



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0043373
(43) 공개일자 2011년04월27일

(51) Int. Cl.

H04L 12/22 (2006.01) H04L 29/06 (2006.01)

(21) 출원번호 10-2009-0100463

(22) 출원일자 2009년10월21일

심사청구일자 2009년10월21일

(71) 출원인

충남대학교산학협력단

대전광역시 유성구 공동 220번지 충남대학교

한신대학교 산학협력단

경기 오산시 양산동 한신대학교내

이형우

경기도 용인시 기흥구 중동 성산마을서해그랑블
3101동 501호

(72) 발명자

이형우

경기도 용인시 기흥구 중동 성산마을서해그랑블
3101동 501호

김태수

경기도 가평군 가평읍 읍내9리 445-2번지

(뒷면에 계속)

(74) 대리인

특허법인태동

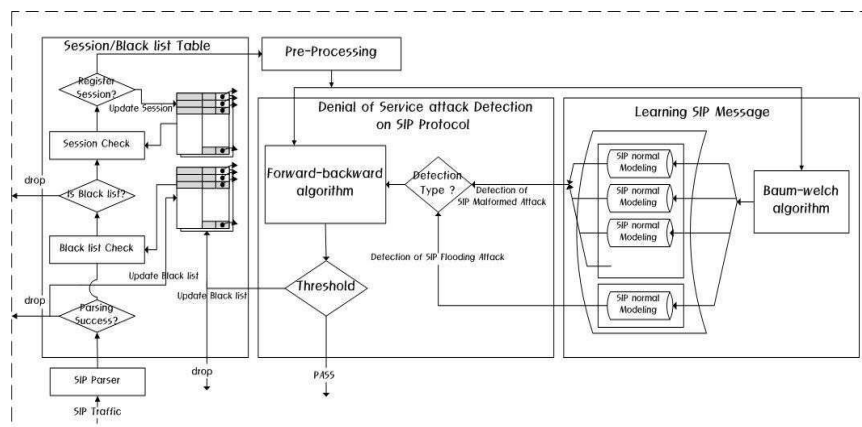
전체 청구항 수 : 총 3 항

(54) 은닉마르코프모델을 이용한 에스아이피 프로토콜 서비스 거부 공격 탐지 및 차단 시스템 및 방법

(57) 요약

본 발명은 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템에 관한 것으로, 유무선 통신망을 통해 연결된 하나 이상의 클라이언트 및 프락시 서버를 포함하는 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템에 있어서, 장치 전반을 제어하는 중앙제어부(110), 입력되는 SIP 통신 패킷을 파싱하되, SIP 파싱 과정에서 공격으로 판정되면, 공격자에 대한 IP와 Mac 정보를 세션/블랙리스트 테이블 중 블랙리스트에 등록하는 SIP 파싱모듈(112), 세션/블랙리스트 테이블(129)과 연계하여 세션 및 블랙리스트를 체크하는 블랙리스트 체크모듈(114), 상기 SIP 파싱모듈(112)을 통해 파싱된 데이터를 HMM의 입력 시퀀스로 변환하기 위한 데이터 가공과정을 수행하는 전처리모듈(122), Baum-Welch 알고리즘(128)을 이용하여 SIP 프로토콜을 모델링하는 학습모듈로서의 SIP 노멀 모델링부(124), 은닉마르코프 기반 SIP 정상 모델과 전처리 과정에서 생성된 시퀀스를 입력하여 각 정상 행위에서 현재 행위가 생성되었을 확률을 forward-backward procedure 알고리즘(126) 이용하여 구하고, 상기 SIP 노멀 모델링부(124)를 통해 각 모델별로 구해진 확률을 전달받아 비정상 행위인지 판정하고, 정상행위 모델링으로부터 구해진 임계값(threshold)과 비교하여 더 낮은 수치를 가질 경우 침입으로 판정하는 공격탐지 및 판정모듈(116), 사용자의 IP나 MAC 정보, 이메일 정보등을 저장 및 관리하는 사용자 정보저장부(121), 및 세션/블랙리스트를 저장 및 관리하는 세션/블랙리스트 테이블(129),을 포함하여 이루어진 것을 특징으로 한다.

대표도 - 도5



(72) 발명자

김득용

경기도 수원시 권선구 평동 14-5

윤하나

경기도 오산시 양산동 286-2 한신오피스텔 C동 20
5호

특허청구의 범위

청구항 1

유무선통신망을 통해 연결된 하나 이상의 클라이언트 및 프락시서버를 포함하는 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템에 있어서,

장치 전반을 제어하는 중앙제어부(110),

입력되는 SIP 통신패킷을 파싱하되, SIP 파싱 과정에서 공격으로 판정되면, 공격자에 대한 IP와 Mac 정보를 세션/블랙리스트 테이블 중 블랙리스트에 등록하는 SIP 파싱모듈(112),

세션/블랙리스트 테이블(129)과 연계하여 세션 및 블랙리스트를 체크하는 블랙리스트 체크모듈(114),

상기 SIP 파싱모듈(112)를 통해 파싱된 데이터를 HMM의 입력 시퀀스로 변환하기 위한 데이터 가공과정을 수행하는 전처리모듈(122),

Baum-Welch 알고리즘(128)을 이용하여 SIP 프로토콜을 모델링하는 학습모듈로서의 SIP 노멀 모델링부(124),

은닉마르코프 기반 SIP 정상 모델과 전처리 과정에서 생성된 시퀀스를 입력하여 각 정상 행위에서 현재 행위가 생성되었을 확률을 forward-backward procedure 알고리즘(126) 이용하여 구하고, 상기 SIP 노멀 모델링부(124)를 통해 각 모델별로 구해진 확률을 전달받아 비정상 행위인지 판정하고, 정상행위 모델링으로부터 구해진 임계값(threshold)과 비교하여 더 낮은 수치를 가질 경우 침입으로 판정하는 공격탐지 및 판정모듈(116),

사용자의 IP나 MAC 정보, 이메일 정보등을 저장 및 관리하는 사용자 정보저장부(121), 및

세션/블랙리스트를 저장 및 관리하는 세션/블랙리스트 테이블(129),을 포함하여 이루어진 것을 특징으로 하는 은닉마르코프모델을 이용한 에스아이피 프로토콜 서비스 거부 공격 탐지/차단 시스템.

청구항 2

제 1 항에 있어서, 상기 공격탐지 및 판정모듈은 정상행위 모델링으로부터 구해진 임계값(threshold)과 비교하여 더 낮은 수치를 가질 경우 침입으로 판정하여 차단하는 것을 특징으로 하는 은닉마르코프모델을 이용한 에스아이피 프로토콜 서비스 거부 공격 탐지/차단 시스템.

청구항 3

유무선통신망을 통해 연결된 하나 이상의 클라이언트 및 프락시서버를 포함하는 제 1 항을 통한 은닉마르코프 모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 방법에 있어서,

클라이언트(사용자)가 접속을 시도할 경우 SIP 파싱모듈이 SIP 메시지를 파싱하는 제1 단계,

세션/블랙리스트를 이용하여 패킷 인증을 시도하는 제2 단계,

인증된 SIP 패킷이 세션정보에 등록되어 있지 않다면, 현재 SIP 패킷에 대하여 세션을 등록하는 제3단계,

전처리 모듈에서는 SIP 패킷을 HMM의 입력 시퀀스 형태로 변환하는 제4단계, 및

SIP 공격 탐지 및 판정 모듈에서 변환된 SIP 패킷에 대한 차단여부를 결정하여 SIP 공격 메시지로 판단될 경우 패킷의 정보를 블랙리스트에 등록하고 차단하는 제5단계,

를 포함하여 이루어진 것을 특징으로 하는 은닉마르코프모델을 이용한 에스아이피 프로토콜 서비스 거부 공격 탐지/차단 방법.

