



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0070123
(43) 공개일자 2010년06월25일

(51) Int. Cl.

H04L 12/26 (2006.01) H04B 7/26 (2006.01)

(21) 출원번호 10-2008-0128732

(22) 출원일자 2008년12월17일

심사청구일자 2008년12월17일

기술이전 희망 : 기술양도, 실시권허여, 기술지도

(71) 출원인

한국전자통신연구원

대전 유성구 가정동 161번지

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

윤병식

대전광역시 서구 만년동 강변아파트 104동 1403호

박만호

대전 유성구 전민동 청구나래아파트 101동 1705호

(뒷면에 계속)

(74) 대리인

유미특허법인

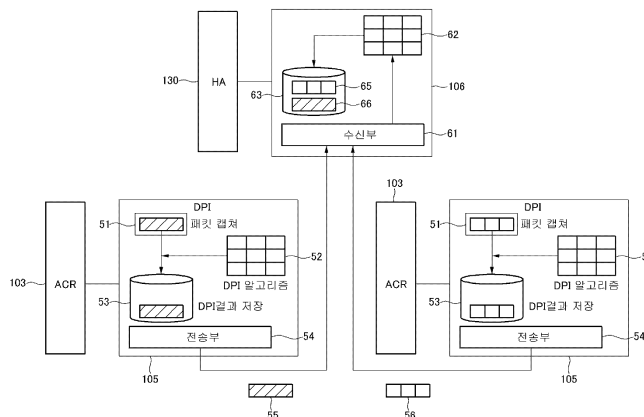
전체 청구항 수 : 총 12 항

(54) 심층 패킷 검사 장치 및 심층 패킷 검사 방법

(57) 요약

본 발명은 무선 통신 시스템의 심층 패킷 검사 방법 및 그 장치에 관한 것이다. 본 발명에 따른 무선 통신 시스템의 심층 패킷 검사 방법은 핸드오버 발생 시, 핸드오버 전의 제1 서브넷으로부터 단말의 패킷에 대한 제1 심층 패킷 검사 결과를 수신하는 단계, 핸드오버 후의 제2 서브넷으로부터 상기 단말의 패킷에 대한 제2 심층 패킷 검사 결과를 수신하는 단계, 그리고 핸드오버 발생 시 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 재정렬하는 단계를 포함한다.

대표도



(72) 발명자

김정학

대전 유성구 관평동 896 대덕테크노밸리 808동 602호

최송인

대전광역시 유성구 어은동 한빛아파트 103동 801호

이명락

서울 성북구 안암동5가 고려대학교자연계캠퍼스 604D

김승빈

서울 성북구 안암동5가 고려대학교자연계캠퍼스 608B

박성준

서울 성북구 안암동5가 고려대학교자연계캠퍼스 608B

인호

서울 성북구 안암동5가 고려대학교자연계캠퍼스 604D

이 발명을 지원한 국가연구개발사업

과제고유번호 2008-S-001-01

부처명 지식경제부 및 정보통신연구진흥원

연구사업명 IT성장동력기술개발

연구과제명 WiBro 네트워크 신뢰성 확보 및 위치 인지 기술 개발

주관기관 한국전자통신연구원

연구기간 2008.03.01~2011.02.28

특허청구의 범위

청구항 1

무선 통신 시스템의 심층 패킷 검사 방법으로서,

핸드오버 발생 시, 핸드오버 전의 제1 서브넷으로부터 단말의 패킷에 대한 제1 심층 패킷 검사 결과를 수신하는 단계,

핸드오버 후의 제2 서브넷으로부터 상기 단말의 패킷에 대한 제2 심층 패킷 검사 결과를 수신하는 단계, 그리고
핸드오버 발생 시 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 재정렬하는 단계
를 포함하는 심층 패킷 검사 방법.

청구항 2

제1항에서,

인증 서버로부터 상기 단말의 식별자를 제공받는 단계, 그리고

홈 에이전트로부터 상기 단말의 보조 주소 및 홈 주소를 제공받는 단계

를 더 포함하는 심층 패킷 검사 방법.

청구항 3

제1항에서,

상기 제1 심층 패킷 검사 결과를 수신하는 단계는, 상기 단말의 식별자, 상기 단말의 상기 제1 서브넷에서의 보조 주소 및 상기 단말의 홈 주소를 수신하는 단계를 포함하며,

상기 제2 심층 패킷 검사 결과를 수신하는 단계는, 상기 단말의 식별자, 상기 단말의 상기 제2 서브넷에서의 보조 주소 및 상기 단말의 홈 주소를 수신하는 단계를 포함하

는 심층 패킷 검사 방법.

청구항 4

제1항 내지 제3항 중 어느 한 항에서,

상기 재정렬하는 단계는 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 상기 단말의 고유 정보에 기초하는 제3 심층 패킷 검사 결과로 재정렬하는 단계를 포함하는 심층 패킷 검사 방법.

청구항 5

제4항에서,

상기 고유 정보는 상기 단말의 식별자, 상기 단말의 홈 주소 및 상기 단말의 인터넷 프로토콜(internet protocol, IP) 주소 중 적어도 하나를 포함하는 심층 패킷 검사 방법.

청구항 6

제1항 내지 제3항 중 어느 한 항에서,

상기 제1 심층 패킷 검사 결과는 상기 제1 서브넷에서 상기 단말의 패킷과 심층 패킷 검사 알고리즘의 패턴의 매칭에 생성되며,

상기 제2 심층 패킷 검사 결과는 상기 제2 서브넷에서 상기 단말의 패킷과 심층 패킷 검사 알고리즘의 패턴의 매칭에 생성되는 심층 패킷 검사 방법.

