(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년04월30일
(11) 등록번호 10-0894908
(24) 등록일자 2009년04월17일

(51) Int. Cl.
*H04L 12/26* (2006.01) *H04L 12/66* (2006.01)
*H04L 29/02* (2006.01)
(21) 출원번호 10-2007-0046950
(22) 출원일자 2007년05월15일
심사청구일자 2007년05월15일
(65) 공개번호 10-2008-0100918
(43) 공개일자 2008년11월21일
(56) 선행기술조사문헌
KR1020070060869 A
US6816455 B2
KR1020070039666 A
KR100636277 B1
전체 청구항 수 : 총 15 항

(73) 특허권자
**고려대학교 산학협력단**

(72) 발명자
**서동원**

**이희조**

(74) 대리인
**유미특허법인**

심사관 : 천대녕

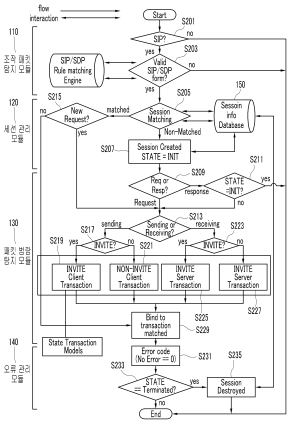
# (54) 인터넷 기반 음성 서비스에서 비정상 패킷을 탐지하는 방법및 컴퓨터로 읽을 수 있는 매체

## (57) 요 약

인터넷 기반 음성 서비스(Voice over Internet protocol, VoIP)를 위한 프로토콜의 하나인 SIP(Session Initiation protocol)에서 예외 패킷을 탐지하는 예외 탐지 모듈은 세션 설정에 관한 패킷을 획득하면, 패킷의 헤더의 복수의 필드의 각각이 규정된 문자 길이를 벗어나는 경우 또는 패킷의 헤더의 복수의 필드의 각각이 포함되어서는 안 되는 문자를 포함하고 있는 경우 획득한 패킷을 폐기한다.

그리고, 예외 탐지 모듈은 패킷이 속하는 세션과 세션의 상태를 확인한다. 예외 탐지 모듈은 패킷의 획득으로 인하여 세션의 특정 상태에서 패킷을 소정의 횟수 이상으로 수신하는 경우, 상기 패킷을 비정상이라고 파악하고, 획득한 패킷을 폐기한다.

*대 표 도* - 도3



## *특허청구의 범위*

**청구항 1**

SIP(Session Initiation protocol)에 따라 송신되는 패킷을 획득하는 단계;

상기 패킷의 헤더가 SIP 프로토콜 통신을 위한 설정 규칙을 위반하는 지를 판단하는 단계;

상기 패킷의 헤더가 상기 설정 규칙을 만족하는 경우, 상기 패킷이 속하는 세션을 확인하는 단계;

상기 세션의 상태를 확인하는 단계;

상기 확인된 세션의 상태에서, 상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계;

상기 세션의 상태에서 상기 패킷을 소정의 횟수 이상 획득하는 경우, 상기 패킷이, SIP를 이용한 공격을 받거나 오류가 발생한 상태를 포함하는 비정상 패킷인 것으로 판단하는 단계

를 포함하는 패킷 탐지 방법을 적어도 하나의 처리기가 실행하도록 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 매체.

**청구항 2**

삭제

**청구항 3**

제1항에 있어서,

상기 설정 규칙을 위반하는 지를 판단하는 단계는,

상기 패킷의 헤더의 복수의 필드의 각각이 규정된 문자 길이를 벗어나는 지를 판단하는 단계;

상기 패킷의 헤더의 복수의 필드의 각각이, 상기 SIP에 따른 패킷에 포함되지 않는 것으로 설정된 문자를 포함하고 있는 지를 판단하는 단계를 포함하는 컴퓨터로 읽을 수 있는 매체.

**청구항 4**

제3항에 있어서,

상기 패킷 탐지 방법은,

상기 세션의 상태가 초기 상태이고 호출 요청 메시지에 해당하는 패킷을 전송하는 경우, 상기 세션의 상태를 호출 상태로 천이시키는 단계를 더 포함하고,

상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계는,

상기 호출 상태에서 호출 요청 메시지에 해당하는 패킷을 소정의 횟수 이상 전송하는 지를 파악하는 단계를 포함하는 컴퓨터로 읽을 수 있는 매체.

**청구항 5**

제4항에 있어서,

상기 패킷 탐지 방법은

상기 세션의 상태가 상기 호출 상태이고 임시 응답 메시지에 해당하는 패킷을 수신하는 경우, 상기 세션의 상태를 처리 상태로 천이시키는 단계;

상기 세션의 상태가 상기 처리 상태이고 300부터 699까지의 SIP 응답 코드에 해당하는 응답 메시지에 해당하는 패킷을 수신하는 경우, 상기 세션의 상태를 완료 상태로 천이시키는 단계를 더 포함하고,

상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계는,

상기 처리 상태에서 응답 메시지에 해당하는 패킷을 소정의 횟수 이상 수신하는 지를 파악하는 단계와,

상기 완료 상태에서 응답 메시지에 해당하는 패킷을 소정의 횟수 이상 수신하는 지를 파악하는 단계를 더 포함

하는 컴퓨터로 읽을 수 있는 매체.

**청구항 6**

제3항에 있어서,

상기 패킷 탐지 방법은

상기 세션의 상태가 초기 상태이고 호출 요청 메시지에 해당하는 패킷을 수신하는 경우, 상기 세션의 상태를 처리 상태로 천이시키는 단계를 더 포함하고,

상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계는,

상기 처리 상태에서 호출 요청 메시지에 해당하는 패킷을 소정의 횟수 이상 수신하거나 응답 메시지를 소정의 횟수 이상 송신하는 지를 파악하는 단계를 포함하는 컴퓨터로 읽을 수 있는 매체.

**청구항 7**

제6항에 있어서,

상기 패킷 탐지 방법은

상기 세션의 상태가 상기 처리 상태이고 300부터 699까지의 SIP 응답 코드에 해당하는 응답 메시지에 해당하는 패킷을 수신하는 경우, 상기 세션의 상태를 완료 상태로 천이시키는 단계; 및

상기 완료 상태에서 확인 메시지에 해당하는 패킷을 수신하는 경우, 상기 세션의 상태를 확인 상태로 천이시키는 단계를 더 포함하고,

상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계는,

상기 완료 상태에서 호출 요청 메시지에 해당하는 패킷을 소정의 횟수 이상 수신하는 지를 파악하는 단계와,

상기 확인 상태에서 호출 요청 메시지에 해당하는 패킷을 수신하는 지 또는 확인 메시지에 해당하는 패킷을 소정의 횟수 이상 수신하는 지를 파악하는 단계를 더 포함하는 컴퓨터로 읽을 수 있는 매체.

**청구항 8**

제3항에 있어서,

상기 패킷 탐지 방법은

상기 세션의 상태가 초기 상태이고 비호출 요청 메시지에 해당하는 패킷을 전송하는 경우, 상기 세션의 상태를 시도 상태로 천이시키는 단계를 더 포함하고,

상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계는,

상기 시도 상태에서 비호출 요청 메시지에 해당하는 패킷을 소정의 횟수 이상 전송하는 지를 파악하는 단계를 포함하는 컴퓨터로 읽을 수 있는 매체.

**청구항 9**

제8항에 있어서,

상기 패킷 탐지 방법은

상기 시도 상태에서 임시 응답 메시지에 해당하는 패킷을 수신하는 경우, 상기 세션의 상태를 처리 상태로 천이시키는 단계; 및

상기 처리 상태에서 200부터 699까지의 SIP 응답 코드에 해당하는 응답 메시지에 해당하는 패킷을 수신하는 경우, 상기 세션의 상태를 완료 상태로 천이시키는 단계를 더 포함하고,

상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계는,

상기 처리 상태에서 비호출 요청 메시지에 해당하는 패킷을 소정의 횟수 이상 전송하거나 응답 메시지에 해당하는 패킷을 소정의 횟수 이상 수신하는 지를 파악하는 단계와,

상기 완료 상태에서 비호출 요청 메시지에 해당하는 패킷을 전송하거나 응답 메시지에 해당하는 패킷을 수신하는 지를 파악하는 단계를 더 포함하는 컴퓨터로 읽을 수 있는 매체.

**청구항 10**

제3항에 있어서,

상기 패킷 탐지 방법은

상기 세션의 상태가 초기 상태이고 비호출 요청 메시지에 해당하는 패킷을 수신하는 경우, 상기 세션의 상태를 시도 상태로 천이시키는 단계를 더 포함하고,

상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계는,

상기 시도 상태에서 비호출 요청 메시지에 해당하는 패킷을 수신하는 지를 파악하는 단계를 포함하는 컴퓨터로 읽을 수 있는 매체.

**청구항 11**

제10항에 있어서,

상기 패킷 탐지 방법은

상기 시도 상태에서 임시 응답 메시지에 해당하는 패킷을 전송하는 경우, 상기 세션의 상태를 처리 상태로 천이시키는 단계; 및

상기 처리 상태에서 200부터 699까지의 SIP 응답 코드에 해당하는 응답 메시지에 해당하는 패킷을 전송하는 경우, 상기 세션의 상태를 완료 상태로 천이시키는 단계를 더 포함하고,

상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계는,

상기 처리 상태에서 비호출 요청 메시지에 해당하는 패킷을 소정의 횟수 이상 수신하거나 응답 메시지에 해당하는 패킷을 소정의 횟수 이상 전송하는 지를 파악하는 단계와,

상기 완료 상태에서 비호출 요청 메시지에 해당하는 패킷을 소정의 횟수 이상 수신하거나 응답 메시지에 해당하는 패킷을 전송하는 지를 파악하는 단계를 더 포함하는 컴퓨터로 읽을 수 있는 매체.

**청구항 12**

SIP(Session Initiation protocol)에 따른 세션 설정에 관한 패킷을 획득하는 단계;

상기 패킷이 속하는 세션을 확인하는 단계;

상기 세션의 상태를 확인하는 단계;

상기 패킷의 획득으로 인하여 상기 세션의 상태에서 상기 패킷을 소정의 횟수 이상으로 수신하는 지를 파악하는 단계; 및

상기 세션의 상태에서 상기 패킷을 상기 소정의 횟수 이상으로 수신하는 경우, 상기 패킷을, SIP를 이용한 공격을 받거나 오류가 발생한 상태를 포함하는 비정상 패킷인 것으로 파악하는 단계를 포함하는 비정상 패킷 탐지 방법.