명세서

발명의 상세한 설명

기술 분야

본 발명은 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템 및 방법에 관한 것으로, 더욱 상세하게는 IP망 기반 SIP 서비스에서 SIP Flooding 공격, SIP Malformed 공격에 대한 효과적인

[0001]

서비스 거부 공격 탐지 및 차단 메커니즘을 가진 은닉마르크프로토콜을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템 및 방법에 관한 것이다.

배경 기술

- [0002] 도 1은 일반적인 에스아이피 프로토콜을 이용한 브이오아이피 서비스망을 개략적으로 나타낸 도면이고, 도 2는 일반적인 에스아이피 메시지 포맷을 나타낸 도면이고, 도 3은 일반적인 에스아이피 플러딩 공격을 나타낸 도면이고, 도 4는 일반적인 간단한 은닉마르크프로토콜(HMM)의 예를 나타낸 도면이다.
- [0003] 도 1을 참조하면, 복수의 클라이언트(사용자)(1-1N, 1-2N), 로케이션 서버(LOCATION SERVER)(20), 프락시 서버(PROXY SERVER)(10)가 인터넷망을 통해 연결되어 있다.
- [0004] Session Initiation Protocol(SIP)는 상용 인터넷 전화를 위해 IETF에서 표준으로 채택된 시그널링 프로토콜로서, 기존 공중전화망(PSTN) 전화 서비스를 IP 기반의 Voice over IP(VoIP) 서비스를 제공하기 위해 제시된 시그널링 프로토콜이다. VoIP 서비스는 인터넷 콜센터, 다자간 화상전화 서비스, 사용자 위치정보 제공 서비스 등의 다양한 어플리케이션 응용이 가능하므로 경제성을 지닌 비즈니스 모델로 가능성이 크다고 할 수 있으며, 기존의 IP망을 그대로 이용하기 때문에 네트워크 자원의 가용성과 효율성을 극대화할 수 있으며, 통신비용 역시 저렴하다. 또한 물리적 위치에 구애받지 않고 인터넷망에 접속할 수 있다면 언제 어디서나 음성 전화 서비스를 이용할 수 있다는 편리함을 갖추고 있다.
- [0005] 그러나 SIP 프로토콜은 기존의 IP망을 그대로 이용하기 때문에 개방형 인터넷망에서 발생할 수 있는 보안 취약성뿐만 아니라 공중전화망과 유무선 인터넷망의 연동에 따른 새로운 취약성에 노출된다는 한계를 가지고 있다. 또한 SIP 상에서만 발생할 수 있는 취약점이 존재하며, 이들은 서비스의 지연 또는 마비를 시켜 서비스 사용자에게 정상적인 서비스를 제공하지 못하는 경우가 발생한다.
- [0006] SIP 서비스 제공시 가장 치명적인 공격은 서비스 거부공격(Denial of Service, DoS)이다. 서비스 거부공격은 VoIP 단말기의 오작동을 유발하거나 아예 단말기 자체를 무력화시켜 네트워크 접속 및 서비스 등이 제 기능을 발휘하지 못하게 하는 것이다.
- [0007] **SIP 프로토콜 서비스 거부 공격 기법**
- [0008] 서비스 거부 공격은 멀티태스킹을 지원하는 운영체제에서 발생할 수 있는 공격 방법으로서, 공격자가 시스템 또는 네트워크 자원을 공격 대상으로 하여 대역폭, 프로세스 처리 능력 및 시스템 자원을 독점하거나, 시스템의 가용성을 소진시켜 대상 시스템이 다른 사용자들에게 올바른 서비스를 제공하지 못하게 하는 것을 말한다. 도 3은 서비스 거부 공격중 하나인 Flooding 공격이다.
- [0009] **Spoofing 공격**
- [0010] 호스트나 라우터로 하여금 공격자의 패킷이 인증된 네트워크로부터 온 것인 것처럼 IP를 Spoofing을 통해, 라우터나 방화벽에서 정상 패킷이 인증된 네트워크로부터 전송된 것으로 의심 없이 통과하도록 만든 다음 본인이 원하는 공격을 한다.
- [0011] **Flooding 공격**
- [0012] Flooding 공격은 victim IP 단말의 개방된 포트로 시스템 자원을 고갈시키기 위하여 무의미한 대량의 더미 패킷을 victim IP로 보내는 공격이다. 이런 Flooding 공격은 한꺼번에 유입되는 대규모의 유해 트래픽을 견디지 못하고 다운된다. 대표적인 Message Flooding 공격은 다음과 같다.
- [0013] - Register Flooding 공격: 공격자의 반복적인 Register를 통해 다른 사용자가 서버를 사용하지 못하도록 과부하는 것은 공격 형태이다.
- [0014] - Invite, RTP Flooding : 공격 대상은 SIP 서버(Register, Redirect, Proxy) Software Switch, 사용자 단말 및 PC(소프트 폰)이며 공격자는 많은 수의 유효한 요청 메시지(SIP INVITE) 또는 음성 메시지를 보내어 시스템이 이에 대하여 응답 메시지를 준비하게 함으로써 해당 시스템의 자원을 고갈 시킨다.

[0015] **Malformed 메시지 공격**

[0016] 비정상 메시지 공격은 SIP의 헤더와 바디 내용이 일반 문자로 되어있다는 점을 이용하여 다른 문자들로 삽입, 변조 혹은 삭제하는 것인데, 엄청난 수의 공백 문자를 넣어 오버플로우 예외를 발생시킨다거나 특수문자(한자어나 non-ASCII)를 넣어 이에 대응하지 못하게 VoIP 서비스의 오동작을 유발한다.

[0017] 위와 같은 서비스 거부 공격은 공격자가 보내는 비정상적인 공격성 패킷과 고객이 전송하는 정상적인 서비스 요청 패킷을 정확한 구분이 어렵기 때문에 공격 패킷을 탐지하기 어렵다. 또한 공격 패킷을 탐지하더라도 즉각적인 트래픽 차단할 수 없다면 과도한 트래픽으로 인해 네트워크 혹은 시스템에 과부하가 걸려 정상적인 서비스를 제공하지 못한다. 이처럼 초기에 호를 설정하는 과정과 호를 끊는 과정을 반복함으로써 시스템 자원을 고갈시키거나 소프트스위치에 비정상적인 요구를 과도하게 함으로써 정상적인 서비스에 방해를 유발시키는 공격방법이 다양하게 존재한다. 따라서 이에 대한 대처 방안이 제시되어야한다.

[0018] 결국 이러한 취약성들로부터 안정적인 서비스를 위해서는 현재의 서비스를 방해하지 않으면서도 특정 위험 요소들을 탐지할 수 있는 보안 메커니즘이 제시되어야 하며, 특히 SIP 헤더 정보를 변경하여 전송하는 DoS 공격인 경우에 능동적으로 이를 탐지하고 차단할 수 있는 방법이 제시되어야 한다.