청구항 7

무선 통신 시스템의 심층 패킷 검사 방법으로서,

제1 서브넷에서 단말에 의해 생성되는 패킷을 포착하는 단계,

포착한 패킷과 심층 패킷 검사 알고리즘의 패턴을 매칭하여 심층 패킷 검사 결과를 생성하는 단계, 그리고

상기 제1 서브넷에서 제2 서브넷으로의 핸드오버 발생 시, 상기 심층 패킷 검사 결과를 상기 제1 서브넷과 상기 제2 서브넷을 관리하는 심층 패킷 검사 서버로 전송하는 단계

를 포함하는 심층 패킷 검사 방법.

청구항 8

제7항에서,

인증 서버로부터 상기 단말의 식별자를 제공받는 단계, 그리고

홈 에이전트로부터 상기 단말의 보조 주소 및 홈 주소를 제공받는 단계

를 더 포함하는 심층 패킷 검사 방법.

청구항 9

제7항에서,

상기 전송하는 단계는, 상기 단말의 식별자, 상기 단말의 상기 제1 서브넷에서의 보조 주소 및 상기 단말의 홈 주소를 전송하는 상기 심층 패킷 검사 서버로 전송하는 심층 패킷 검사 방법.

청구항 10

핸드 오버 발생시 핸드 오버 전의 제1 서브넷으로부터 단말의 패킷에 대한 제1 심층 패킷 검사 결과를 수신하며, 핸드오버 후의 제2 서브넷으로부터 상기 단말의 패킷에 대한 제2 심층 패킷 검사 결과를 수신하는 수신부, 그리고

핸드오버(handover) 발생 시 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 재정렬하여 제3 심층 패킷 검사 결과를 생성하는 재정렬부

를 포함하는 심층 패킷 검사 장치.

청구항 11

제10항에서,

단말의 패킷과 검사 알고리즘의 패턴을 매칭하여 상기 제1 심층 패킷 검사 결과를 생성하며 상기 제1 서브넷에 포함되어 있는 제1 심층 패킷 검사 클라이언트, 그리고

단말의 패킷과 검사 알고리즘의 패턴을 매칭하여 상기 제1 심층 패킷 검사 결과를 생성하며 상기 제2 서브넷에 포함되어 있는 제2 심층 패킷 검사 클라이언트

를 더 포함하는 심층 패킷 검사 장치.

청구항 12

제10항에서,

상기 재정렬부는 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 상기 단말의 고유 정보에 기초하는 제3 심층 패킷 검사 결과로 재정렬하는 심층 패킷 검사 장치.

명세서

발명의 상세한 설명

기술 분야

- [0001] 본 발명은 심층 패킷 검사 장치 및 심층 패킷 검사 방법에 관한 것이다.
- [0002] 본 발명은 지식경제부 및 정보통신연구진흥원의 IT성장동력기술개발의 일환으로 수행한 연구로부터 도출된 것이다[과제관리번호: 2008-S-001-01, 과제명: WiBro 네트워크 신뢰성 확보 및 위치 인지 기술 개발].

배경 기술

- [0003] 최근 무선 통신 시스템은 사용자의 이동에 따른 핸드 오버 발생 시에도 서비스의 중단 없이 지속적인 인터넷 서비스를 제공하고 있다. 이러한 발전과 함께 보안 위협 또한 증가하였는데, 무선 구간에서 무단 인증, 무단 접속, 패킷(packet) 가로채기, IP(internet protocol) 고갈(Starvation) 공격 등이 대표적이다. 이와 같은 공격 형태가 진화함에 따라, 사용자의 이동성을 제공하는 환경에서의 보안 위협은 다양한 형태가 될 것으로 예상된다. 따라서, 핸드 오버 발생 시에도 특정 패킷들에 대한 지속적인 심층 검사(Deep Inspection)가 이루어지는 것이 매우 중요하다.
- [0004] 심층 패킷 검사(DPI: Deep Packet Inspection)란, 패킷의 헤더 검색은 물론 패킷의 내용까지 검색하는 패킷 필터링 기술이다. IP 이동성이 제공되는 환경에서는 패킷의 내용에 대한 검사가 중요한 이슈가 되고 있다. 기존의 유선망 중심의 심층 패킷 검사는 하나의 서브넷을 중심으로 이루어졌으나, 이동 IP를 지원하는 환경에서는 기존 방식의 심층 패킷 검사로는 특정 이동 단위(unit)를 중심으로 연결된 패킷들의 지속적인 감시 추적이 곤란하다. 특히, 이와 같이 이동 IP를 지원하는 사용자가 유무선 통합 서비스를 이용하면서 끊임 없이 핸드 오버가 이루어질 때 악성 패킷을 포함하고 있는 패킷을 송수신하는 특정 사용자의 지속적인 추적이 곤란하다.

발명의 내용

해결 하고자하는 과제

- [0005] 본 발명이 이루고자 하는 기술적 과제는 사용자의 이동에 따른 핸드 오버가 발생할 때에도 특정 사용자의 패킷을 지속적으로 추적하는 것이다.

