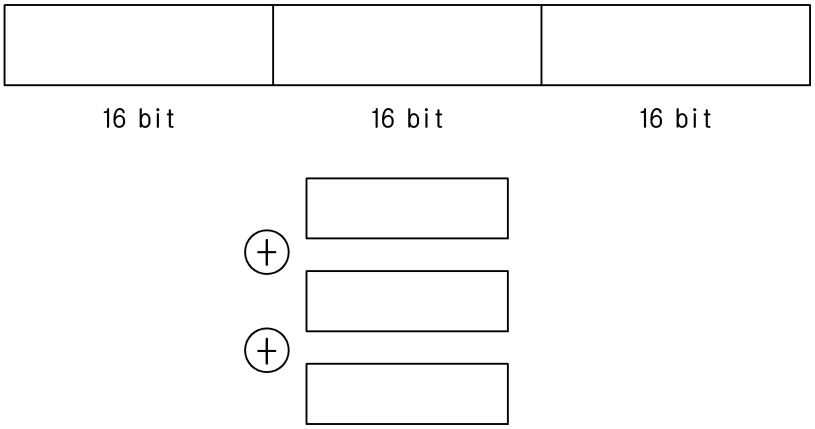
AP's IP 32bit

Client's Mac Address 48bit

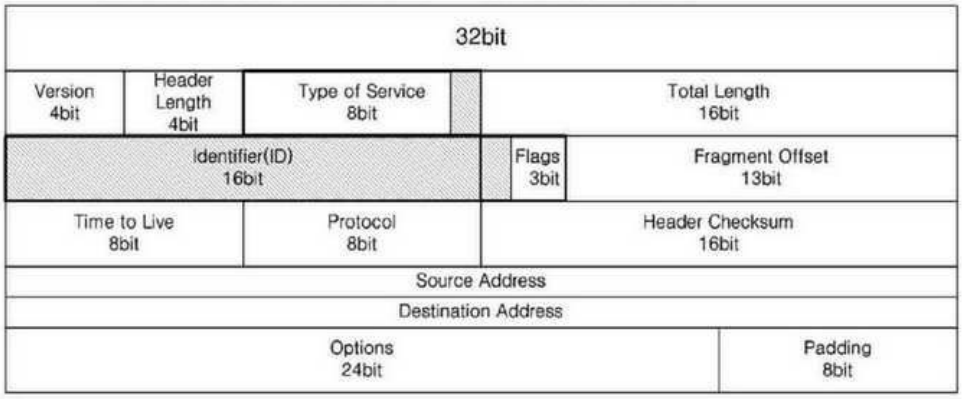
$$48bit_variable=(ID_{(16)}|AP_{IP(32)})\oplus Client_{MAC(48)}$$