[0019] **SIP 프로토콜**

[0020] SIP 프로토콜은 ITU-T의 H.323에 대응되는 보단 간편한 프로토콜로서, 인터넷상에서 통신 하고자 하는 지능형 단말(전화, 인터넷 콘퍼런스, 인스턴트 메신저 등)들이 서로를 식별하여 그 위치를 찾고, 그들 상호 간에 멀티미디어 통신 세션을 생성하거나 삭제 또는 변경하기 위한 절차를 명시한 응용 계층의 시그널링 프로토콜이다. 인터넷 기반 회의, 전화, 인스턴트 메시징 등 멀티미디어 서비스 세션의 생성, 수정, 종료를 제어하는 Request/Response의 클라이언트/서버 구조로서 TCP와 UDP프로토콜 모두 사용할 수 있으며, 각 사용자들을 구분하기 위하여 E-mail 주소와 비슷한 SIP URL을 사용함으로써 IP 주소에 종속되지 않고 서비스를 제공받을 수 있는 프로토콜이다. 또한 SIP 프로토콜은 HTTP와 SMTP의 많은 부분을 그대로 사용하여 개발된 텍스트 기반으로 구현이 용이하며, 인터넷상에서 사용되는 다른 많은 프로토콜과 결합하여 다양한 서비스들을 제공할 수 있는 유연성과 확장성이 존재한다. 요청 메소드(Method)는 INVITE, ACK, CANCEL, BYE, REGISTER, OPTION, UPDATE, SUBSCRIBE이 있으며 응답 메소드는 HTTP와 유사하게 응답 코드를 갖는 메시지를 전송한다. SIP 메시지 형식은 HTTP와 동일하게 헤더와 바디로 구성되고 헤더와 바디는 CR/LF로 구별된다. 표 1은 SIP 표준에서 제공하는 메소드와 기능을 나타내며, 도 2는 SIP 메시지 포맷을 나타낸다.

표 1

(표 1) SIP 요청 및 응답 메시지

Request Method	의 미	Response Method	의 미	상 태
INVITE	콜 요청	1xx	Informational	Provisional
ACK	INVITE에 대한 최종 응답	2xx	Success	Final
BYE	콜 종료	3xx	Redirection	Final
CANCEL	미결정 콜 해지	4xx	Client Error	Final
OPTION	Capability 정보 요청	5xx	Server Error	Final
REGISTER	위치정보 등록 및 삭제 수정	6xx	Global Failure	Final

[0021]

[0022]

SIP 프로토콜 취약점

[0023]

SIP 프로토콜은 기존의 IP망을 그대로 이용하기 때문에 개방형 인터넷망에서 발생할 수 있는 보안 취약성뿐만 아니라, SIP 세션설정을 위한 시그널링으로 인해, SIP 상에서만 발생할 수 있는 취약점이 존재한다. 최근까지 알려진 SIP 관련 보안 취약성은 표 2와 같이 요약할 수 있다.

표 2

최근까지 알려진 SIP 프로토콜 취약점	
스니핑(Sniffing)	음성 트래픽을 불법으로 스니핑 하여 미디어로 재생, 정보를 수집하려는 시도
스푸핑(Spoofing)	TCP/IP 프로토콜의 약점을 악용하여 발신주소를 조작, 정상적인 사용자로 위장
재사용 공격 (Replay Protection)	전자서명과 같은 암호화된 데이터를 주고받을 때 권한 없는 공격자가 이를 복사해 두었다가 나중에 그대로 사용하여 합법적 이용자로 가장하려는 시도
중간자 공격	불법적인 제 3자가 양단간 통신에 개입할 수 있는 권한을 획득하여 경당한 통신주체로 참여하려는 시도
Session Hijacking	공격자가 세션에 직접 개입하여 불법 정보를 발생시킬 수 있는 능동적 공격 시도
VoIP 스텝 및 음성메일 폭탄공격	불특정 다수에게 보내지는 음성광고 메시지로 인해 음성사서함이 무용화 되는 시도나 공격
악의적인 호 발생 공격	양단간 전화통화에 개입하여 악의적인 패킷을 통화 중에 삽입하여 통신을 방해하는 행위
비인가 장치	인증 받지 않은 불법 VoIP 단말이나 시스템이 망에 접속하여 정상적인 시스템으로 위장
서비스 거부공격 (DOS 공격)	IP Server 같은 주요 시스템에 대한 자원을 고갈시키거나 독점 및 파괴하여 해당시스템이 서비스를 제공하지 못하도록 무력화하는 공격

[0024]

[0025]

은닉마르코프모델

[0026]

은닉마르코프(Hidden Markov Model, HMM)모델은 관찰이 불가능한 미지(Hidden)의 확률적 전이과정을 관찰이 가

능한 기호(Symbol)로 발생시키는 다른 확률적 전이과정을 통하여 모델링하는 이중의 확률론적 과정이며, 실제적인 관측을 통해서 변화되는 통계적인 특성을 확률적으로 모델링하기 위해서 마르코프 과정(Markov Process)을 이용한다. HMM에서 확률적으로 어떤 분포를 갖는 각각의 상태는 직접적으로 파악되지 않지만, 그 상태(state)에 의해 영향 받는 관찰 심벌(Observation symbol)을 파악할 수 있다. HMM은 상태라고 불리는 N개의 노드와 상태간의 전이를 표현하는 가지(edge)로 구성된 그래프로 볼 수 있다. 각 상태들은 은닉 상태(Hidden State)라 하며, 상태간의 전이 확률을 전이 확률이라 한다. 각 상태노드에는 초기 상태 분포와 해당 상태에서 M개의 관찰 가능한 심벌(Observable state) 중 특정 심벌을 관찰할 확률분포가 저장되어 있으며, 특정 심벌을 관찰할 확률을 관찰 확률이라 한다.

[0027] HMM은 각각의 관측 시점 t에서 새로운 상태는 그 이전 상태에 의존하여 전이 된다는 마르코프 가정과, 생성 확률 분포는 시간에 구애 없이 상태에 의존하는 출력 독립 가정을 이용하여 시간 t이후 모든 상태에 대하여 그 의존성이 일반화된다. HMM 모델은 기호로 $\lambda = (\Pi, A, B)$ 의 간결한 표시로 표현되며, 은닉 상태 수 N, 관찰 심벌의 개수 M이라 할 때, 다음 표 3과 같은 구성요소를 가진다.