**청구항 13**

제12항에 있어서,

상기 패킷의 헤더의 복수의 필드의 각각이 규정된 문자 길이를 벗어나는 경우, 상기 패킷을 폐기하는 단계를 더 포함하는 비정상 패킷 탐지 방법.

**청구항 14**

제13항에 있어서,

상기 패킷의 헤더의 복수의 필드의 각각이, 상기 SIP에 따른 패킷에 포함되지 않는 것으로 설정된 문자를 포함

하고 있는 경우, 상기 패킷을 폐기하는 단계를 더 포함하는 비정상 패킷 탐지 방법.

**청구항 15**

제12항 내지 제14항 중 어느 한 항에 있어서,

상기 패킷을 비정상 패킷이라고 파악하는 경우, 상기 패킷을 폐기하는 단계를 더 포함하는 비정상 패킷 탐지 방법.

**청구항 16**

SIP(Session Initiation protocol)에 따른 세션 설정에 관한 패킷을 획득하는 단계;

상기 패킷의 헤더의 복수의 필드의 각각이 규정된 문자 길이를 벗어나는 지를 판단하는 단계;

상기 패킷의 헤더의 복수의 필드의 각각이, 상기 SIP에 따른 패킷에 포함되지 않는 것으로 설정된 문자를 포함하고 있는 지를 판단하는 단계;

상기 패킷의 헤더의 복수의 필드의 각각이 규정된 문자 길이를 벗어나지 않고 상기 설정된 문자를 포함하지 않은 경우, 상기 패킷이 속하는 세션을 확인하는 단계;

상기 세션의 상태를 확인하는 단계;

상기 확인된 세션의 상태에서 상기 패킷을 획득한 횟수를 측정하는 단계;

상기 패킷을 획득한 횟수가, 상기 패킷이, SIP를 이용한 공격을 받거나 오류가 발생한 상태를 포함하는 비정상 패킷임을 판단하기 위하여 설정한 소정 횟수 이상인 경우에, 상기 패킷이 비정상 패킷인 것으로 파악하는 단계를 포함하는 비정상 패킷 탐지 방법.

**청구항 17**

삭제

# *명 세 서*

## *발명의 상세한 설명*

### *발명의 목적*

#### *발명이 속하는 기술 및 그 분야의 종래기술*

<10> 본 발명은 인터넷 기반 음성 서비스에서 비정상 패킷을 탐지하는 방법에 관한 것이다.

<11> 인터넷 기반 음성 서비스(Voice over Internet protocol, VoIP)에서 세션을 연결하는 프로토콜에는 H.323과 세션 초기화 프로토콜(Session Initiation protocol, SIP)가 있다. 하지만 H.323은 SIP에 비해서 연결을 맺고 끊는 과정이 복잡하고, 구현을 하기가 SIP에 비해서 어려운 편이다. 그래서, 최근의 VoIP 서비스는 H.323보다 낮은 복잡도, 높은 확장성을 가진 SIP를 이용하고 있다.

<12> 하지만, VoIP도 여러 가지 취약점이 존재하는데 그 수준은 VoIP 사용자를 단순히 신경 쓰이게 하는 수준에서부터, VoIP 서비스 자체를 마비시키는 수준까지 다양하다. VoIP에서의 공격들로 SIP 공격과 RTP(Real-time Transportation Protocol) 공격을 들 수 있다. RTP는 세션 연결 이후 음성데이터를 전송하기 위한 프로토콜이다.

<13> SIP를 이용한 공격으로는 서비스 거부(Denial of Service, DoS) 공격과 유사한 SIP flooding 공격, SIP 헤더의 내용을 변조 하는 비정상 SIP 메시지(Malformed SIP message) 공격 그리고 공격자 자신의 정보를 숨기거나 위장하는 Spoofing 공격이 있다. RTP를 이용한 공격으로는 임의의 음성 정보를 다량으로 특정인에게 전송하는 RTP flooding 공격, 음성 광고를 전송하는 Media spamming 공격 그리고 두 사람간의 전송되는 패킷을 가로채서 도청하는 MITM (Man In The Middle) 공격이 있다.

<14> 인터넷 등에 존재하는 VoIP 공격 툴의 대부분은 SIP flooding 공격을 할 수 있는 패킷 생성기이거나, SIP의 헤더 필드의 내용을 임의로 바꿀 수 있는 툴이다. Spoofing 공격이나 MITM 공격 등은 그 과정이 어렵고 성공할 확

률이 높지 않지만, 비정상 SIP 메시지 공격과 SIP 메시지 Flooding 공격은 앞에서 말한 공개 툴을 이용하여 공격 방법을 다양하고, 손쉽게 행할 수 있다는 점에서 그 위험도가 매우 높다.

<15> 이러한 SIP 기반 VoIP 취약성에 대한 기존의 연구와 논문은 존재 하지만, 이것을 실제로 구현, 적용한 VoIP 서비스들은 거의 존재하지 않고, 있더라도 그 수준이 미흡한 상태이다.

## *발명이 이루고자 하는 기술적 과제*

<16> 본 발명이 이루고자 하는 기술적 과제는 VoIP와 같은 패킷 기반의 음성 서비스에서의 취약점을 탐색할 수 있는 방법 및 프로그램을 기록한 컴퓨터로 읽을 수 있는 매체를 제공하는 것이다.

## *발명의 구성 및 작용*

<17> 본 발명의 한 실시예에 따른 방법을 적어도 하나의 처리기가 실행하도록 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 매체에서, 상기 방법은 패킷을 획득하는 단계와, 상기 패킷의 헤더가 제1 규칙을 위반하는 지를 판단하는 단계와, 상기 패킷의 헤더가 상기 제1 규칙을 만족하는 경우, 상기 패킷이 속하는 세션을 확인하는 단계와, 상기 세션의 상태를 확인하는 단계와, 상기 세션의 상태에서 상기 패킷에 대한 획득하는 것이 제2 규칙을 위반하는 지를 판단하는 단계와, 상기 제2 규칙을 위반하는 경우, 상기 패킷을 비정상이라고 파악하는 단계를 포함한다.

<18> 이때, 상기 제2 규칙을 위반하는 지를 판단하는 단계는, 상기 패킷의 획득으로 상기 세션의 상태에서 상기 패킷을 소정의 횟수 이상 획득하는 지를 파악하는 단계를 포함할 수 있다. 또한 이때, 상기 패킷을 비정상으로 파악하는 단계는, 상기 세션의 상태에서 상기 패킷을 소정의 횟수 이상 획득하는 경우, 상기 패킷을 비정상으로 파악하는 단계를 포함할 수 있다.

<19> 그리고, 상기 제1 규칙을 위반하는 지를 판단하는 단계는, 상기 패킷의 헤더의 복수의 필드의 각각이 규정된 문자 길이를 벗어나는 지를 판단하는 단계와, 상기 패킷의 헤더의 복수의 필드의 각각이 포함되어서는 안되는 문자를 포함하고 있는 지를 판단하는 단계를 포함할 수 있다.

<20> 본 발명의 한 실시예에 따른 비정상 패킷 탐지 방법은 세션 설정에 관한 패킷을 획득하는 단계와, 상기 패킷이 속하는 세션을 확인하는 단계와, 상기 세션의 상태를 확인하는 단계와, 상기 패킷의 획득으로 인하여 상기 세션의 상태에서 상기 패킷을 소정의 횟수 이상으로 수신하는 지를 파악하는 단계와, 상기 세션의 상태에서 상기 패킷을 상기 소정의 횟수 이상으로 수신하는 경우, 상기 패킷을 비정상이라고 파악하는 단계를 포함한다.

<21> 이때, 상기 패킷의 헤더의 복수의 필드의 각각이 규정된 문자 길이를 벗어나는 경우, 상기 패킷을 폐기하는 단계를 더 포함할 수 있다.

<22> 그리고, 상기 패킷의 헤더의 복수의 필드의 각각이 포함되어서는 안되는 문자를 포함하고 있는 경우, 상기 패킷을 폐기하는 단계를 더 포함할 수 있다.

<23> 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.

<24> 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.

<25> 다음은 도 1을 참조하여 본 발명의 실시예에 따른 호출 절차를 설명한다.

<26> 도 1은 본 발명의 실시예에 따른 호출 절차를 도시한 흐름도이다.

<27> 도 1에 도시된 바와 같이, SIP를 위한 시스템은 호출 발신자(caller)인 사용자 에이전트 클라이언트(User Agent Client, UAC)(10), 프록시 서버(20), 프록시 서버(30), 호출 수신자(callee)인 사용자 에이전트 서버(User Agent Server, UAS)(40)를 포함한다.

<28> SIP 메시지에는 요청 메시지와 응답 메시지가 있다. SIP 메시지를 설명하기 위하여, UAC(10)를 클라이언트라 하기로 하고, 프록시 서버(20), 프록시 서버(30), UAS(40) 등을 서버라 하기로 한다.

<29> 요청 메시지는 주로 클라이언트가 서버에 전송하는 메시지로, 호출 요청 메시지(INVITE request message), 확인 메시지(ACK message), 호출 종료 요청 메시지(BYE request message), 취소 요청 메시지(CANCEL request message), 등록 요청 메시지(REGISTER request message), 옵션 요청 메시지(OPTIONS request message)가 있다.

<30> 호출 요청 메시지는 UAC(10)가 UAS(40)를 호출하기 위하여 전송하는 메시지이다.

<31> 확인 메시지는 UAS(40)의 수락 메시지에 대한 UAC(10)의 수신 확인 메시지이다.

<32> 호출 종료 요청 메시지는 생성된 호출을 종료하기 위하여 UAC(10) 또는 UAS(40)가 상대에게 전송하는 메시지이다.

<33> 취소 요청 메시지는 아직 완료되지 않은 요청을 철회하기 위한 메시지이다. 예를 들어 UAC(10)가 UAS(40)를 호출하기 위하여 호출 요청 메시지를 전송한 경우, UAC(10)는 호출을 취소하기 위하여 취소 요청 메시지를 전송한다.

<34> 등록 요청 메시지는 클라이언트가 자신의 위치 정보, SIP 주소, IP(Internet Protocol) 주소 등을 서버에 등록하기 위하여 전송하는 메시지이다.

<35> 옵션 요청 메시지는 서버에 대한 정보를 요구하기 위하여 클라이언트가 전송하는 메시지이다.

<36> 한편, 응답 메시지는 주로 서버가 클라이언트에 전송하는 메시지로, 임시 응답 메시지(Provisional response message), 성공 응답 메시지(Success response message), 리다이렉션 응답 메시지(Redirection response message), 클라이언트 오류 응답 메시지(Client Error response message), 서버 오류 응답 메시지(Server Error response message), 총체적 실패 응답 메시지(Global Failure response message)가 있다.