$$16bit_variable=sum(divide_3part(48bit_variable))$$

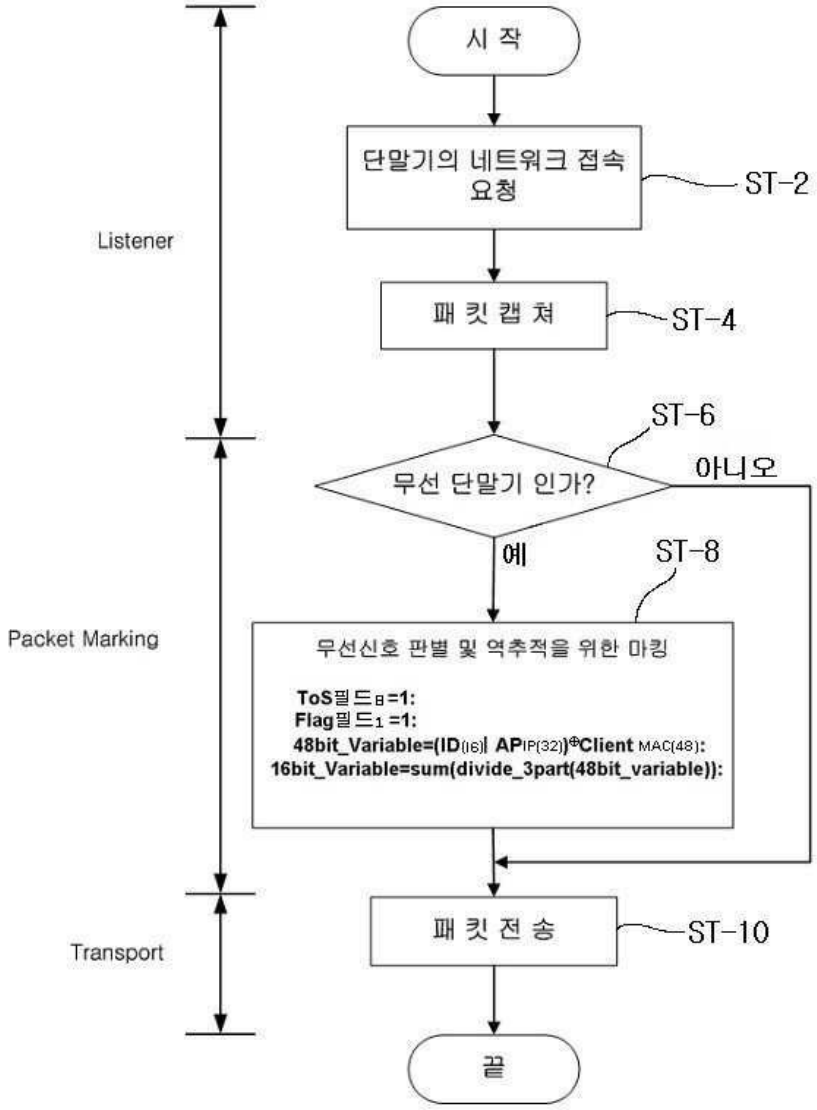
도면10b



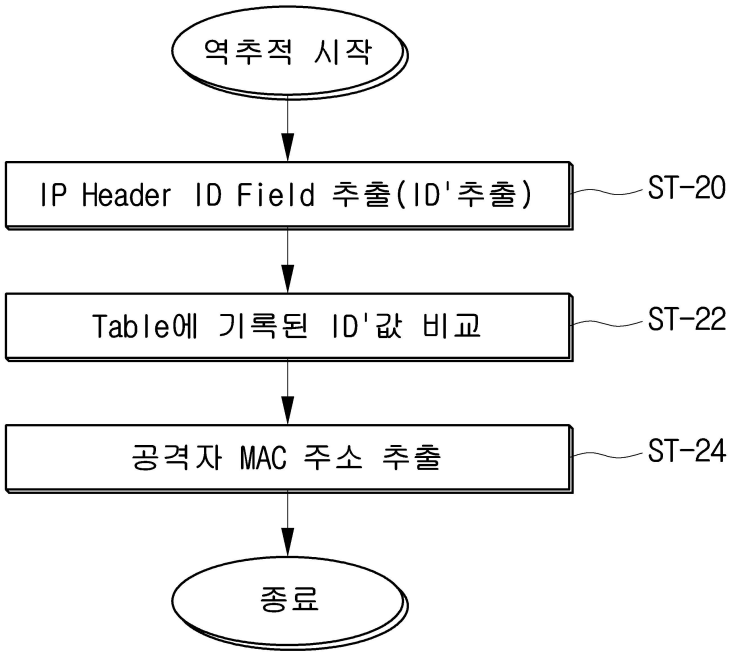
도면11


32bit
Version 4bit
Header Length 4bit
Type of Service 8bit
Total Length 16bit
Identifier(ID) 16bit
Flags 3bit
Fragment Offset 13bit
Time to Live 8bit
Protocol 8bit
Header Checksum 16bit
Source Address
Destination Address
Options 24bit
Padding 8bit

도면12


시 작
단말기의 네트워크 접속 요청
ST-2
Listener
패 킷 캡 쳐
ST-4
ST-6
무선 단말기 인가?
아니오
예
ST-8
Packet Marking
무선신호 판별 및 역추적을 위한 마킹
ToS필드B=1:
Flag필드1=1:
48bit_Variable=(ID(16)| APIP(32))⊕Client MAC(48):
16bit_Variable=sum(divide_3part(48bit_variable)):
패 킷 전 송
ST-10
Transport
끝

도면13



도면14

ID'	Client MAC
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....