표 3

- T : 관측열의 길이 또는 관측열의 개수 ($O_1, O_2, O_3, \dots, O_t$)
- N : 모델의 상태 수를 나타내며, 상태는 관찰되지 않는 감추어진(Hidden) 상태이며 모델에 따라 한 상태에서 다른 어떤 상태로의 전이가 가능하거나 또는 어떠한 제약에 의해 불가능 할 수 있다.
- M : 관찰 심벌의 수를 나타내며, 각 상태에서 관측되는 심벌로서 모델링된 시스템에서 출력하는 값
- $Q = \{q_1, q_2, q_3, \dots, q_n\}$: 은닉상태 집합
- $V = \{v_1, v_2, v_3, \dots, v_m\}$: 각 상태마다 관측 가능한 심벌의 집합
- $O = \{o_1, o_2, o_3, \dots, o_{t-1}, o_t\}$: 관찰 심벌로 이루어진 관측열
- $A = \{a_{ij}\}, a_{ij} = \Pr(q_j \text{ at } t | q_i \text{ at } t-1), 1 \leq i, j \leq N$: A는 상태 전이 확률 분포이며, a_{ij} 는 상태 i에서 상태 j로 전이할 확률을 나타낸다.
- $B = \{b_j(k)\}, b_j(k) = \Pr(v_k \text{ at } t | q_j \text{ at } t), 1 \leq k \leq M$: b_{jk} 가 상태 j에서 v_k 를 생성하는 확률을 나타내며, B는 관측 심벌 확률 분포
- $\Pi = \{\pi_i\}, \pi_i = \Pr(q_i \text{ at } t=1)$: 모든 상태의 초기 확률 분포

[0028]

[0029] 도 4에서 HMM을 이용하여 모델링하면 다음과 같다. 각각의 항아리에 해당하는 상태 i를 정의하고, 그 항아리에서의 관측 가능한 색공의 출력 확률을 $b_j(0)$ 로서 표현한다. 그리고 관측 심벌 b_{jk} 는 특정 항아리에서 선택된 색공의 색깔을 나타내며, 항아리의 선택은 초기 상태 분포와 상태 전이 확률의 분포로서 모델링된다. 도 4는 상태 수가 3인 간단한 HMM 모델을 보여주고 있다.

[0030] 기존 SIP 공격 탐지 시스템

[0031] 가. 침입탐지(Intruduction Detection System : IDS) 기술

[0032] IDS는 단순한 접근 제어 기능을 넘어서 침입의 패턴 데이터베이스와 Expert System을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. IDS는 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행 중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다. 침입탐지 기법은 크게 비정상적인 침입탐지 기법과 오용침입탐지 기법으로 나눌 수 있다. 즉, 침입탐지 시스템이라는 것은 허가를 받지 않은 침입자가 비정상적인 방법으로 접근을 시도하거나 네

트위크를 마비시키려는 시도, 혹은 시스템 전체를 장악하려는 프로세스 등을 감시하고 찾아내는 시스템이다. 따라서 이미 네트워크에 침입했거나 침입하려는 시도를 검출하고 그 침입자를 차단하는 기능을 한다.

[0033] 나. 기존 SIP 공격 탐지 시스템 문제점

[0034] 기존의 침입탐지 시스템은 기존에 알려진 공격패턴을 기반으로 탐지 규칙을 정의하고 그 규칙을 바탕으로 공격을 탐지한다. 그러나 대다수의 침입탐지 시스템은 SIP에 특화된 룰을 제공하지 않고 있어서 공격에 대한 탐지가 어렵다. 또한 기존 침입탐지 시스템 대부분이 패킷 기반 탐지 정책이어서 세션 단위로 탐지가 이루어져야하는 SIP 프로토콜에 바로 적용하기에는 무리가 있다. 서비스 거부 공격 중 SIP 패킷 Flooding 공격 유형들은 비정상적인 트래픽으로 인하여 일부 기존 침입탐지 시스템에서 대응이 가능하지만 SIP Malformed 공격 같은 단일 패킷의 SIP 보안 취약점 공격에 대해서는 탐지를 하지 못하거나 탐지율이 매우 낮으며, SIP 정규식을 이용하여 일부 SIP Malformed 공격을 탐지하는 방법만이 제시된 상태이다.

발명의 내용

해결 하고자하는 과제

[0035] 본 발명의 목적은 IP망 기반 SIP 서비스에서 SIP Flooding 공격, SIP Malformed 공격에 대한 효과적인 서비스 거부 공격 탐지 및 차단 메커니즘을 가진 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템 및 방법에 제공함에 있다.

과제 해결수단

[0036] 상기한 바와 같은 목적을 달성하기 위한 본 발명의 바람직한 실시예에 따르면, 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템 은

[0037] 유무선통신망을 통해 연결된 하나 이상의 클라이언트 및 프락시서버를 포함하는 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템에 있어서,

[0038] 장치 전반을 제어하는 중앙제어부,

[0039] 입력되는 SIP 통신패킷을 파싱하되, SIP 파싱 과정에서 공격으로 판정되면, 공격자에 대한 IP와 Mac 정보를 세션/블랙리스트 테이블 중 블랙리스트에 등록하는 SIP 파싱모듈,

[0040] 세션/블랙리스트 테이블과 연계하여 세션 및 블랙리스트를 체크하는 블랙리스트 체크모듈,

[0041] 상기 SIP 파싱모듈을 통해 파싱된 데이터를 HMM의 입력 시퀀스로 변환하기 위한 데이터 가공과정을 수행하는 전처리모듈,

[0042] Baum-Welch 알고리즘을 이용하여 SIP 프로토콜을 모델링하는 학습모듈로서의 SIP 노멀 모델링부,

[0043] 은닉마르코프 기반 SIP 정상 모델과 전처리 과정에서 생성된 시퀀스를 입력하여 각 정상 행위에서 현재 행위가 생성되었을 확률을 forward-backward procedure 알고리즘을 이용하여 구하고, 상기 SIP 노멀 모델링부를 통해 각 모델별로 구해진 확률을 전달받아 비정상 행위인지 판정하고, 정상행위 모델링으로부터 구해진 임계값(threshold)과 비교하여 더 낮은 수치를 가질 경우 침입으로 판정하는 공격탐지 및 판정모듈,

[0044] 사용자의 IP나 MAC 정보, 이메일 정보등을 저장 및 관리하는 사용자 정보저장부, 및

[0045] 세션/블랙리스트를 저장 및 관리하는 세션/블랙리스트 테이블을 포함하여 이루어진 것을 특징으로 하는 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템이 제공된다.

[0046] 본 발명의 다른 측면에 따르면,

[0047] 유무선통신망을 통해 연결된 하나 이상의 클라이언트 및 프락시서버를 포함하는 제 1항을 통한 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 방법에 있어서,

[0048] 클라이언트(사용자)가 접속을 시도할 경우 SIP 파싱모듈이 SIP 메시지를 파싱하는 제1 단계,

- [0049] 세션/블랙리스트를 이용하여 패킷 인증을 시도하는 제2 단계,
- [0050] 인증된 SIP 패킷이 세션정보에 등록되어 있지 않다면, 현재 SIP 패킷에 대하여 세션을 등록하는 제3단계,
- [0051] 전처리 모듈에서는 SIP 패킷을 HMM의 입력 시퀀스 형태로 변환하는 제4단계, 및
- [0052] SIP 공격 탐지 및 판정 모듈에서 변환된 SIP 패킷에 대한 차단여부를 결정하여 SIP 공격 메시지로 판단될 경우 패킷의 정보를 블랙리스트에 등록하고 차단하는 제5단계,
- [0053] 를 포함하여 이루어진 것을 특징으로 하는 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 방법이 제공된다.

- [0054] SIP 프로토콜의 서비스 거부 공격에 대한 보안 위협 및 취약점을 보안하기 위하여, SIP 프로토콜의 보안 요구사항 및 방향에 대해서 분석하고, SIP 프로토콜의 정상행위를 은닉마르코프모델을 기반으로 모델링하여 외부 또는 내부 네트워크에서 전송되는 SIP 서비스 거부 공격을 탐지하고, 이를 즉각적으로 탐지 및 차단한다. SIP 메시지를 구성하는 각각의 헤더를 하나의 단일 시퀀스로 보고, SIP 프로토콜의 통계적인 순서정보를 이용하여 정상행위를 모델링한다. 정상행위 모델링에는 순서정보를 통계적으로 모델링하고 평가하는데 적합한 HMM(Hidden Markov Model)을 사용하고, 세션 단위로 탐지가 이루어져야하는 SIP 메시지에 대해 세션/블랙리스트 기반 인증을 수행한다. HMM 입력 시퀀스로 파싱/변환하는 전처리 과정을 수행하여, 이를 바탕으로 SIP 서비스 거부 공격을 탐지/차단하는 방법을 제안한다.