과제 해결수단

- [0006] 본 발명의 한 실시예에 따른 심층 패킷 검사 방법은, 무선 통신 시스템의 심층 패킷 검사 방법으로서, 핸드오버 발생 시, 핸드오버 전의 제1 서브넷으로부터 단말의 패킷에 대한 제1 심층 패킷 검사 결과를 수신하는 단계, 핸드오버 후의 제2 서브넷으로부터 상기 단말의 패킷에 대한 제2 심층 패킷 검사 결과를 수신하는 단계, 그리고 핸드오버 발생 시 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 재정렬하는 단계를 포함한다.
- [0007] 인증 서버로부터 상기 단말의 식별자를 제공받는 단계, 그리고 홈 에이전트로부터 상기 단말의 보조 주소 및 홈 주소를 제공받는 단계를 더 포함할 수 있다.
- [0008] 상기 제1 심층 패킷 검사 결과를 수신하는 단계는, 상기 단말의 식별자, 상기 단말의 상기 제1 서브넷에서의 보조 주소 및 상기 단말의 홈 주소를 수신하는 단계를 포함하며, 상기 제2 심층 패킷 검사 결과를 수신하는 단계는, 상기 단말의 식별자, 상기 단말의 상기 제2 서브넷에서의 보조 주소 및 상기 단말의 홈 주소를 수신하는 단계를 포함할 수 있다.
- [0009] 상기 재정렬하는 단계는 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 상기 단말의 고유 정보에 기초하는 제3 심층 패킷 검사 결과로 재정렬하는 단계를 포함할 수 있다.
- [0010] 상기 고유 정보는 상기 단말의 식별자, 상기 단말의 홈 주소 및 상기 단말의 인터넷 프로토콜(internet protocol, IP) 주소 중 적어도 하나를 포함할 수 있다.
- [0011] 상기 제1 심층 패킷 검사 결과는 상기 제1 서브넷에서 상기 단말의 패킷과 심층 패킷 검사 알고리즘의 패킷의 매칭에 생성되며, 상기 제2 심층 패킷 검사 결과는 상기 제2 서브넷에서 상기 단말의 패킷과 심층 패킷 검사 알고리즘의 패킷의 매칭에 생성될 수 있다.
- [0012] 본 발명의 다른 실시예에 따른 심층 패킷 검사 방법은 무선 통신 시스템의 심층 패킷 검사 방법으로서, 제1 서브넷에서 단말에 의해 생성되는 패킷을 포착하는 단계, 포착한 패킷과 심층 패킷 검사 알고리즘의 패킷을 매칭

하여 심층 패킷 검사 결과를 생성하는 단계, 그리고 상기 제1 서브넷에서 제2 서브넷으로의 핸드오버 발생 시, 상기 심층 패킷 검사 결과를 상기 제1 서브넷과 상기 제2 서브넷을 관리하는 심층 패킷 검사 서버로 전송하는 단계를 포함한다.

- [0013] 인증 서버로부터 상기 단말의 식별자를 제공받는 단계, 그리고 홈 에이전트로부터 상기 단말의 보조 주소 및 홈 주소를 제공받는 단계를 더 포함할 수 있다.
- [0014] 상기 전송하는 단계는, 상기 단말의 식별자, 상기 단말의 상기 제1 서브넷에서의 보조 주소 및 상기 단말의 홈 주소를 전송하는 상기 심층 패킷 검사 서버로 전송할 수 있다.
- [0015] 본 발명의 다른 실시예에 따른 심층 패킷 검사 장치는 핸드 오버 발생시 핸드 오버 전의 제1 서브넷으로부터 단말의 패킷에 대한 제1 심층 패킷 검사 결과를 수신하며, 핸드오버 후의 제2 서브넷으로부터 상기 단말의 패킷에 대한 제2 심층 패킷 검사 결과를 수신하는 수신부, 그리고 핸드오버(handover) 발생 시 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 재정렬하여 제3 심층 패킷 검사 결과를 생성하는 재정렬부를 포함한다.
- [0016] 단말의 패킷과 검사 알고리즘의 패턴을 매칭하여 상기 제1 심층 패킷 검사 결과를 생성하며 상기 제1 서브넷에 포함되어 있는 제1 심층 패킷 검사 클라이언트, 그리고 단말의 패킷과 검사 알고리즘의 패턴을 매칭하여 상기 제1 심층 패킷 검사 결과를 생성하며 상기 제2 서브넷에 포함되어 있는 제2 심층 패킷 검사 클라이언트를 더 포함할 수 있다.
- [0017] 상기 재정렬부는 상기 제1 심층 패킷 검사 결과 및 상기 제2 심층 패킷 검사 결과를 상기 단말의 고유 정보에 기초하는 제3 심층 패킷 검사 결과로 재정렬할 수 있다.

효 과

- [0018] 본 발명에 따르면 사용자의 이동에 따른 핸드 오버가 발생할 때에도 특정 사용자의 패킷을 지속적용 추적하여 보안 위협을 줄일 수 있다.

발명의 실시를 위한 구체적인 내용

- [0019] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0020] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.
- [0021] 본 명세서에서 단말(terminal)은 이동국(Mobile Station, MS), 이동 단말(Mobile Terminal, MT), 가입자국(Subscriber Station, SS), 휴대 가입자국(Portable Subscriber Station, PSS), 사용자 장치(User Equipment, UE), 접근 단말(Access Terminal, AT) 등을 지칭할 수도 있고, 이동국, 이동 단말, 가입자국, 휴대 가입자국, 사용자 장치, 접근 단말 등의 전부 또는 일부의 기능을 포함할 수도 있다.
- [0022] 본 명세서에서 기지국(base station, BS)은, 기지국(Base Station, BS), 접근점(Access Point, AP), 무선 접근국(Radio Access Station, RAS), 노드B(Node B), 고도화 노드B(evolved NodeB, eNodeB), 송수신 기지국(Base Transceiver Station, BTS), MMR(Mobile Multihop Relay)-BS 등을 지칭할 수도 있고, 접근점, 무선 접근국, 노드B, eNodeB, 송수신 기지국, MMR-BS 등의 전부 또는 일부의 기능을 포함할 수도 있다.
- [0023] 이제 도 1을 참고하여 본 발명의 한 실시예에 따른 심층 패킷 검사 장치를 설명한다.
- [0024] 도 1은 본 발명의 한 실시예에 따른 심층 패킷 검사 장치를 포함하는 무선 통신 시스템을 도시하는 블록도이다.
- [0025] 도 1을 참고하면, 무선 통신 시스템(100)은 복수의 서브넷(subnet)(110, 120), 홈 에이전트(Home Agent, HA) 및 인증(Authentication Authorization Accounting, AAA) 서버(140)를 포함한다.