<37> 임시 응답 메시지는 응답 코드 1XX(100~199)에 해당하는 메시지로, 서버가 요청 메시지를 수신하여 처리 중임을 알리는 메시지이다. 임시 응답 메시지 중에서 응답 코드 100에 해당하는 시도 응답 메시지(Trying response message)는 요청 메시지가 서버에 수신되었으나 최종 목적지에 도달하지 않았음을 알리는 메시지이다. 임시 응답 메시지 중에서 응답 코드 180에 해당하는 링 응답 메시지(Ringing response message)는 요청 메시지가 최종 목적지에 도달하여 처리 대기 상태에 있음을 알리는 메시지이다.

<38> 성공 응답 메시지는 응답 코드 2XX(200~299)에 해당하는 메시지로, 서버가 요청 메시지를 성공적으로 수신하고 이해하여 수용하였음을 알리는 메시지이다. 성공 응답 메시지 중에서 응답 코드 200에 해당하는 수락 응답 메시지(OK response message)는 UAS(40)가 요청을 수락함을 알리기 위한 메시지이다.

<39> 리다이렉션 응답 메시지는 응답 코드 3XX(300~399)에 해당하는 메시지로, 요청 메시지에 해당하는 요청을 완성하기 위하여 필요한 추가적인 동작이 있음을 알리는 메시지이다.

<40> 클라이언트 오류 응답 메시지는 응답 코드 4XX(400~499)에 해당하는 메시지로, 요청 메시지에 오류가 포함되어 있거나 해당 서버가 요청 메시지를 처리할 수 없음을 알리는 메시지이다.

<41> 서버 오류 응답 메시지는 응답 코드 5XX(500~599)에 해당하는 메시지로, 요청 메시지는 유효하나 해당 서버가 요청 메시지를 처리할 수 없음을 알리는 메시지이다.

<42> 총체적 실패 응답 메시지는 응답 코드 6XX(600~699)에 해당하는 메시지로, 요청 메시지에 해당하는 요청이 어떠한 서버에서도 처리될 수 없음을 알리는 메시지이다.

<43> 도 1에 도시된 호출 생성 절차를 살펴보면, 먼저 UAC(10)는 호출 요청 메시지를 프록시 서버(20)에 전송한다(S101).

<44> 호출 요청 메시지를 수신한 프록시 서버(20)는 이를 프록시 서버(30)에 전달하고(S103), 시도 응답 메시지를 UAC(10)에 전송한다(S105).

<45> 호출 요청 메시지를 수신한 프록시 서버(30)는 이를 UAS(40)에 전달하고(S107), 시도 응답 메시지를 프록시 서버(20)에 전송한다(S109).

<46> 호출 요청 메시지를 수신한 UAS(40)는 링 응답 메시지를 프록시 서버(30)에 전송하고(S111), 링 응답 메시지를 수신한 프록시 서버(30)는 이를 프록시 서버(20)에 전달하며(S113), 링 응답 메시지를 수신한 프록시 서버(20)

는 이를 UAC(10)에 전달한다(S115).

<47> UAS(40)가 호출을 수락하는 경우, UAS(40)는 수락 응답 메시지를 프록시 서버(30) 및 프록시 서버(20)를 통해 UAC(10)에 전송한다(S117, S119, 및 S121).

<48> 수락 응답 메시지를 수신한 UAC(10)가 확인 메시지를 UAS(40)에 전송하면(S123), UAC(10)와 UAS(40) 사이에 미디어 세션이 생성된다(S125).

<49> 이 후, 호출을 종료하고자 하는 UAC(10)는 호출 종료 요청 메시지를 UAS(40)에 전송하고(S127), UAS(40)가 수락 응답 메시지를 UAC(10)에 전송함으로써(S129) 미디어 세션은 파괴되고, 호출은 종료된다.

<50> 다음은 도 2를 참조하여 본 발명의 실시예에 따른 SIP 예외 탐지 모듈(100)을 설명한다.

<51> 도 2는 본 발명의 실시예에 따른 SIP 예외 탐지 모듈을 도시한 블록도이다.

<52> 도 2에 도시된 바와 같이, SIP 예외 탐지 모듈(100)은 조작 패킷 탐지 모듈(Malformed SIP Detection Module)(110), 세션 관리 모듈(Session Management Module)(120), 패킷 범람 탐지 모듈(SIP Flooding detection Module)(130), 오류 관리 모듈(Error Management Module)(140), 세션 정보 저장부(Session information database)(150)을 포함한다.

<53> SIP 예외 탐지 모듈(100)은 UAC(10), 프록시 서버(20, 30), UAS(40)의 내부 모듈일 수 있다.

<54> SIP 예외 탐지 모듈(100)이 포함하는 각 모듈에 대하여는 도 3을 참조하여 설명한다.

<55> 도 3은 본 발명의 실시예에 따른 SIP 예외 탐지 방법을 도시한 흐름도이다.

<56> 먼저, 조작 패킷 탐지 모듈(110)은 패킷을 획득하면 이 패킷이 SIP 패킷인지를 확인한다(S201). 조작 패킷 탐지 모듈(110)은 획득한 패킷이 SIP 패킷이 아닌 경우 획득한 패킷을 폐기한다.

<57> 획득한 패킷이 SIP 패킷인 경우, 조작 패킷 탐지 모듈(110)은 획득한 패킷이 SIP 패킷 규칙을 만족하는 지를 확인한다(S203). 획득한 패킷이 SIP 패킷 규칙을 만족하지 않는 경우, 조작 패킷 탐지 모듈(110)은 획득한 패킷을 폐기한다. 획득한 패킷이 SIP 패킷 규칙을 만족하는 경우, 조작 패킷 탐지 모듈(110)은 획득한 패킷을 세션 관리 모듈(120)에 전달한다.

<58> SIP 패킷 규칙에 대하여는 도 4를 참조하여 설명한다.

<59> 도 4는 본 발명의 실시예에 따른 SIP 패킷 규칙을 도시한 도면이다.

<60> 도 4에 도시된 바와 같이, 본 발명의 실시예에 따른 SIP 패킷 규칙은 종래의 RFC 3261에 따른 규칙을 수정한 것이다. 수정된 부분은 도 4에서 굵게 표시되어 있다. 본 발명의 실시예에 따른 SIP 패킷 규칙은 문자 길이 제한, 특수 문자 제한 등을 포함한다.

<61> 조작 패킷 탐지 모듈(110)은 패킷의 헤더가 문자 길이 제한, 특수 문자 제한 등을 위반하는 지를 파악하여, 위반하는 경우 패킷을 폐기한다. 구체적으로, 조작 패킷 탐지 모듈(110)은 패킷의 헤더의 복수의 필드의 각각에 대하여 문자 길이 제한을 벗어나는 지를 파악하여, 문자 길이 제한을 벗어하는 경우 해당 패킷을 폐기한다. 또한, 조작 패킷 탐지 모듈(110)은 패킷의 헤더의 복수의 필드의 각각이 포함되어서는 안 되는 특수 문자를 포함하고 있는 지를 파악하여, 포함하는 경우 해당 패킷을 폐기한다.

<62> 계속하여 도 3에 대하여 설명한다.

<63> 세션 관리 모듈(120)은 세션 정보 저장부(150)를 조회하여 획득한 패킷에 해당하는 세션이 생성되어 있는 지를 확인한다(S205).

<64> 획득한 패킷에 해당하는 세션이 생성되어 있지 않은 경우(S205), 세션 관리 모듈(120)은 해당 세션을 생성하고 세션의 상태를 초기화하며, 생성한 세션의 정보를 세션 정보 저장부(150)에 저장한다(S207).

<65> 세션을 설정한 후, 패킷 범람 탐지 모듈(130)은 획득한 패킷이 요청 메시지인지 응답 메시지인지를 확인한다(S209).

<66> 획득한 패킷이 응답 메시지인 경우, 패킷 범람 탐지 모듈(130)은 세션의 상태가 초기 상태인지를 확인한다(S211). 세션의 상태가 초기 상태인 경우(S211), 패킷 범람 탐지 모듈(130)은 예외 탐지를 종료한다. 세션의 상태가 초기 상태가 아닌 경우(S211), 패킷 범람 탐지 모듈(130)은 획득한 패킷이 송신 메시지인지 아니면 수신

메시지인지를 확인한다(S213).

<67> 한편, 획득한 패킷에 해당하는 세션이 이미 존재 하는 경우(S205), 세션 관리 모듈(120)은 획득한 패킷이 해당 세션의 새로운 요청 메시지인지를 확인한다(S213).

<68> 획득한 패킷이 해당 세션의 새로운 요청 메시지인 경우(S215), 패킷 범람 탐지 모듈(130)은 획득한 패킷이 송신 메시지인지 아니면 수신 메시지인지를 확인한다(S213).

<69> 획득한 패킷이 송신 메시지인 경우(S213), 패킷 범람 탐지 모듈(130)은 획득한 패킷이 호출 요청 메시지인지를 확인한다(S217).

<70> 획득한 패킷이 호출 요청 메시지인 경우, 패킷 범람 탐지 모듈(130)은 획득한 패킷에 해당하는 세션을 호출 클라이언트(INVITE Client)로 처리한다(S219).

<71> 획득한 패킷이 호출 요청 메시지가 아닌 경우, 패킷 범람 탐지 모듈(130)은 획득한 패킷에 해당하는 세션을 비호출 클라이언트(Non-INVITE Client)로 처리한다(S221).

<72> 획득한 패킷이 수신 메시지인 경우(S213), 패킷 범람 탐지 모듈(130)은 획득한 패킷이 호출 요청 메시지인지를 확인한다(S223).

<73> 획득한 패킷이 호출 요청 메시지인 경우(S223), 패킷 범람 탐지 모듈(130)은 획득한 패킷에 해당하는 세션을 호출 서버(INVITE Server)로 처리한다(S225).

<74> 획득한 패킷이 호출 요청 메시지가 아닌 경우(S223), 패킷 범람 탐지 모듈(130)은 획득한 패킷에 해당하는 세션을 비호출 서버(Non-INVITE Server)로 처리한다(S227).

<75> 다음으로, 패킷 범람 탐지 모듈(130)은 획득한 패킷에 해당하는 세션의 상태를 관리한다(S229). 한편, 획득한 패킷이 해당 세션의 새로운 요청 메시지가 아닌 경우에도(S215), 패킷 범람 탐지 모듈(130)은 획득한 패킷에 해당하는 세션의 상태를 관리한다(S229).