효 과

- [0055] 상기 설명한 바와 같이, 본 발명에 따른 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템 및 방법에 의하면, SIP 프로토콜의 정상행위를 은닉마르코프모델을 기반으로 모델링하여 유무선 네트워크에서 발생하는 SIP 서비스 거부 공격을 실시간으로 탐지하고, 이를 즉각적으로 차단하는 효과가 있다.
- [0056] 또한, 본 발명에 따른 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템 및 방법에 의하면, SIP 프로토콜을 이용하는 서비스에 본 연구 결과를 적용할 수 있을 것으로 예상되며, 능동적이고 효율적인 SIP 프로토콜 탐지/대응 기술을 제시할 수 있을 것으로 기대된다.

발명의 실시를 위한 구체적인 내용

- [0057] 이하 본 발명에 따른 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템 및 방법을 첨부도면을 참조로 상세히 설명한다.
- [0058] 도 5는 본 발명에 따른 은닉마르코프모델(HMM)기반 에스아이피 공격 탐지 및 차단 시스템의 동작흐름을 나타낸 도면이고, 도 6은 도 5의 일부 확대도로서, 세션/블랙리스트 테이블 및 처리과정을 나타낸 도면이고, 도 7은 본 발명에서 에스아이피 요청라인(request-line)에 대한 에스아이피(SIP) 파서(Parser) 수행과정을 나타낸 도면이고, 도 8은 도 5의 일부 확대도로서, 에스아이피 정상 메시지 모델링 및 공격 탐지 과정을 나타낸 도면이고, 도 9는 본 발명에 따른 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템의 구체적인 블록도이다.
- [0059] 본 발명에서는 다음과 같은 발명을 수행하고자 한다. 우선 세션단위 탐지가 이루어져야 하는 SIP 프로토콜에 대해 세션을 분리하고, 등록하는 세션 리스트를 구성하고, SIP 공격자로 식별된 사용자를 데이터베이스화하여 송신자 주소에 대하여 필터링하는 모듈(도시안됨-시스템(100)내에 구성될 수 있음)을 제시하며, 정규식을 이용하여 RFC 3261에 존재하는 ABNF (Augument Backus-Naur Form)의 SIP Base Rule을 가지고 SIP 메시지를 파싱하는 모듈(112)과, HMM 모델의 입력 시퀀스로 변환하기 위한 전처리 모듈(122)을 제시한다. 이를 이용하여 HMM 모델을 이용하여 SIP 메시지를 모델링하여 SIP 프로토콜의 서비스 공격에 대해 탐지/대응하는 방법을 제공하고자 한다.
- [0060] 이하 본 발명에 관한 설명에 있어서, 이 분야에서 잘 알려진 용어를 그대로 사용하며 그에 대한 개념정의 등 자세한 설명은 생략하기로 한다.

[0061] **HMM 기반 SIP 공격 탐지/차단 시스템(100) 구조**

[0062] HMM 기반 SIP 공격 탐지 및 차단은 SIP 메시지를 파싱하는 SIP Parser 모듈(112), 사용자를 세션 단위로 구분하고, 블랙리스트를 관리하는 세션/블랙리스트 테이블(129)을 이용한 블랙리스트 체크모듈(114), SIP 메시지를 HMM의 입력 시퀀스로 변환하기 위한 전처리 모듈(122), HMM 모델을 이용하여 SIP 정상 메시지를 모델링하는 학습 모듈과 SIP 공격을 탐지하는 공격 탐지 및 판정 모듈(116)로 구성된다. 도 5는 HMM 기반 SIP 공격 탐지 및 차단 시스템의 전체 구성도이다.

[0063] 사용자가 SIP 프로토콜을 이용하여 통신을 시도하는 경우 본 발명에서 제안하는 시스템은 아래와 같은 단계를 수행한다.

[0064] - 1단계 : 사용자가 접속을 시도할 경우 SIP Parser(SIP 파싱모듈(112))는 SIP 메시지를 파싱한다.

[0065] - 2단계 : 세션/블랙리스트를 이용하여 패킷 인증을 시도한다.

[0066] - 3단계 : 인증된 SIP 패킷이 세션정보에 등록되어 있지 않다면, 현재 SIP 패킷에 대하여 세션을 등록한다.

[0067] - 4단계 : 전처리 모듈(122)에서는 SIP 패킷을 HMM의 입력 시퀀스 형태로 변환한다.

[0068] - 5단계 : 4단계를 거친 패킷은 SIP 공격 탐지 및 판정 모듈(116)에서 SIP 패킷에 대한 차단여부를 결정한다.

[0069] - 6단계 : 5단계에서 SIP 공격 메시지로 판단될 경우 패킷의 정보를 블랙리스트에 등록하고 차단한다.

[0070] **세션/블랙리스트 테이블(129)**

[0071] 세션/블랙리스트 테이블(129)은 SIP 공격자로 식별된 사용자를 데이터베이스화 하여 송신자 주소에 대하여 필터링하고, 사용자별 세션을 분리한다. 블랙리스트에 포함되는 주소는 SIP 사용자를 식별하는 모든 형태로 설정할 수 있지만, 이메일 주소나 도메인 전체 주소는 쉽게 변경이 가능하다. 따라서 본 발명에서는 사용자를 식별하는 주소의 효율성을 높이기 위하여 IP와 Mac 정보를 블랙리스트의 식별자로 사용하였다. 또한 세션 리스트의 식별자로는 IP와 이메일 주소를 식별자로 사용하였다.

[0072] 세션/블랙리스트에서는 SIP 파싱모듈(112)에서 파싱된 데이터를 이용하여 세션/블랙리스트 테이블의 정보와 비교하여 합법적인 클라이언트에 대한 필터링 기능을 수행하여, 차단 유무를 결정한다. 합법적인 클라이언트인 경우 세션 리스트와 비교하여 새로운 클라이언트일 경우 새로운 세션을 등록한다.

[0073] **SIP 패킷 파싱 모듈(112)**

[0074] SIP 패킷이 들어오면 SIP Parser는 정규식을 이용하여 RFC 3261에 존재하는 ABNF (Augument Backus-Naur Form)의 SIP Base Rule을 가지고 SIP 메시지를 파싱한다. SIP Parser 수행 시 SIP 메시지를 파싱하지 못하면, ABNF의 형식에 맞지 않는 것이므로 파싱되지 않은 SIP 메시지를 SIP Malformed 공격으로 1 차 판정한다. 도 7은 SIP Request-Line에 대한 SIP 파서를 수행한 결과이다.

[0075] SIP Parser 과정에서 공격으로 판정되면, 공격자에 대한 IP와 Mac 정보를 세션/블랙리스트 테이블 중 블랙리스트에 등록한다.