- [0026] 각 서버넷(110, 120)은 단말(terminal)(101), 기지국(102), 제어국(Access Control Router, ACR)(103) 및 심층 패킷 검사 장치(deep packet inspection device)(104)를 포함한다.
- [0027] 단말(101)은 무선 채널의 종단점으로 무선 통신 시스템, 예를 들면 휴대 인터넷 시스템의 무선 접속 규격에 따른 송수신 기능과 매체 접근 제어(Medium Access Control, MAC) 처리 기능을 이용하여 무선 접근국(102)에 접속하고 고속 패킷 데이터를 송수신한다.
- [0028] 무선 접근국(102)은 단말(101)로부터 무선 신호를 수신하여 제어국(103)으로 전달하거나 제어국(103)으로부터 수신되는 데이터들을 무선 신호로 변환하여 단말(101)로 전달하며, 단말(101)와 초기 접속, 섹터간 핸드 오버 제어 기능 및 서비스 품질(QoS: Quality of Service) 제어 기능을 수행한다.
- [0029] 제어국(103)은 무선 접근국(102)과 IP(Internet Protocol) 기반 유선으로 접속을 통해 인터넷 망을 구성하는 IP 기반 핵심 망에 접속하고 인증, 이동 IP(Mobile Internet Protocol), 무선 접근국(102) 간의 핸드 오버(handover), 제어국(103)간 핸드 오버 제어 기능 및 서비스 품질 제어 기능을 수행한다.
- [0030] 심층 패킷 검사 장치(104)는 심층 패킷 검사 클라이언트(deep packet inspection client)(105) 및 심층 패킷 검사 서버(deep packet inspection server)(106)를 포함하며, 제어국(103)과 연결되어 제어국(103) 수준에서 패킷을 검사한다. 심층 패킷 검사 클라이언트(105)는 하나의 서버넷(110, 120)에서 통신 중인 단말(101)이 다른 서버넷(110, 120)으로 이동하여 핸드오버가 발생하는 경우, 심층 패킷 검사 서버(106)로 특정 단말(101)의 과거 심층 패킷 검사 결과를 전송한다.
- [0031] 홈 에이전트(130)는 단말(101)의 홈 주소(Home Address)를 등록하며, 단말(101)이 해당 서버넷(110, 120)을 떠날 때 보조 주소(CoA: Care of Address)를 등록함으로써 단말(101)의 현재 위치 정보를 유지시킨다. 또한 홈 에이전트(130)는 단말(101)이 다른 서버넷(110, 120)에서 자신이 속한 서버넷(110, 120)으로 통신할 수 있도록 데이터그램을 캡슐화한다.
- [0032] 인증 서버(140)는 사업자 별로 휴대 인터넷 사용자의 컴퓨터 자원 접근 처리를 하며, 서비스 제공에 있어서 인증(Authentication) 인가(Authorization), 과금(Accounting) 기능을 제공하며, 단말(101)의 식별자(Identification)를 등록한다.
- [0033] 이제 도 2 및 도 3을 참고하여 본 발명의 한 실시예에 따른 심층 패킷 검사 장치에 대하여 상세하게 설명한다.
- [0034] 도 2는 본 발명의 한 실시예에 따른 심층 패킷 검사 장치를 도시하는 블록도이며, 도 3은 본 발명의 한 실시예에 따라 심층 패킷 검사를 수행하는 순서를 도시하는 흐름도이다.
- [0035] 먼저 도 2를 참고하면, 심층 패킷 검사 클라이언트(105)는 수신부(51), 패턴 매칭부(52), 저장부(53) 및 전송부(54)를 포함하며, 심층 패킷 검사 서버(106)는 수신부(61), 재정렬부(coordinator)(62) 및 저장부(63)를 포함한다.
- [0036] 심층 패킷 검사 클라이언트(105)의 수신부(51)는 단말(101)에 의해 생성되는 데이터 패킷(45, 46)을 포착(capture)하여 수신하며, 홈 에이전트(130)로부터 단말(101)의 식별자 및 홈 주소를 수신하고, 단말(101)이 이동하는 경우 홈 에이전트(130)로부터 단말(101)의 보조 주소를 수신한다.
- [0037] 패턴 매칭부(52)는 수신된 패킷(45, 46)을 미리 저장되어 있는 심층 패킷 검사 알고리즘과 패턴 매칭하여 심층 패킷 검사 결과(55, 56)를 생성한다.
- [0038] 저장부(53)는 즉 심층 패킷 검사 결과(55, 56)를 저장한다.
- [0039] 전송부(55)는 핸드 오버가 발생한 경우 심층 패킷 검사 결과를 심층 패킷 검사 서버(106)로 전송한다. 심층 패킷 검사 결과는 하나의 단말(101)이 서로 다른 제어국(102, 103)을 이동할 때, 매칭이 이루어져 전송되는 패킷(55, 56)이다. 이때 전송부(55)는 심층 패킷 검사 결과와 함께 단말(101)의 식별자, 홈 주소 및 보조 주소를 심층 패킷 검사 서버(106)로 전송한다.
- [0040] 심층 패킷 검사 서버(106)의 수신부(61)는 심층 패킷 검사 클라이언트(105)로부터 심층 패킷 검사 결과(55, 56), 단말(101)의 식별자, 홈 주소 및 보조 주소를 수신한다.
- [0041] 재정렬부(62)는 단말(101)의 식별자, 홈 주소 및 보조 주소를 기초로 심층 패킷 검사 결과(55, 56)를 단말의 고유 정보로 재정렬하며, 저장부(63)는 재정렬된 심층 패킷 검사 결과(65, 66)를 저장한다. 고유 정보는 단말의 IP 주소, 홈 주소, 식별자 등이 될 수 있다.