<76> 패킷 범람 탐지 모듈(130)이 세션의 상태를 관리하는 방법에 대하여 도 5 내지 도 8을 참조하여 설명한다.

<77> 도 5는 본 발명의 실시예에 따른 호출 클라이언트가 세션의 상태를 관리하는 방법을 도시한 상태 천이도이다.

<78> 도 5에 도시된 바와 같이, 호출 클라이언트의 세션의 상태로는 호출 상태(Calling State)(ST11), 처리 상태(Proceeding State)(ST12), 완료 상태(Completed state)(ST13), 종료 상태(Terminated State)(ST14)가 있다.

<79> 먼저, 호출 클라이언트는 초기 상태에서 호출 요청 메시지를 송신하는 경우 세션의 상태를 호출 상태(ST11)로 천이시킨다(S301).

<80> 호출 상태(ST11)에서 타이머 A가 만료되는 경우, 호출 클라이언트는 타이머 A를 리셋시키고, 호출 요청 메시지를 재전송한다(S303). 이때, RFC 3261에 따르면, 타이머 A는 T1(500 miliseconds) 후에 만료된다.

<81> 호출 클라이언트는 호출 상태(ST11)에서 응답 코드 2XX에 해당하는 성공 응답 메시지를 수신하는 경우에, 확인 메시지를 전송하고, 세션의 상태를 종료 상태(ST14)로 천이시킨다(S305).

<82> 호출 클라이언트는 호출 상태(ST11)에서 응답 코드 1XX에 해당하는 임시 응답 메시지를 수신하는 경우에, 세션의 상태를 처리 상태(ST12)로 천이시킨다(S307).

<83> 호출 상태(ST11)에서 타이머 B가 만료되거나 호출 클라이언트가 에러를 전송하는 경우에, 호출 클라이언트는 세션의 상태를 종료 상태(ST14)로 천이시킨다(S309). 이때, RFC 3261에 따르면, 타이머 B는 T1*64 miliseconds 후에 만료된다.

<84> 호출 클라이언트는 처리 상태(ST12)에서 응답 코드 1XX에 해당하는 임시 응답 메시지를 수신하는 경우에, 세션의 상태를 처리 상태(ST12)로 유지시킨다(S311).

<85> 호출 클라이언트는 처리 상태(ST12)에서 응답 코드 2XX에 해당하는 성공 응답 메시지를 수신하는 경우에, 확인 메시지를 전송하고, 세션의 상태를 종료 상태(ST14)로 천이시킨다(S313).

<86> 호출 클라이언트는 처리 상태(ST12)에서 300부터 699까지의 응답 코드에 해당하는 응답 메시지를 수신하는 경우에, 확인 메시지를 전송하고, 세션의 상태를 완료 상태(ST13)로 천이시킨다(S315).

<87> 한편, 호출 클라이언트는 호출 상태(ST11)에서 300부터 699까지의 응답 코드에 해당하는 응답 메시지를 수신하

는 경우에, 확인 메시지를 전송하고, 세션의 상태를 완료 상태(ST13)로 천이시킨다(S317).

<88> 호출 클라이언트는 완료 상태(ST13)에서 300부터 699까지의 응답 코드에 해당하는 응답 메시지를 수신하는 경우에, 확인 메시지를 전송하고, 세션의 상태를 완료 상태(ST13)로 유지시킨다(S319).

<89> 호출 클라이언트는 완료 상태(ST13)에서 에러를 전송하는 경우에 세션의 상태를 종료 상태(ST14)로 천이 시킨다(S321).

<90> 완료 상태(ST13)에서 타이머 D가 만료되는 경우에, 호출 클라이언트는 세션의 상태를 종료 상태(ST14)로 천이시킨다(S323). 이때, RFC 3261에 따르면, 타이머 D는 32000 milliseconds 후에 만료된다.

<91> 호출 클라이언트는 호출 상태(ST11)에서 호출 요청 메시지를 소정의 횟수 이상으로 전송하는 경우, 비정상(공격 또는 오류)으로 판단한다(S325).

<92> 호출 클라이언트는 처리 상태(ST12)에서 응답 메시지를 소정의 횟수 이상으로 수신하거나 호출 요청 메시지를 전송하는 경우, 비정상(공격 또는 오류)으로 판단한다(S327).

<93> 호출 클라이언트는 완료 상태(ST13)에서 응답 메시지를 소정의 횟수 이상으로 수신하거나 호출 요청 메시지를 전송하는 경우, 비정상(공격 또는 오류)으로 판단한다(S329).

<94> 도 6은 본 발명의 실시예에 따른 호출 서버가 세션의 상태를 관리하는 방법을 도시한 상태 천이도이다.

<95> 도 6에 도시된 바와 같이, 호출 서버의 세션의 상태로는 처리 상태(Proceeding State)(ST21), 완료 상태(Completed State)(ST22), 확인 상태(Confirmed State)(ST23), 종료 상태(Terminated State)(ST24)가 있다.

<96> 호출 서버는 초기 상태에서 호출 요청 메시지를 수신하는 경우 세션의 상태를 처리 상태(ST21)로 천이시킨다(S401).

<97> 호출 서버는 처리 상태(ST21)에서 응답 코드 1XX에 해당하는 임시 응답 메시지를 전송하는 경우, 세션의 상태를 처리 상태(ST21)로 유지한다(S403).

<98> 호출 서버는 처리 상태(ST21)에서 호출 요청 메시지를 다시 수신하는 경우, 100에 해당하는 시도 응답 메시지를 전송하고 세션의 상태를 처리 상태(ST21)로 유지한다(S405).

<99> 호출 서버는 처리 상태(ST21)에서 응답 코드 2XX에 해당하는 성공 응답 메시지를 전송하는 경우, 세션의 상태를 종료 상태(ST24)로 천이시킨다(S407).

<100> 처리 상태(ST21)에서 타이머 B가 만료하거나 호출 서버가 오류를 전송하는 경우, 호출 서버는 세션의 상태를 종료 상태(ST24)로 천이시킨다(S408).

<101> 호출 서버는 처리 상태(ST21)에서 300부터 699까지의 응답 코드에 해당하는 응답 메시지를 전송하는 경우, 세션의 상태를 완료 상태(ST22)로 천이시키다(S409).

<102> 호출 서버는 완료 상태(ST22)에서 호출 요청 메시지를 수신하거나 응답 코드 100에 해당하는 시도 응답 메시지를 전송하는 경우에, 세션의 상태를 완료 상태(ST22)로 유지한다(S411).

<103> 호출 서버는 완료 상태(ST22)에서 오류를 전송하는 경우, 세션의 상태를 종료 상태(ST24)로 천이시킨다(S413).

<104> 호출 서버는 완료 상태(ST22)에서 확인 메시지를 수신하는 경우, 세션의 상태를 확인 상태(ST23)로 천이시킨다(S415).

<105> 호출 서버는 확인 상태(ST23)에서 확인 메시지를 다시 수신하는 경우, 세션의 상태를 확인 상태(ST23)로 유지한다(S417).

<106> 확인 상태(ST23)에서 타이머 I가 만료하는 경우, 호출 서버는 세션의 상태를 종료 상태(ST24)로 천이시킨다(S419). 이때, RFC 3261에 따르면, 타이머 I는 T4 (4000 milliseconds) 후에 만료된다.

<107> 호출 서버는 처리 상태(ST21)에서 호출 요청 메시지를 소정의 횟수 이상으로 수신하거나 응답 메시지를 소정의 횟수 이상으로 전송하는 경우, 비정상(공격 또는 오류)으로 판단한다(S421).

<108> 호출 서버는 완료 상태(ST22)에서 호출 요청 메시지를 소정의 횟수 이상으로 수신하는 경우, 비정상(공격 또는 오류)로 판단한다(S423).

<109> 호출 서버는 확인 상태(ST23)에서 호출 요청 메시지를 수신하거나 확인 메시지를 소정의 횟수 이상으로 수신하

거나 응답 메시지를 수신하는 경우, 비정상(공격 또는 오류)로 판단한다(S425).

<110> 도 7은 본 발명의 실시예에 따른 비호출 클라이언트가 세션의 상태를 관리하는 방법을 도시한 상태 천이도이다.

<111> 도 7에 도시된 바와 같이, 비호출 클라이언트의 세션의 상태로는 시도 상태(Trying State)(ST31), 처리 상태(Proceeding State)(ST32), 완료 상태(Completed state)(ST33), 종료 상태(Terminated State)(ST34)가 있다.

<112> 비호출 클라이언트는 초기 상태에서 호출 요청 메시지를 제외한 요청 메시지인 비호출 요청 메시지를 송신하는 경우, 세션의 상태를 시도 상태(ST31)로 천이시킨다(S501).

<113> 시도 상태(ST31)에서 타이머 E가 만료하는 경우, 비호출 클라이언트는 비호출 요청 메시지를 다시 송신하고, 세션의 상태를 시도 상태(ST31)로 유지한다(S503). 이때, RFC 3261에 따르면, 타이머 E는 T1(500 milliseconds) 후에 만료된다.

<114> 시도 상태(ST31)에서 타이머 F가 만료하거나 비호출 클라이언트가 오류를 전송하는 경우, 비호출 클라이언트는 세션의 상태를 종료 상태(ST34)로 천이시킨다(S505). 이때, RFC 3261에 따르면, 타이머 F는 T1*64 milliseconds 후에 만료된다.

<115> 비호출 클라이언트는 시도 상태(ST31)에서 200부터 699까지의 응답 코드에 해당하는 응답 메시지를 수신하는 경우, 세션의 상태를 완료 상태(ST33)로 천이시킨다(S507).

<116> 비호출 클라이언트는 시도 상태(ST31)에서 응답 코드 1xx에 해당하는 임시 응답 메시지를 수신하는 경우, 세션의 상태를 처리 상태(ST32)로 천이시킨다(S509).

<117> 처리 상태(ST32)에서 타이머 E가 만료하는 경우, 비호출 클라이언트는 비호출 요청 메시지를 송신하고, 세션의 상태를 처리 상태(ST32)로 유지한다(S511).

<118> 비호출 클라이언트는 처리 상태(ST32)에서 응답 코드 1xx에 해당하는 임시 응답 메시지를 수신하는 경우, 세션의 상태를 처리 상태(ST32)로 유지한다(S513).

<119> 처리 상태(ST32)에서 타이머 F가 만료하거나 비호출 클라이언트가 오류를 전송하는 경우, 비호출 클라이언트는 세션의 상태를 종료 상태(ST34)로 천이시킨다(S515).