[0076] **SIP 메시지 전처리 단계**

[0077] 전처리 과정에서는 SIP Parser를 거쳐 파싱된 데이터를 HMM의 입력 시퀀스로 변환하기 위한 데이터 가공 과정을 수행한다. SIP 헤더는 다수의 헤더 필드가 존재하는데, 각 헤더를 구성하는 헤더 필드마다 하나의 관찰 심벌로 구성한다. 그 중 헤더 필드의 값이 통계적 특성을 가지지 않는 필드 값이 존재하며, 이러한 userinfo, hostport, IP, branch-tag 등의 필드 값의 경우 모든 데이터를 수집 하고 학습하기가 불가능하다. 따라서 이러한 통계적인 특성을 가지지 못한 헤더 필드 값의 자료부족 문제를 해결하기 위하여 숫자(digit), 알파벳(alpa), 워드(word), 도메인(domain)등의 심벌 값으로 변환하여 할당하였다. 또한 SIP 프로토콜에서 SP 필드는 다수의

공백이나 하나의 공백을 모두 동일한 필드 값으로 취급하지만, 본 논문에서는 SIP 필드에서 허용되는 모든 공백은 공백의 수를 고려하여 필드의 값을 상수로 나타내어 관찰 심벌을 생성하였다. 표 4는 전처리 과정에서 SIP 메시지를 모델링하기 위하여 데이터 가공을 수행함으로써 심벌을 생성한 결과이다.

표 4

파싱된 SIP 메시지 데이터 가공 과정

SIP 메시지 헤더	SIP 헤더 필드	SIP 파싱 결과	생성된 관찰 심벌
request-line	Method	INVITE	INVITE
	SP	space-bar	1
	userinfo	sip:userB	sip:alba
	hostport	aaa.ac.kr	domain
	uri-parameters	transport=udp	transport=udp
	uri-header		
	SIP-Version	SIP/2.0	SIP/2.0
Via header	Via	Via	Via
	HCOLON	:	0:
	sent-protocol	SIP/2.0/UDP	SIP/2.0/UDP
	:	:	:
From header	:	:	:

위의 과정을 거쳐 생성된 관찰 심벌을 SIP Flooding 공격, SIP Malformed 공격에 대한 서비스 거부 공격 탐지를 위한 HMM의 입력 시퀀스로 생성하였다. 플로딩 공격은 대량의 메시지를 보내는 것이므로 일정량의 SIP Request Method를 가지고 입력 시퀀스를 생성하였다. 또한 비정상 메시지는 경우 단일 SIP 메시지에 대해 전체적으로 고려하여야 함으로 SIP 메시지를 각 헤더별로 나누어 입력 시퀀스를 생성하여, SIP 메시지 전체를 모델링할 수 있도록 하였으며, HMM모델에서 각 헤더를 모델링하게 되는 상태수는 파싱된 SIP 메시지를 구성하는 각 헤더의 필드 개수를 상태수로 정의하였다.

HMM을 이용한 SIP 메시지 정상행위 모델링

정상 메시지 모델링은 전처리 단계에서 생성된 정상메시지 시퀀스를 기반으로 HMM의 매개변수를 결정하는 과정이다. HMM의 매개변수 결정은 주어진 관찰열 o 가 해당 모델 λ 로부터 나왔을 확률인 $\Pr(O|\lambda)$ 값이 최대가 되도록 $\lambda = (I, A, B)$ 를 조정한다. 본 논문에서는 관찰열 $O = \{o_1, o_2, o_3, \dots, o_{t-1}, o_t\}$ 이 모델 $\lambda = (I, A, B)$ 에서 관측되었을 확률을 최대화하는 모델 λ 의 매개변수 π, a_{ij}, b_j 각각의 확률 값을 구하기 위하여 Baum-Welch의 재추정식(128)을 사용하였다.

HMM 기반 SIP 공격 탐지

SIP 공격 탐지 관점에서는 이미 구축되어 있는 은닉마르코프 기반 SIP 정상 모델과 전처리 과정에서 생성된 시퀀스를 입력하여 각 정상 행위에서 현재 행위가 생성되었을 확률을 구한다. 각 모델별로 구해진 확률은 공격 탐지 및 판정 모듈(116)에 전달되어 비정상 행위인지 판정한다. 이때 정상행위 모델링으로부터 구해진 임계값(threshold)과 비교하여 더 낮은 수치를 가질 경우 침입으로 간주한다. 현재 행위가 생성되었을 확률을 구하는 과정은 forward-backward procedure 알고리즘(126) 이용하였다.

SIP 메시지만 경우 HMM 기반 forward-backward procedure 알고리즘(126)에서 사용하는 변수는 다음과 같이 정의할 수 있다. T는 SIP 입력 시퀀스의 개수를 의미하며, N은 SIP 메시지에 대한 파싱 상태 수이고, M은 SIP 메시지에 대한 파싱 후 생성된 고유 토큰의 개수를 나타낸다. 따라서 $Q = \{q_1, q_2, q_3, \dots, q_n\}$ 는 SIP 메시지에 대한 파싱 후

은닉상태 집합이고, $V = \{v_1, v_2, v_3, \dots, v_m\}$ 는 SIP 메시지에 대한 파싱 후 생성된 고유 토큰의 관측 가능한 심벌 집합, $O = \{o_1, o_2, o_3, \dots, o_{t-1}, o_t\}$ 는 파싱된 SIP 메시지 입력 시퀀스로 이루어진 관측열을 의미한다.

- [0085] 도 9를 참조하면, 본 발명에 따른 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템은
- [0086] 장치 전반을 제어하는 중앙제어부(110),
- [0087] 입력되는 SIP 통신패킷을 파싱하는 SIP 파싱모듈(112)
- [0088] 세션/블랙리스트 테이블(129)과 연계하여 세션 및 블랙리스트를 체크하는 블랙리스트 체크모듈(114),
- [0089] 상기 SIP 파싱모듈(112)를 통해 파싱된 데이터를 HMM의 입력 시퀀스로 변환하기 위한 데이터 가공과정을 수행하는 전처리모듈(122),
- [0090] Baum-Welch 알고리즘(128)을 이용하여 SIP 프로토콜을 모델링하는 학습모듈로서의 SIP 노멀 모델링부(124),
- [0091] 은닉마르코프 기반 SIP 정상 모델과 전처리 과정에서 생성된 시퀀스를 입력하여 각 정상 행위에서 현재 행위가 생성되었을 확률을 forward-backward procedure 알고리즘(126) 이용하여 구하고, 상기 SIP 노멀 모델링부(124)를 통해 각 모델별로 구해진 확률을 전달받아 비정상 행위인지 판정하되, 이때 정상행위 모델링으로부터 구해진 임계값(threshold)과 비교하여 더 낮은 수치를 가질 경우 침입으로 간주하는 공격탐지 및 판정모듈(116),
- [0092] 사용자의 IP나 MAC 정보, 이메일 정보등을 저장 및 관리하는 사용자 정보저장부(121), 및
- [0093] 세션/블랙리스트를 저장 및 관리하는 세션/블랙리스트 테이블(129),을 포함하여 이루어진다.
- [0094] 상기 SIP 파싱 모듈(112)은 SIP Parser 과정에서 공격으로 판정되면, 공격자에 대한 IP와 Mac 정보를 세션/블랙리스트 테이블 중 블랙리스트에 등록한다.