- [0042] 도 3을 참고하면, 먼저 심층 패킷 검사 클라이언트(105)는 패킷을 수신한다 (S301). 그런 후 수신한 패킷과 심층 패킷 검사 알고리즘의 패턴과 매칭되는지 여부를 검사한다(S302). 여기서 수신한 패킷과 심층 패킷 검사 알고리즘의 패턴이 일치하면 패턴 매칭 정보를 생성하여 저장한다(S303).
- [0043] 만일 수신한 패킷과 심층 패킷 검사 알고리즘의 패턴이 일치하지 않으면, 다른 패킷을 다시 심층 패킷 검사 알고리즘의 패턴과 비교하기 위해서 패킷 존재 여부를 판단한다(S307). 판단 결과 패킷이 존재하는 경우 다시 처음부터 패턴 매칭을 다시 수행하고, 존재하지 않는 경우 종료한다.
- [0044] 패턴 매칭 정보를 생성하여 저장(S303)한 후, 핸드 오버가 발생하는지 여부를 판단한다(S304). 핸드 오버가 발생한 경우, 심층 패킷 검사 클라이언트(105)는 감시 중이던 단말의 패턴 매칭 결과, 즉 심층 패킷 검사 결과를 심층 패킷 검사 서버(106)로 전달한다(S305). 만일 핸드 오버가 발생하지 않은 경우에는 감시 중이던 단말의 패턴 매칭 결과를 심층 패킷 검사 서버(106)로 전달하지 않고, 다시 새로운 패킷에 대한 검사를 시작한다 (S307).
- [0045] 한편, 단말(101)은 서브넷(120)으로 이동하였으므로, 핸드오버 지시에 따라 심층 패킷 검사 클라이언트(106)가 단계 S301, S302, S303 및 S307의 과정을 통하여 단말(101)이 서브넷(120)으로 송신하는 패킷에 대한 패턴 매칭 결과를 심층 패킷 검사 서버(106)로 전달한다.
- [0046] 심층 패킷 검사 클라이언트(105, 106)가 패턴 매칭 결과를 심층 패킷 검사 서버(106)로 전달(S305)한 후, 심층 패킷 검사 서버(106)는 심층 패킷 검사 클라이언트(105, 106)로부터의 패턴 매칭 결과를 재정렬하여 이를 저장한다(S306).
- [0047] 그러면 도 4 내지 도 7을 참고하여 심층 패킷 검사 서버(106)의 동작에 대하여 상세하게 설명한다.
- [0048] 도 4는 단말의 이동이 발생한 경우 본 발명의 한 실시예에 따른 심층 패킷 검사 장치의 동작을 설명하는 도면이며, 도 5는 본 발명의 한 실시예에 따라 보조 주소 기반의 부분 정보들을 홈 주소 기반의 정보로 재정렬하는 하나의 예를 도시하는 도면이며, 도 6은 본 발명의 한 실시예에 따른 심층 패킷 검사 서버의 재정렬부에서 패턴 매칭 결과를 생성하는 과정을 나타내는 도면이며, 도 7은 본 발명의 한 실시예에 따른 재정렬 작업의 예를 도시하는 도면이다.
- [0049] 도 4를 참고하면, 단말(101)은 홈 에이전트(130)로부터 홈 주소(402, 403)을 할당 받았으며, 이동한 지역의 홈 에이전트, 즉 외부 에이전트(FA: Foreign Agent)(131)로부터 새로 보조 주소(401, 404)를 할당 받는다. 심층 패킷 검사 서버(106)의 재정렬부(62)는 이동하는 단말(101)이 위치한 지역의 심층 패킷 검사 클라이언트(105)로부터 받은 보조 주소(401, 404) 기반의 패킷 검사 결과들을 홈 주소(402, 403) 기반의 패킷 검사 결과로 종합하여 동일한 단말의 패킷 검사 결과들을 하나의 통합된 패킷 검사 결과로 생성한다.
- [0050] 도 5를 참고하면, 심층 패킷 검사 클라이언트(105)가 위치한 지역에서 부분적인 심층 패킷 검사를 수행한 결과 (501, 502)가 도시되어 있다. 이러한 부분 심층 패킷 검사 결과(501, 502)는 심층 패킷 검사 서버(106)에서 종합하여 완전한 패킷 검사 결과(500)가 생성된다.
- [0051] 이제 도 6을 참고하여, 핸드 오버 발생시 심층 패킷 검사 클라이언트(105)의 지역에서 실시한 심층 패킷 검사 결과를 이용하여 재정렬부(62)가 심층 패킷 검사 서버(106) 지역에서 새로운 패킷 검사 결과 생성하는 과정을 설명한다.
- [0052] 도 6을 참고하면, 심층 패킷 검사 클라이언트(105, 106)가 심층 패킷 검사를 수행할 때 단말의 식별자(ID: Identification), 보조 주소 및 심층 패킷 검사 결과인 로그 정보(logged information)을 저장(605, 606)하여, 단말의 핸드 오버가 발생하는 경우 심층 패킷 검사 서버(106)가 위치하는 지역으로 심층 패킷 검사 결과를 전송한다.
- [0053] 심층 패킷 검사 서버(106)는 재정렬부(62)에 의해서 보조 주소의 기반의 부분적인 심층 패킷 검사 결과를 조합하여, 단말의 식별자 및/또는 홈 주소 중심의 완전한 심층 패킷 검사 결과를 생성한다.
- [0054] 한편, 도 7에는 보조 주소와 홈 주소를 비교하여 단말의 패킷 검사 결과를 하나의 IP로 추출해내는 알고리즘의 한 예가 도시되어 있다. 재정렬부(62)는 도 7과 같은 알고리즘을 이용하여 완전한 심층 패킷 검사 결과를 생성할 수 있다.
- [0055] 이와 같이 핸드오버가 발생하는 경우 심층 패킷 검사 결과를 심층 패킷 검사서버에 전송하여 이를 재정렬함으로써, 단말이 이동하는 경우에도 특정 단말의 패킷을 지속적으로 추적할 수 있다.