<120> 비호출 클라이언트는 처리 상태(ST32)에서 200부터 699까지의 응답 코드에 해당하는 응답 메시지를 수신하는 경우, 세션의 상태를 완료 상태(ST33)로 천이시킨다(S517).

<121> 완료 상태(ST33)에서 타이머 K가 만료하는 경우, 비호출 클라이언트는 세션의 상태를 종료 상태(ST34)로 천이시킨다(S519). 이때, RFC 3261에 따르면, 타이머 K는 T4(4000 milliseconds) 후에 만료된다.

<122> 비호출 클라이언트는 시도 상태(ST31)에서 비호출 요청 메시지를 소정의 횟수 이상으로 전송하는 경우, 비정상(공격 또는 오류)으로 판단한다(S521).

<123> 비호출 클라이언트는 처리 상태(ST32)에서 비호출 클라이언트를 소정의 횟수 이상으로 전송하거나 응답 메시지를 소정의 횟수 이상으로 수신하는 경우, 비정상(공격 또는 오류)으로 판단한다(S523).

<124> 비호출 클라이언트는 완료 상태(ST33)에서 비호출 요청 메시지를 전송하거나 응답 메시지를 수신하는 경우, 비정상(공격 또는 오류)을 판단한다(S525).

<125> 도 8은 본 발명의 실시예에 따른 비호출 서버가 세션의 상태를 관리하는 방법을 도시한 상태 천이도이다.

<126> 도 8에 도시된 바와 같이, 비호출 서버의 세션의 상태로는 시도 상태(Trying State)(ST41), 처리 상태(Proceeding State)(ST42), 완료 상태(Completed state)(ST43), 종료 상태(Terminated State)(ST44)가 있다.

<127> 비호출 서버는 초기 상태에서 비호출 요청 메시지를 수신하는 경우, 세션의 상태를 시도 상태(ST41)로 천이시킨다(S601).

<128> 비호출 서버는 시도 상태(ST41)에서 200부터 699까지의 응답 코드에 해당하는 응답 메시지를 전송하는 경우, 세션의 상태를 완료 상태(ST43)로 천이시킨다(S603).

<129> 비호출 서버는 시도 상태(ST41)에서 응답 코드 1xx에 해당하는 임시 응답 메시지를 전송하는 경우, 세션의 상태를 처리 상태(ST42)로 천이시킨다(S605).

<130> 비호출 서버는 처리 상태(ST42)에서 비호출 요청 메시지를 수신하는 경우, 응답 메시지를 전송하고 세션의 상태

를 처리 상태(ST42)로 유지시킨다(S607).

<131> 비호출 서버는 처리 상태(ST42)에서 응답 코드 1xx에 해당하는 임시 응답 메시지를 전송하는 경우, 세션의 상태를 처리 상태(ST42)로 유지시킨다(S609).

<132> 비호출 서버는 처리 상태(ST42)에서 오류를 전송하는 경우, 세션의 상태를 종료 상태(ST44)로 천이시킨다(S611).

<133> 비호출 서버는 처리 상태(ST42)에서 200부터 699까지의 응답 코드에 해당하는 응답 메시지를 전송하는 경우, 세션의 상태를 완료 상태(ST43)로 천이시킨다(S613).

<134> 비호출 서버는 완료 상태(ST43)에서 비호출 요청 메시지를 수신하는 경우, 응답 메시지를 전송하고 세션의 상태를 완료 상태(ST43)로 유지시킨다(S615).

<135> 완료 상태(ST43)에서 타이머 J가 만료하거나 비호출 서버가 오류를 전송하는 경우, 비호출 서버는 세션의 상태를 종료 상태(ST44)로 천이시킨다(S617). 이때, RFC 3261에 따르면, 타이머 J는 T1*64 milliseconds 후에 만료된다.

<136> 비호출 서버는 시도 상태(ST41)에서 비호출 요청 메시지를 수신하는 경우, 비정상(공격 또는 오류)으로 판단한다(S619).

<137> 비호출 서버는 처리 상태에서 비호출 요청 메시지를 소정의 횟수 이상으로 수신하거나 응답 메시지를 소정의 횟수 이상으로 전송하는 경우, 비정상(공격 또는 오류)으로 판단한다(S621).

<138> 비호출 서버는 완료 상태에서 비호출 요청 메시지를 소정의 횟수 이상으로 수신하거나 응답 메시지를 소정의 횟수 이상으로 전송하는 경우, 비정상(공격 또는 오류)으로 판단한다(S623).

<139> 계속하여 도 3을 설명한다.

<140> 오류 관리 모듈(140)은 패킷 범람 탐지 모듈(130)로부터 오류에 관한 정보를 수신한다(S231). 오류 관리 모듈(140)은 획득한 패킷이 오류라고 판단되는 경우, 해당 패킷을 폐기한다.

<141> 그리고, 오류 관리 모듈(140)은 세션의 상태가 종료 상태인지를 파악한다(S233).

<142> 세션의 상태가 종료 상태인 경우, 오류 관리 모듈(140)은 해당 세션을 삭제(destroy)하고(S235) 획득한 패킷에 대한 처리를 종료한다.

<143> 다음은 도 9를 참조하여 본 발명의 실시예에 따른 SIP 패킷의 오류 탐지 방법의 효과를 설명한다.

<144> 도 9는 본 발명의 실시예의 효과를 보여주는 그래프이다.

<145> 도 9를 참조하면, SIP를 규정하는 RFC 3261에 따라 예외 상황을 탐지하는 것 보다 본 발명의 실시예에 따라 예외 상황을 탐지하는 것이 더 효과적임을 알 수 있다.

<146> 특히, 본 발명의 효과를 알아보기 위하여, 실제로 SIP 패킷 생성기와 SIP 공격 탐지기를 구현하여 실험하였다. 비정상 SIP 메시지 공격으로는 2426개의 SIP 헤더가 변조된 패킷을 사용하였으며, 실험 결과 단순히 RFC 규칙을 따를 때는 34.9%의 공격 패킷이 탐지되었지만, 본 발명의 실시예에 따른 방법을 적용하는 경우 10.67%만이 탐지가 되지 않았다. 하지만 실험 군중에는 상황에 따라서는 정상이라고 판단할 수 있는 경우도 있어서, 이 같은 경우를 제외하면 거의 100% 비정상 SIP 메시지를 탐지한다고 볼 수 있다.

<147> SIP flooding 공격 실험을 위해서는 전 세계적으로 많이 사용되는 VoIP 서비스 업체 중에 무료이면서 SIP를 기반으로 하는 서비스를 5개 선정하였다. 이 서비스들의 바탕으로 정상적인 상황의 SIP 패킷 전송을 분석하였고, 그 결과 State transaction 모델에서 SIP flooding 공격의 기준점이 설정될 수 있었다. 정상적인 경우 각 상태(State)당 송수신하는 SIP 패킷의 수가 초당 8개를 넘지 않았고, 이 값을 기준점으로 하여 5개의 서로 다른 PPS(Packet Per Second)를 적용하여, SIP flooding 공격의 탐지 가능 여부를 실험하였다. 적용된 PPS는 1pps, 3pps, 5pps, 10pps, 34pps이다. 1pps의 경우에는 그 속도가 매우 느려 flooding 공격으로 간주 되지 않았으며, 3pp는 3.1초 뒤, 5pps는 1.9초 뒤, 10pps는 0.8초 뒤, 34pps는 0.2초 뒤에 SIP flooding 공격이라고 탐지되었다. State 당 8pps의 기준점이 적용된다는 점을 감안하면 5pps 이상부터가 SIP flooding 공격으로 간주된다고 할 수 있다.

<148> 본 발명의 실시예는 이상에서 설명한 장치 및/또는 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시

예의 구성에 대응하는 기능을 실현하기 위한 프로그램, 그 프로그램이 기록된 기록 매체 등을 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

<149> 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.

## *발명의 효과*

<150> 본 발명의 실시예에 따르면, VoIP와 같은 패킷 기반의 음성 서비스에서 비정상적인 패킷이 용이하게 탐지될 수 있다.

<151> 특히, 본 발명의 실시예에 따르면, 비정상 SIP 메시지 공격과 SIP 메시지 Flooding 공격이 용이하게 탐지될 수 있다.

## *도면의 간단한 설명*

<1> 도 1은 본 발명의 실시예에 따른 호출 절차를 도시한 흐름도이다.

<2> 도 2는 본 발명의 실시예에 따른 SIP 예외 탐지 모듈을 도시한 블록도이다.

<3> 도 3은 본 발명의 실시예에 따른 SIP 예외 탐지 방법을 도시한 흐름도이다.

<4> 도 4는 본 발명의 실시예에 따른 SIP 패킷 규칙을 도시한 도면이다.

<5> 도 5는 본 발명의 실시예에 따른 호출 클라이언트가 세션의 상태를 관리하는 방법을 도시한 상태 천이도이다.

<6> 도 6은 본 발명의 실시예에 따른 호출 서버가 세션의 상태를 관리하는 방법을 도시한 상태 천이도이다.