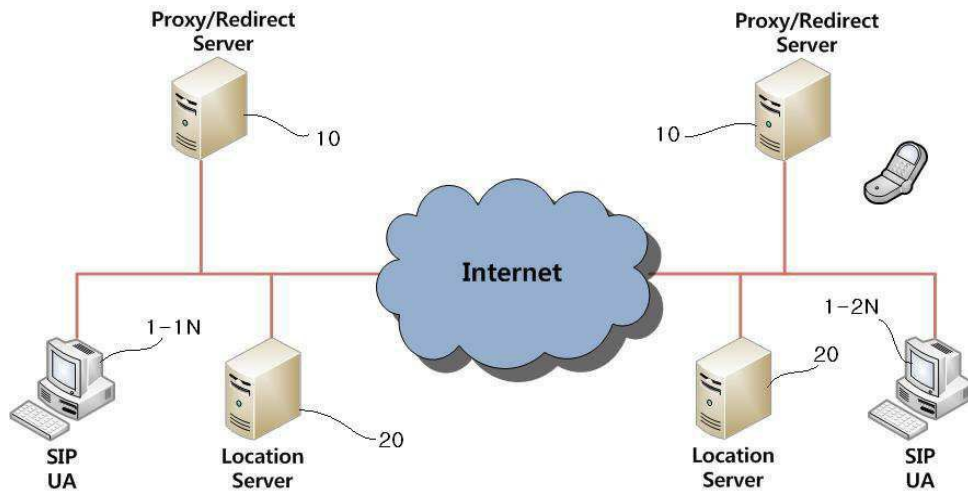
도면의 간단한 설명

- [0095] 도 1은 일반적인 에스아이피 프로토콜을 이용한 브이오아이피 서비스망을 개략적으로 나타낸 도면이다.
- [0096] 도 2는 일반적인 에스아이피 메시지 포맷을 나타낸 도면이다.
- [0097] 도 3은 일반적인 에스아이피 플러딩 공격을 나타낸 도면이다.
- [0098] 도 4는 일반적인 간단한 은닉마르코프모델(HMM)의 예를 나타낸 도면이다.
- [0099] 도 5는 본 발명에 따른 은닉마르코프모델(HMM)기반 에스아이피 공격 탐지 및 차단 시스템의 동작흐름을 나타낸 도면이다.
- [0100] 도 6은 도 5의 일부 확대도로서, 세션/블랙리스트 테이블 및 처리과정을 나타낸 도면이다.
- [0101] 도 7은 본 발명에서 에스아이피 요청라인(request-line)에 대한 에스아이피 파서 수행과정을 나타낸 도면이다.
- [0102] 도 8은 도 5의 일부 확대도로서, 에스아이피 정상 메시지 모델링 및 공격 탐지 과정을 나타낸 도면이다.
- [0103] 도 9는 본 발명에 따른 은닉마르코프모델을 이용한 SIP 프로토콜 서비스 거부 공격 탐지/차단 시스템의 구체적인 블록도이다.
- [0104] * 도면의 주요부분에 대한 부호의 설명 *
- [0105] 1-1N, 1-2N: 클라이언트(사용자)
- [0106] 10: 프락시서버
- [0107] 110: 중앙제어부
- [0108] 112: SIP 파싱모듈
- [0109] 114: 블랙리스트 체크모듈
- [0110] 122: 전처리모듈

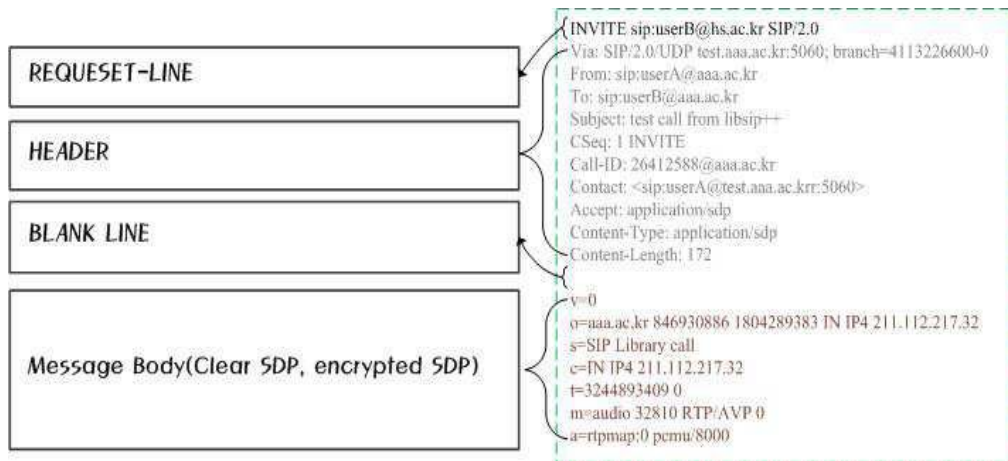
- [0111] 124: SIP 노멀 모델링부
- [0112] 116: 공격탐지 및 판정모듈
- [0113] 121: 사용자 정보저장부
- [0114] 129: 세션/블랙리스트 테이블