[0056] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

[0057] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면의 간단한 설명

[0058] 도 1은 본 발명의 한 실시예에 따른 심층 패킷 검사 장치를 포함하는 무선 휴대 인터넷 시스템을 도시하는 블록도이다.

[0059] 도 2는 본 발명의 한 실시예에 따른 심층 패킷 검사 장치를 도시하는 블록도이다.

[0060] 도 3은 본 발명의 한 실시예에 따라 심층 패킷 검사를 수행하는 순서를 도시하는 흐름도이다.

[0061] 도 4는 단말의 이동이 발생한 경우 본 발명의 한 실시예에 따른 심층 패킷 검사 시스템의 동작을 설명하는 도면이다.

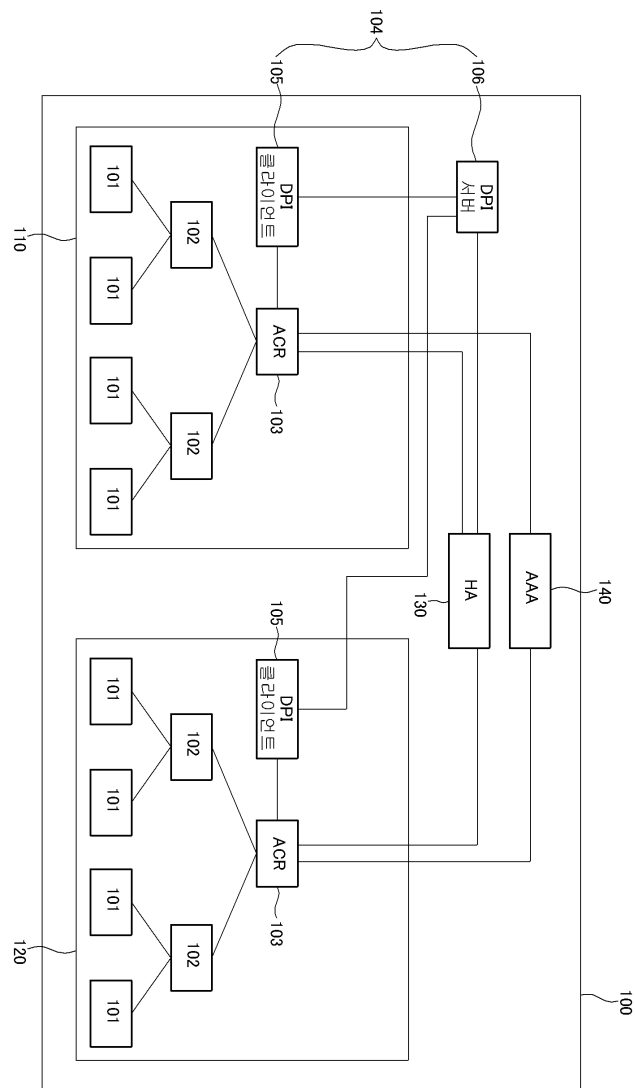
[0062] 도 5는 본 발명의 한 실시예에 따라 보조 주소 기반의 부분 정보들을 홈 주소 기반의 정보로 재정렬하는 하나의 예를 도시하는 도면이다.

[0063] 도 6은 본 발명의 한 실시예에 따른 심층 패킷 검사 서버의 재정렬부에서 패턴 매칭 결과를 생성하는 과정을 나타내는 도면이다.