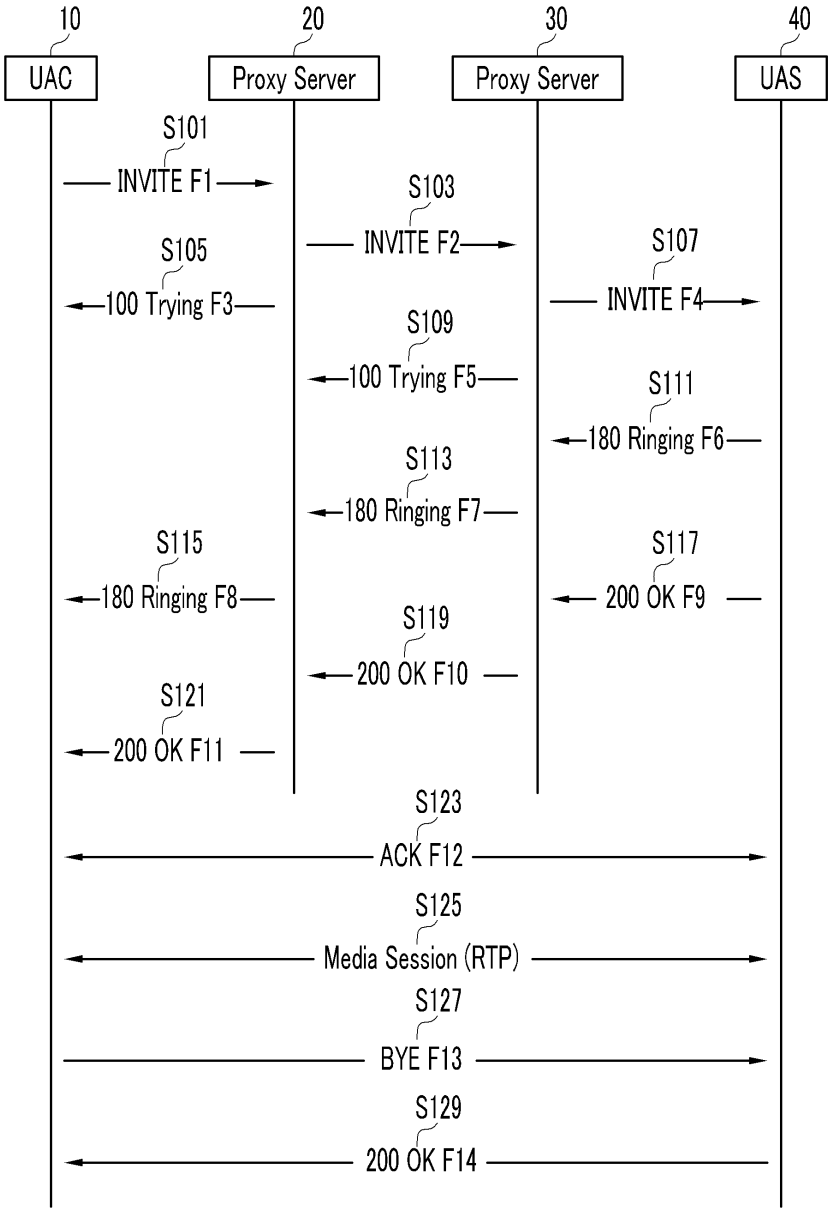
<7> 도 7은 본 발명의 실시예에 따른 비호출 클라이언트가 세션의 상태를 관리하는 방법을 도시한 상태 천이도이다.

<8> 도 8은 본 발명의 실시예에 따른 비호출 서버가 세션의 상태를 관리하는 방법을 도시한 상태 천이도이다.

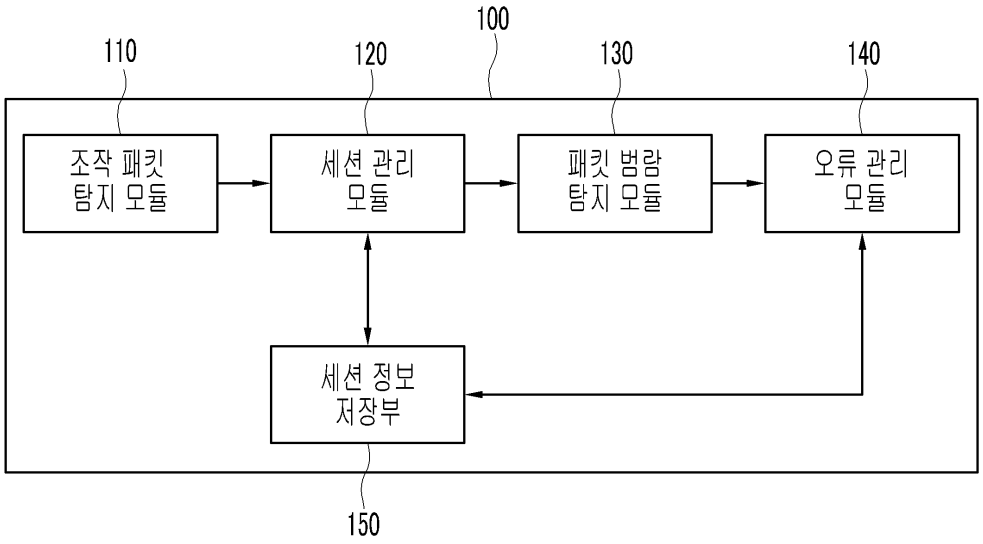
<9> 도 9는 본 발명의 실시예의 효과를 보여주는 그래프이다.

## 도면

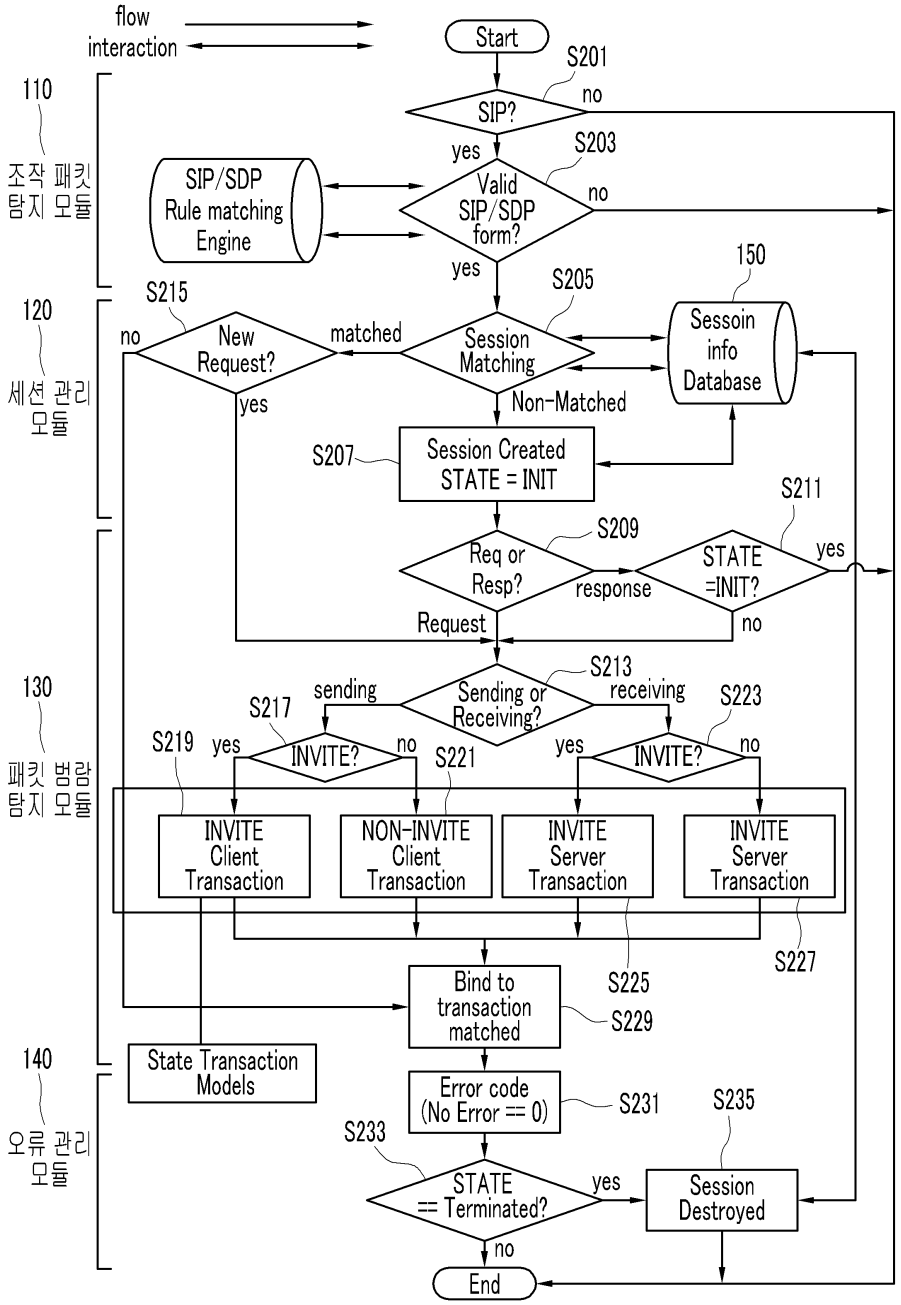
### 도면1


10
20
30
40
UAC
Proxy Server
Proxy Server
UAS
S101
INVITE F1
S103
INVITE F2
S105
100 Trying F3
S107
INVITE F4
S109
100 Trying F5
S111
180 Ringing F6
S113
180 Ringing F7
S115
180 Ringing F8
S117
200 OK F9
S119
200 OK F10
S121
200 OK F11
S123
ACK F12
S125
Media Session (RTP)
S127
BYE F13
S129
200 OK F14