도면

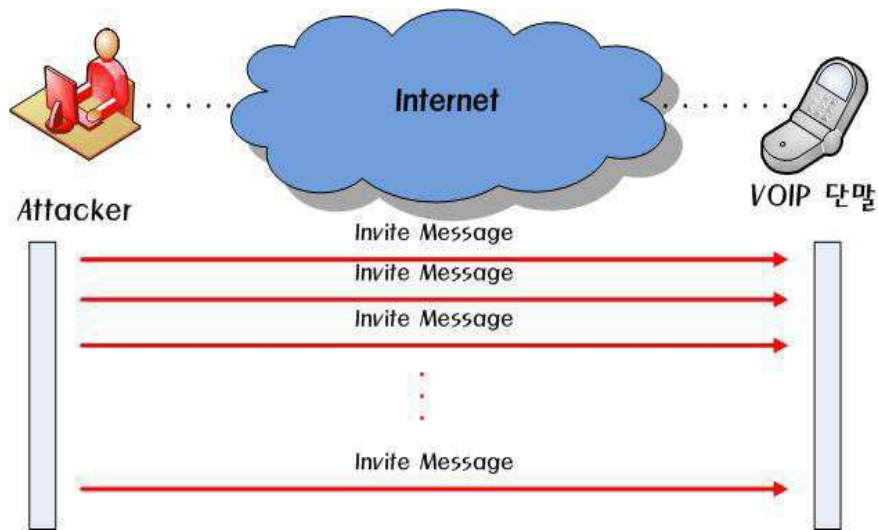
도면1



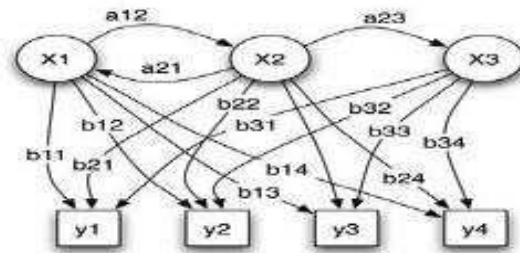
도면2



도면3

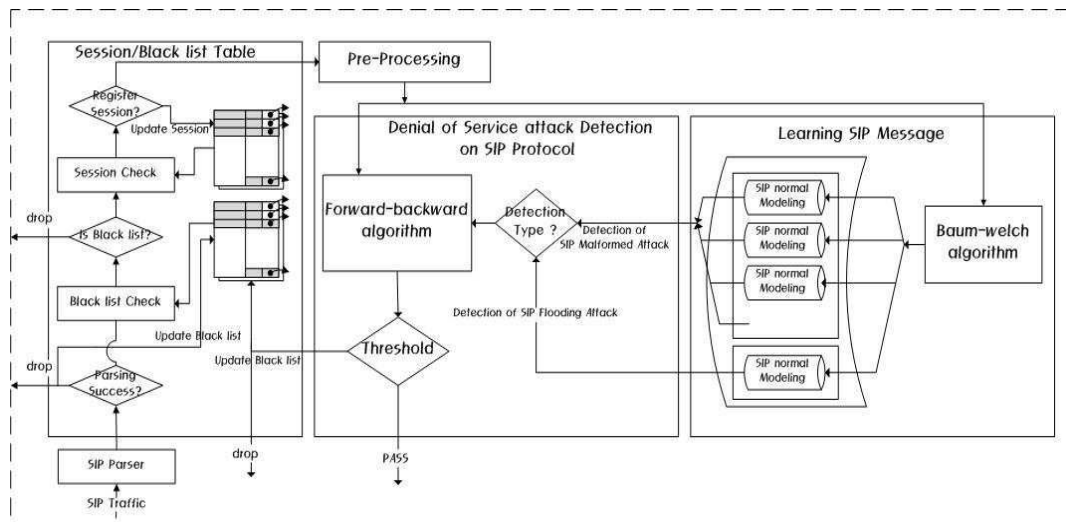


도면4

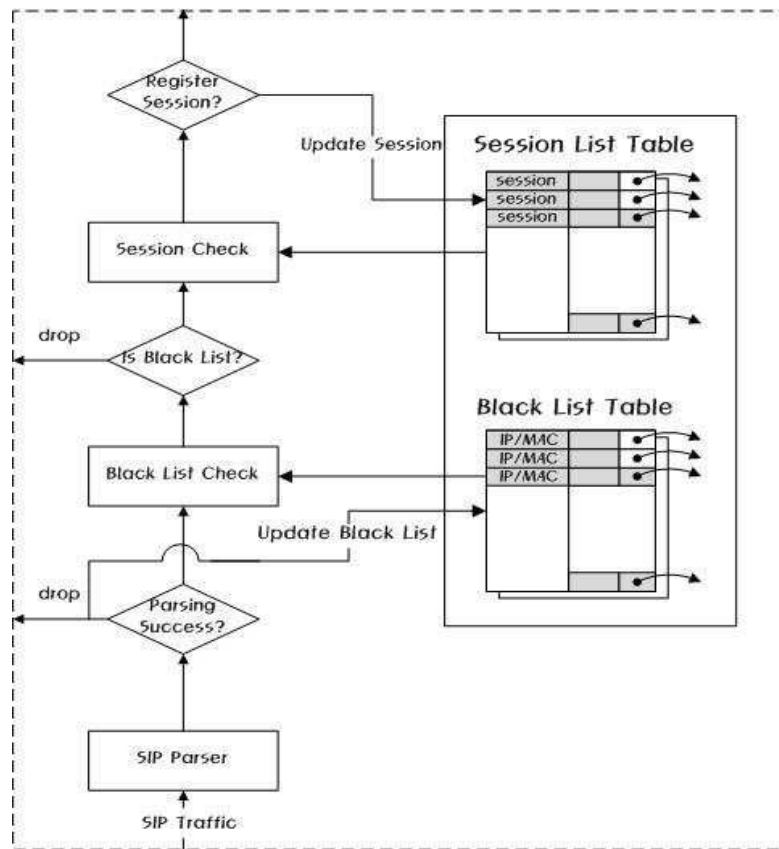


간단한 HMM 모델의 예

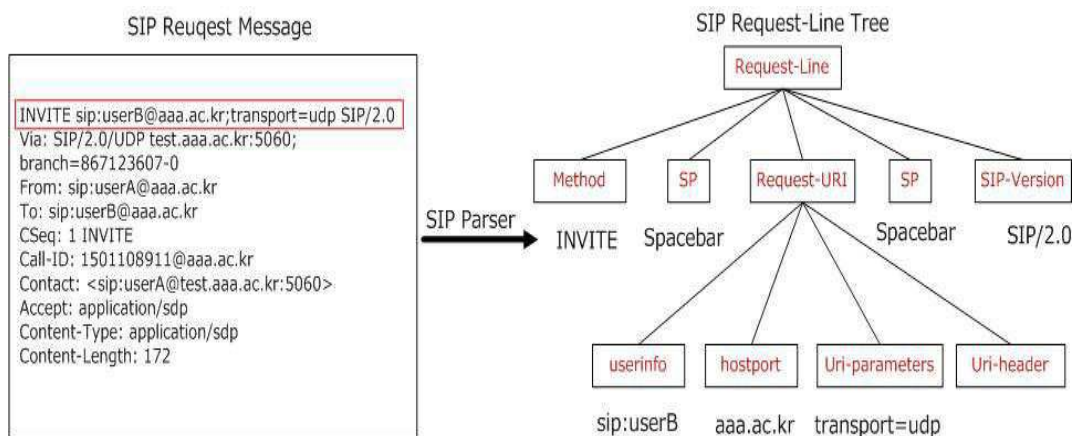
도면5



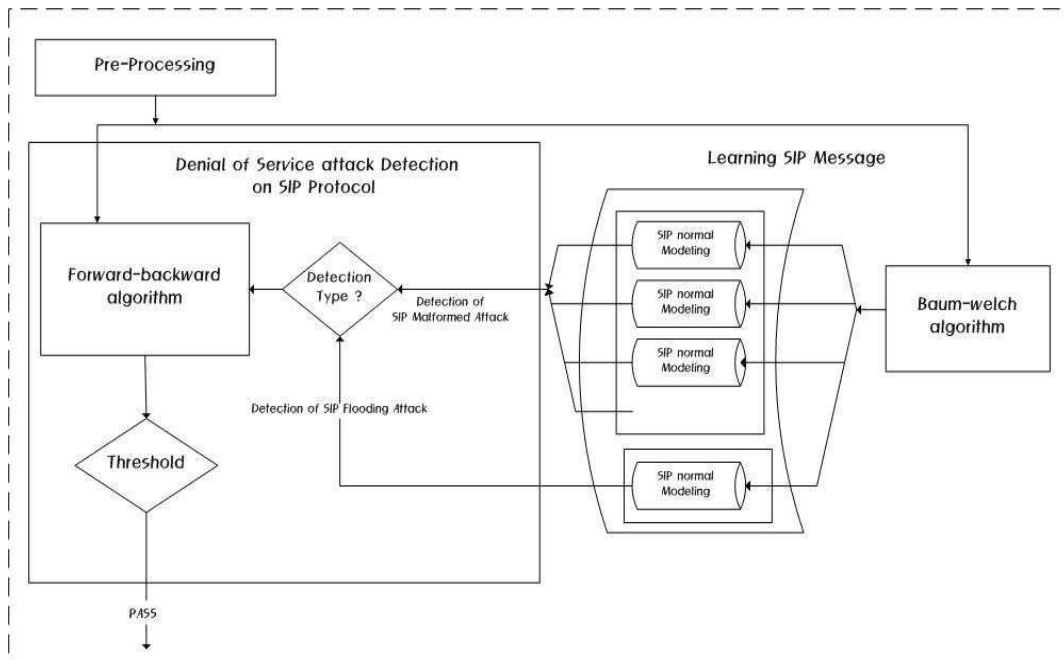
도면6



도면7



도면8



도면9