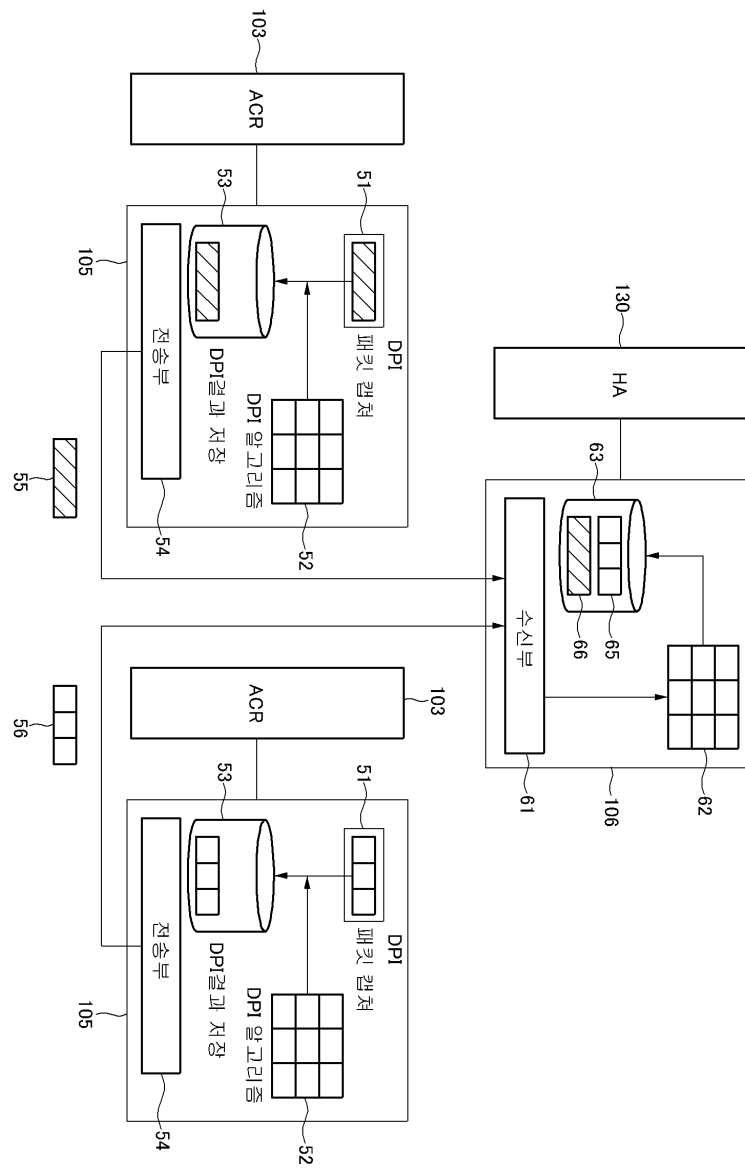
[0064] 도 7은 본 발명의 한 실시예에 따른 재정렬 작업의 예를 도시하는 도면이다.