도면2


100
110
120
130
140
조작 패킷
탐지 모듈
세션 관리
모듈
패킷 범람
탐지 모듈
오류 관리
모듈
세션 정보
저장부
150

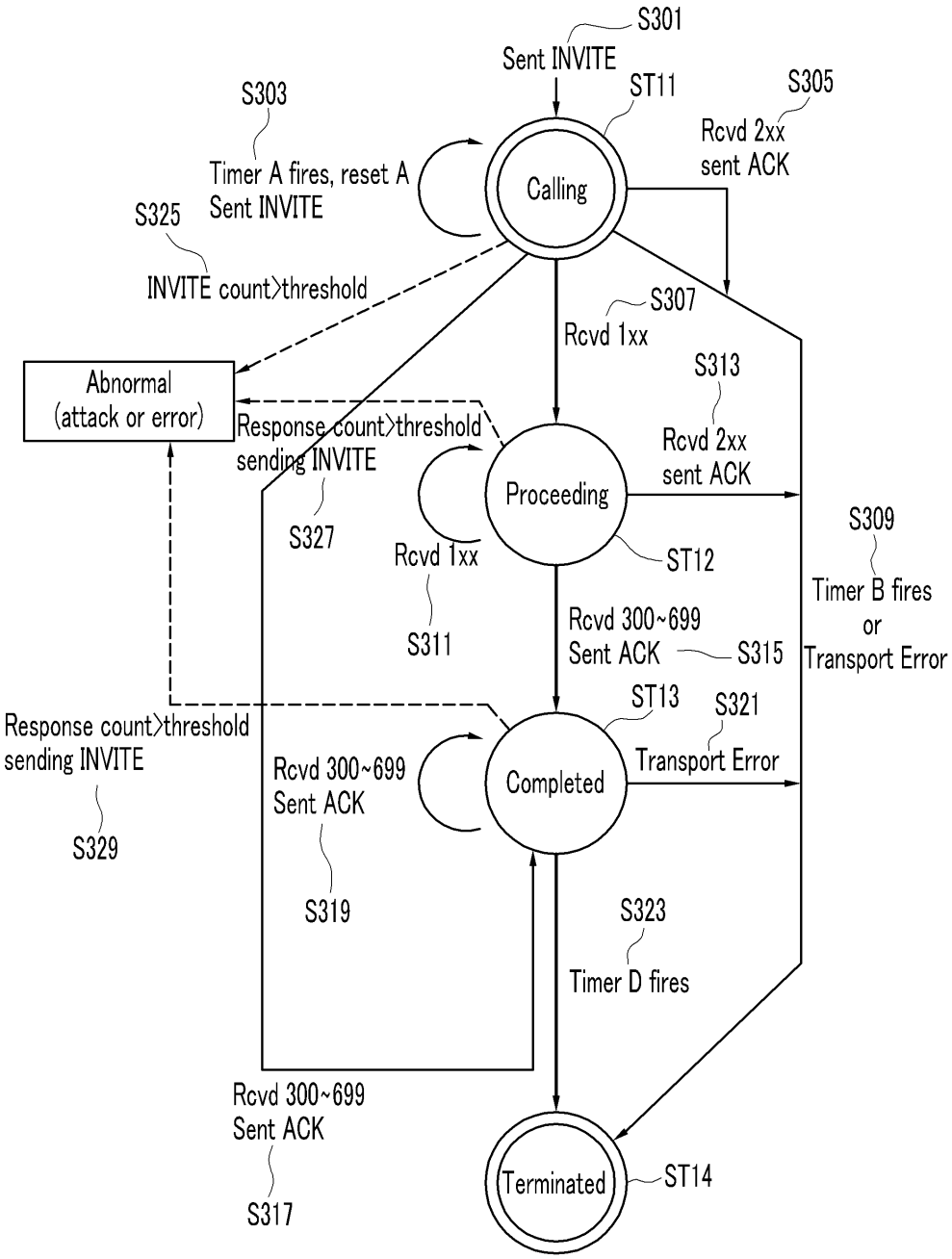
도면3


flow
interaction
Start
S201
SIP?
no
yes
S203
Valid SIP/SDP form?
no
SIP/SDP Rule matching Engine
yes
S205
150
Sessoin info Database
110
조작 패킷 탐지 모듈
S215
120
세션 관리 모듈
no
New Request?
matched
Session Matching
yes
Non-Matched
S207
Session Created STATE = INIT
S211
S209
Req or Resp?
response
STATE =INIT?
yes
Request
no
S213
130
패킷 범람 탐지 모듈
sending
Sending or Receiving?
receiving
S223
S217
S219
yes
INVITE?
no
S221
yes
INVITE?
no
INVITE Client Transaction
NON-INVITE Client Transaction
INVITE Server Transaction
INVITE Server Transaction
S227
S225
Bind to transaction matched
S229
140
오류 관리 모듈
State Transaction Models
Error code (No Error == 0)
S231
S235
S233
STATE == Terminated?
yes
Session Destroyed
no
End

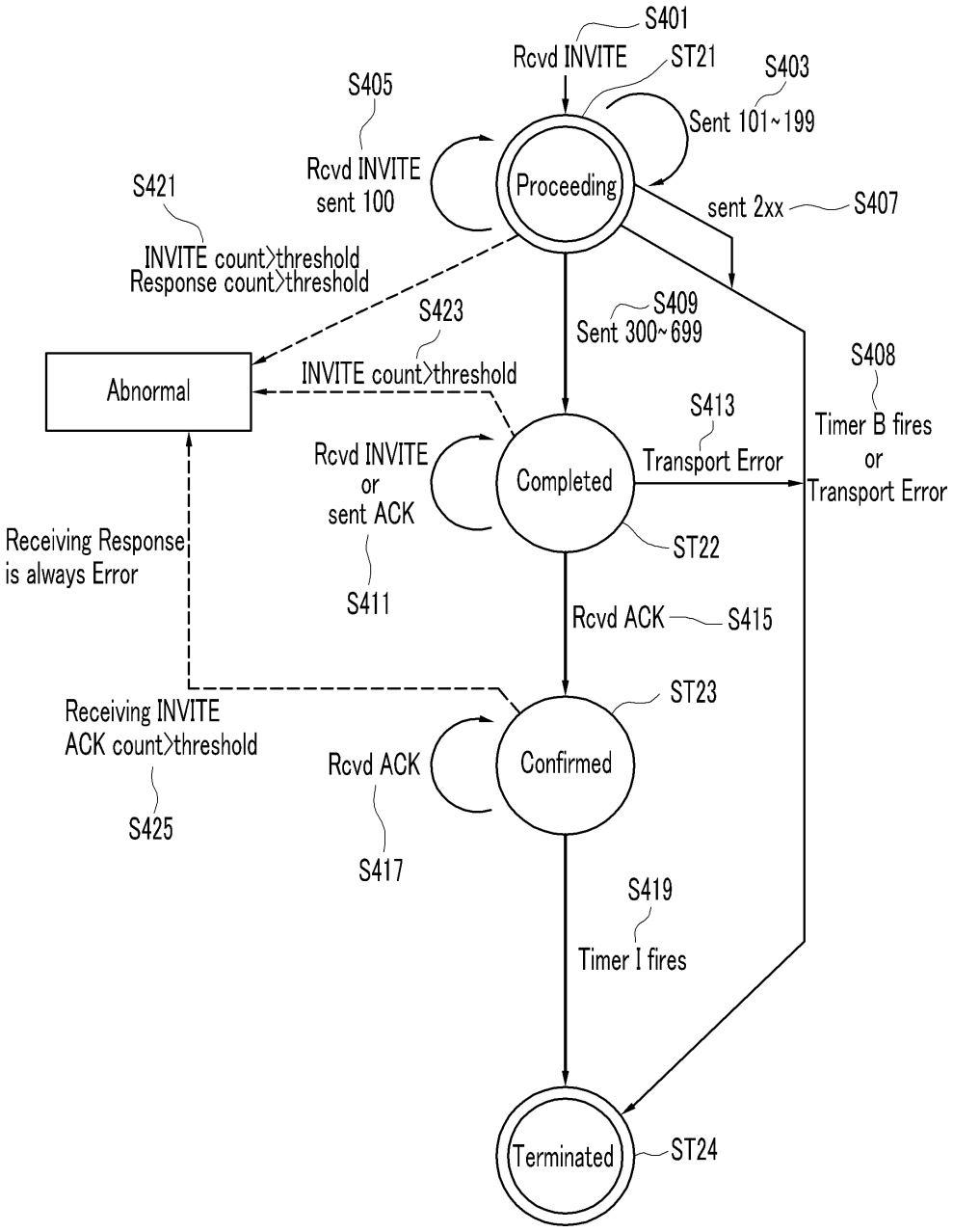
| Original RFC rules | Improved rules |
|---|---|
| user:((#unreserved#\|#escaped#\|#user_unreserved#)+) | user:((**#alphanum#**\|_\|\-)+**{1,12}**) |
| userinfo:((#user#)(\:#password#)?\@) | userinfo:(((#user#)(\:#password#)?\@)**{2,26}**) |
| password:((#unreserved#\|#escaped#\|\&\|\=\|\+\|\$\|\.)*) | password:(((#unreserved#\|#escaped#\|\&\|\=\|\+\|\$\|\.)*)**{0,12}**) |
| SIP_Version:(SIP\/\d\.\d) | SIP_Version:((SIP\/\d\.\d)**{7,9}**) |
| port:(\d+) | port:(\d{4,5}) |
| hostname:((#domainlabel#\.)*#toplabel#(\.)?) | hostname:(((#domainlabel#\.)*#toplabel#(\.)?)**{3,255}**) |
| extension_method:(#token#) | extension_method:(**#ASCII_NAME#{1,20}**) |
| uric_no_slash:(#unreserved#\|#escaped#\|\;\|\?\|\:\|\@\|\&\|\=\|\+\|\$\|\,) | uric_no_slash:(#unreserved#\|#escaped#\|**\;\|\?\|\&**\|\=\|\+\|\$\|\,) |
| protocol_version:(#token#) | protocol_version:(\d**{1,2}**\.\d**{1,2}**) |
| protocol_name:(SIP\|#token#) | protocol_name:(SIP\|**\w{1,10}**) |
| display_name:((#token##LWS#)*\|#quoted_string#) | display_name:((**\w**\| )**{1,32}**\|#quoted_string#) |
| callid:(#word#(\@#word#)?) | callid:(**#ASCII#{1,50}**(\@(**\w\.***){**1,32**})?) |
| delta_seconds:(\d+) | delta_seconds:(\d**{1,4}**) |
| Max-Forwards:(Max-Forwards#HCOLON#\d+#CRLF#) | Max-Forwards:(Max-Forwards#HCOLON#\d**{1,4}**#CRLF#) |
| x_token:(x\-#token#) | x_token:(x\-**\w{1,32}**) |
| ietf_token:(#token#) | ietf_token:(**\w{1,32}**) |
| iana_token:(#token#) | iana_token:(**\w{1,32}**) |

도면4

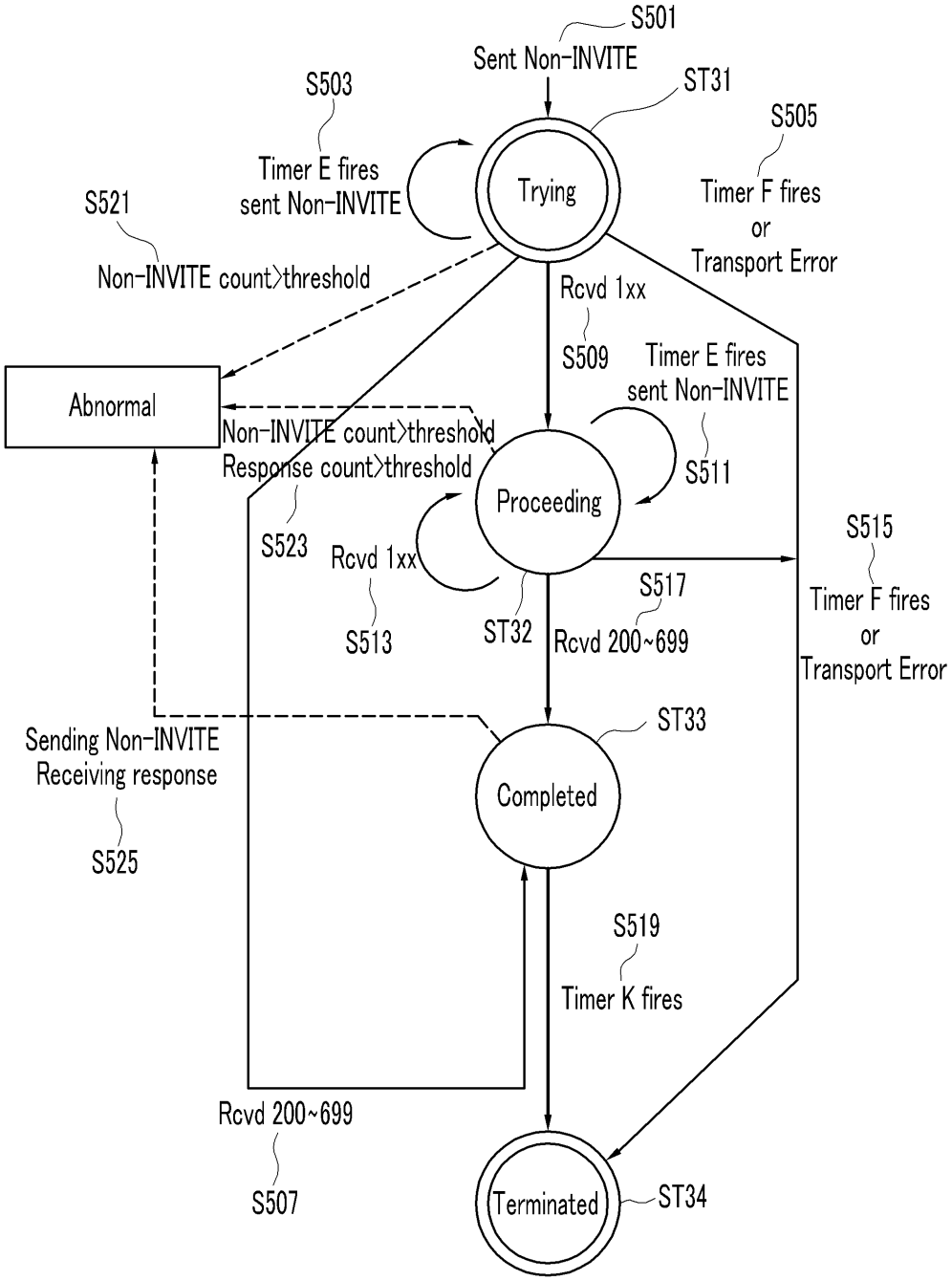
도면5


S301
Sent INVITE
ST11
S305
Rcvd 2xx
sent ACK
S303
Timer A fires, reset A
Sent INVITE
Calling
S325
INVITE count>threshold
S307
Rcvd 1xx
S313
Abnormal
(attack or error)
Response count>threshold
sending INVITE
Rcvd 2xx
sent ACK
S327
Proceeding
S309
Timer B fires
or
Transport Error
Rcvd 1xx
ST12
S311
Rcvd 300~699
Sent ACK
S315
ST13
S321
Response count>threshold
sending INVITE
Transport Error
Rcvd 300~699
Sent ACK
Completed
S329
S319
S323
Timer D fires
Rcvd 300~699
Sent ACK
S317
Terminated
ST14

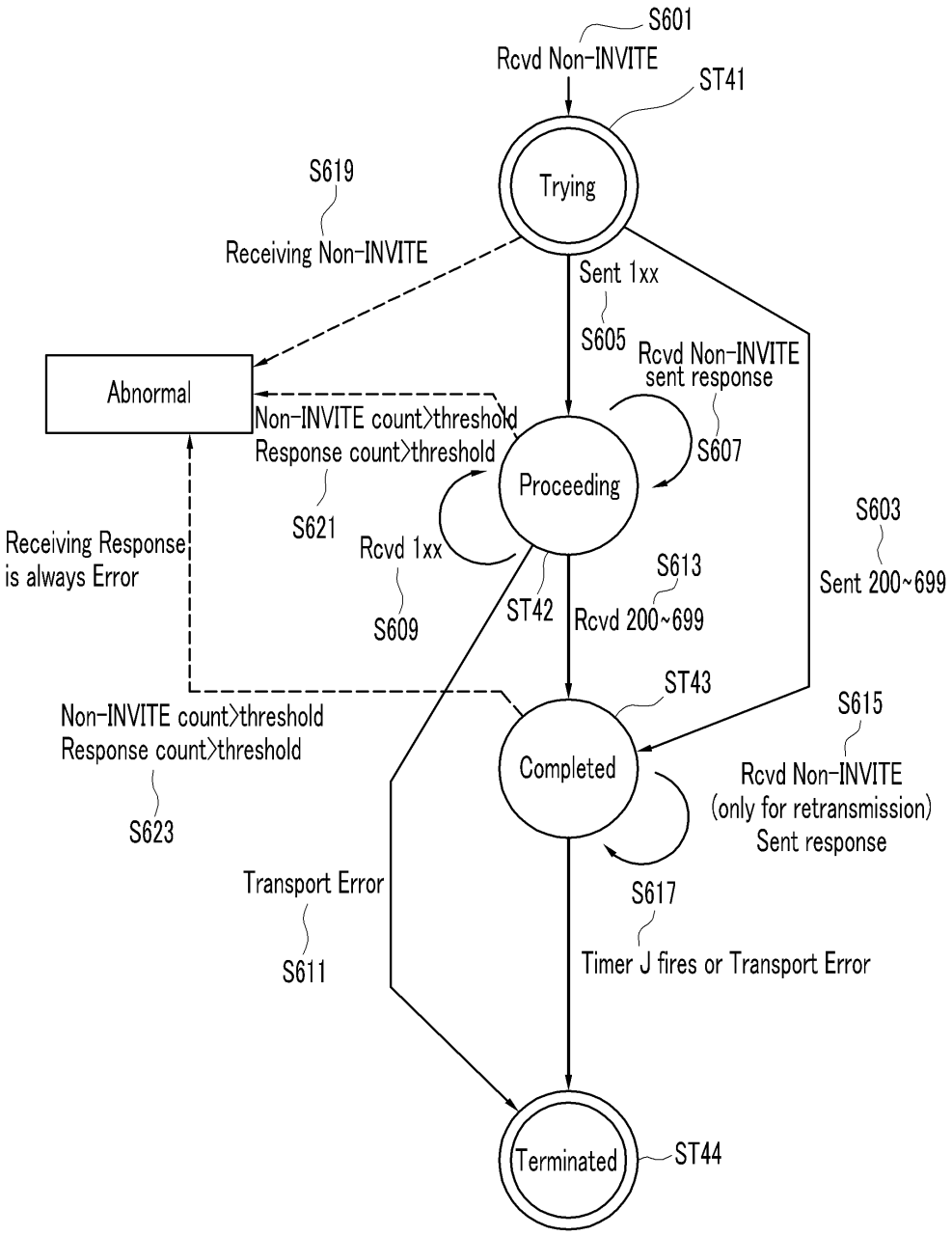
도면6


S401
Rcvd INVITE
ST21
S403
Sent 101~199
S405
Rcvd INVITE
sent 100
Proceeding
S421
INVITE count>threshold
Response count>threshold
sent 2xx
S407
S423
S409
Sent 300~699
S408
Abnormal
INVITE count>threshold
S413
Timer B fires
or
Transport Error
Rcvd INVITE
or
sent ACK
Completed
Transport Error
Receiving Response
is always Error
ST22
S411
Rcvd ACK
S415
ST23
Receiving INVITE
ACK count>threshold
Rcvd ACK
Confirmed
S425
S417
S419
Timer I fires
Terminated
ST24

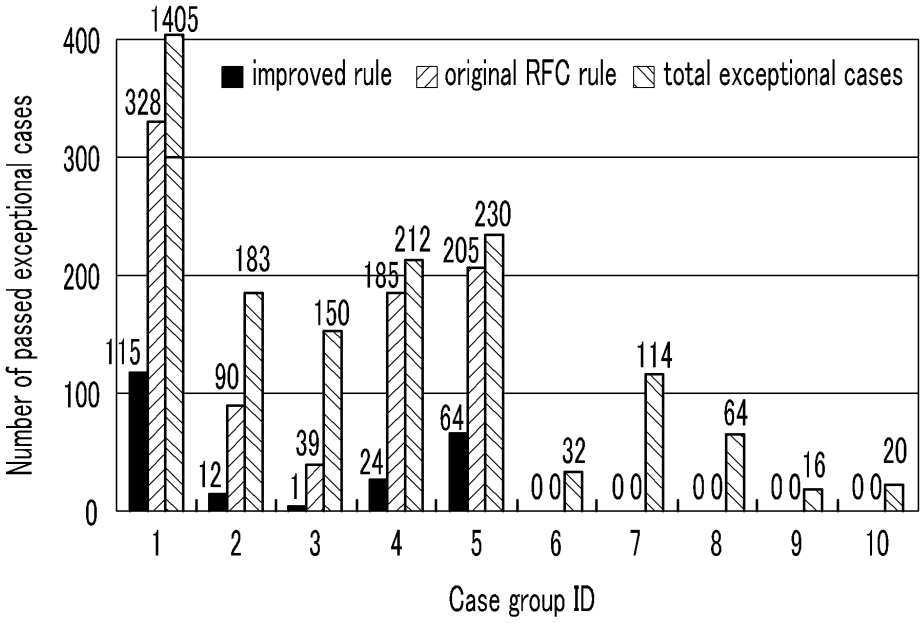
도면7


S501
Sent Non-INVITE
ST31
S503
Timer E fires
sent Non-INVITE
Trying
S505
Timer F fires
or
Transport Error
S521
Non-INVITE count>threshold
Rcvd 1xx
S509
Timer E fires
sent Non-INVITE
Abnormal
Non-INVITE count>threshold
Response count>threshold
Proceeding
S511
S523
Rcvd 1xx
S513
ST32
S517
Rcvd 200~699
S515
Timer F fires
or
Transport Error
Sending Non-INVITE
Receiving response
S525
ST33
Completed
S519
Timer K fires
Rcvd 200~699
S507
Terminated
ST34

도면8


S601
Rcvd Non-INVITE
ST41
Trying
S619
Receiving Non-INVITE
Sent 1xx
S605
Rcvd Non-INVITE
sent response
S607
Abnormal
Non-INVITE count>threshold
Response count>threshold
S621
Proceeding
S603
Sent 200~699
Receiving Response
is always Error
Rcvd 1xx
S609
ST42
S613
Rcvd 200~699
ST43
S615
Non-INVITE count>threshold
Response count>threshold
S623
Completed
Rcvd Non-INVITE
(only for retransmission)
Sent response
S617
Transport Error
S611
Timer J fires or Transport Error
Terminated
ST44

도면9


improved rule
original RFC rule
total exceptional cases
Number of passed exceptional cases
Case group ID
400
300
200
100
0
1
2
3
4
5
6
7
8
9
10
115
328
1405
12
90
183
1
39
150
24
185
212
64
205
230
0 0
32
0 0
114
0 0
64
0 0
16
0 0
20