도면

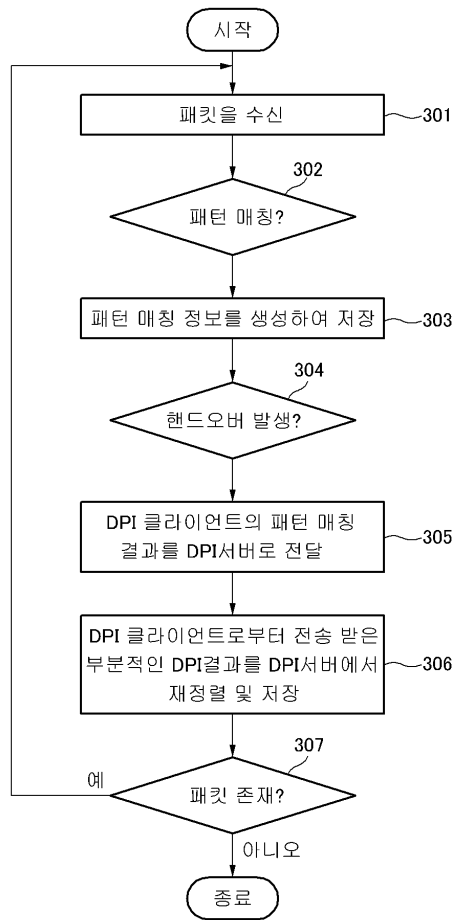
도면1



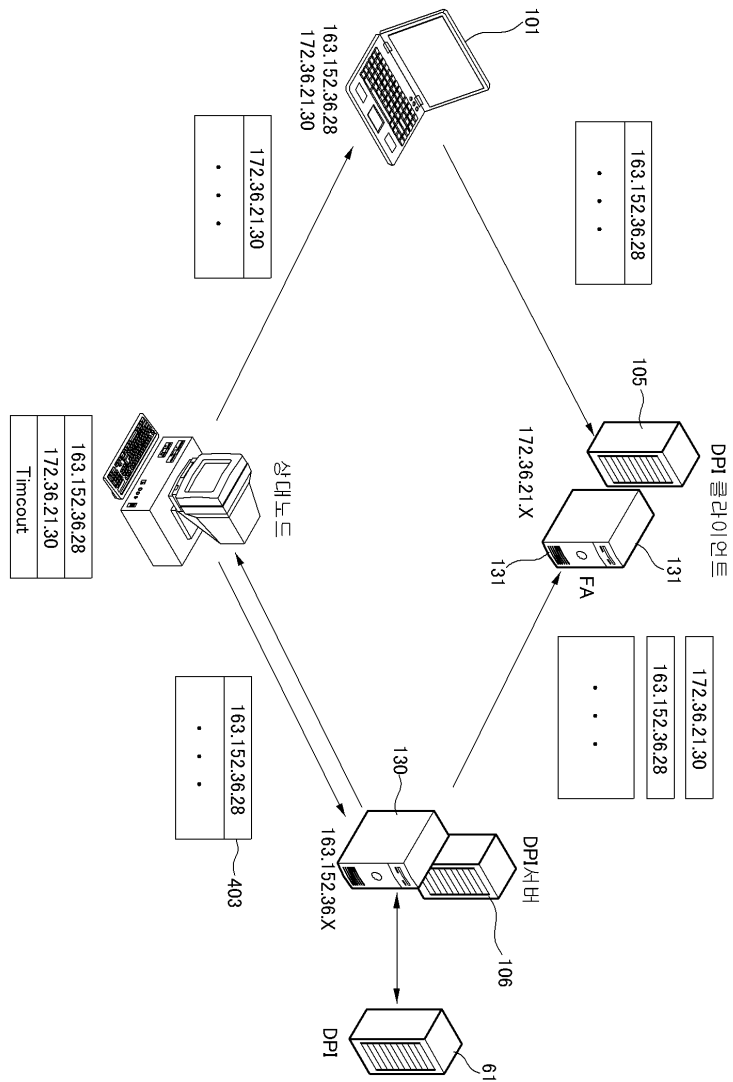
도면2



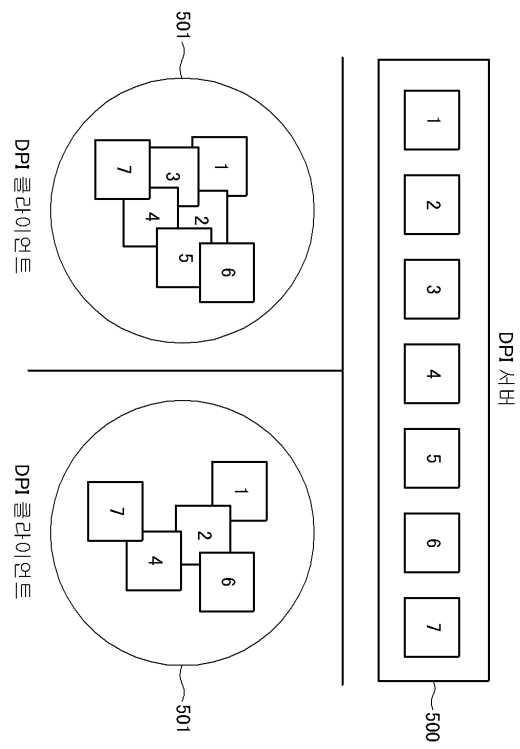
도면3



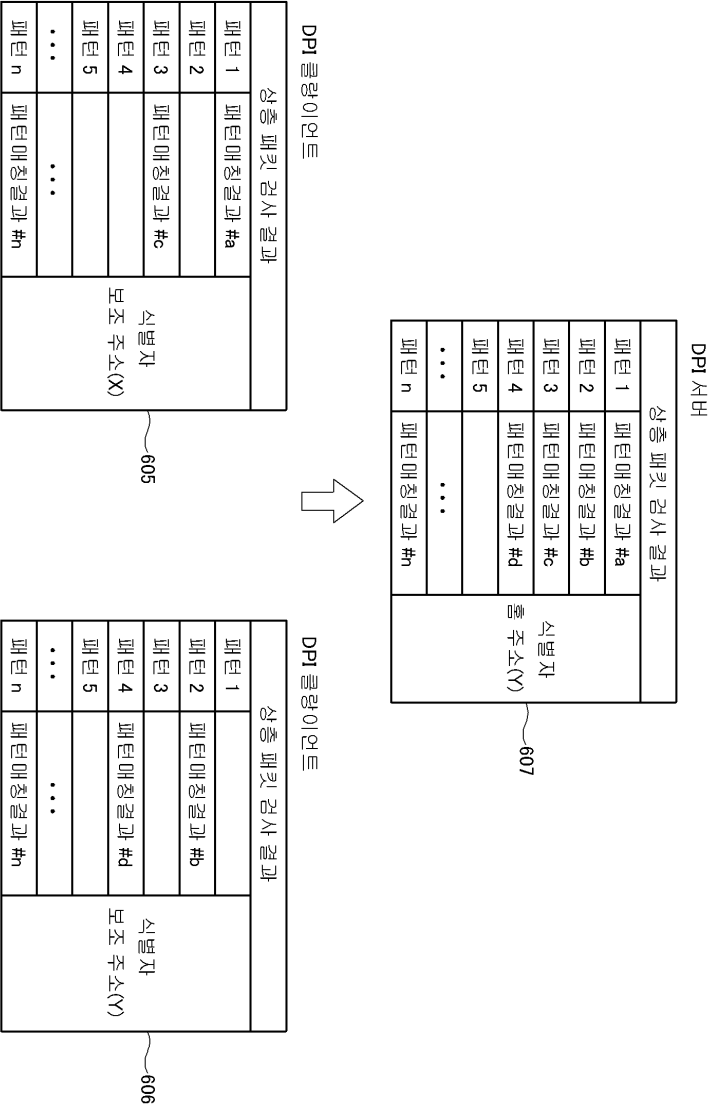
도면4



도면5



도면6



도면7

<pre> procedure recDPI(time) begin for 1 to n in DPI begin update(matched, receive(i, time)); end; end; procedure integration() begin recDPI(time); update(ipTable, receive(CoATable)); for 1 to n in matched begin if compare(matched, ipTable); begin matched[i].ip=ipTable.ip; end; end; sort(matched); </pre>	
지정 시간의 DPI 매칭 결과 정보 수신 <pre> { DPI 장비 1부터 n까지 수신 { 지정 시간의 매칭 결과 수신; } } </pre> DPI 결과 통합 <pre> { DPI 장비로부터 지정 시간의 패턴 매칭 결과 수신; CoA로부터 IP테이블을 수신; DPI 장비로부터 수신한 패턴 매칭 결과를 1부터 n개까지 반복 { 만약 수신한 패턴 매칭 결과의 IP주소와 CoA의 IP테이블의 주소가 일치할 경우 { i번째 패턴 매칭 결과의 IP주소를 CoA의 IP주소로 변경 } } 패턴 매칭 결과를 IP주소로 정렬; } </pre>	