논문 15-40-10-17 The Journal of Korean Institute of Communications and Information Sciences '15-10 Vol.40 No.10
http://dx.doi.org/10.7840/kics.2015.40.10.1994

VoIP 네트워크 내의 Fraud와 SIM Box Fraud 검출 방법에 대한 연구

이 정 원•, 엄 종 훈*, 박 태 흠*, 김 승 호°

Study on Fraud and SIM Box Fraud Detection Method in VoIP Networks

Jung-won Lee•, Jong-hoon Eom*, Ta-hum Park*, Sung-ho Kim°

요 약

다양한 기술들이 하나로 융합된 VoIP(Voice over Internet Protocol) 서비스는 IP 망을 통해 음성뿐만 아니라 멀티미디어 서비스와 각종 부가서비스를 제공한다. 현재 대역폭 사용효율과 저비용성 등의 장점들 때문에 기존 PSTN 전화에서 VoIP 시스템으로 비즈니스가 전환되고 있다. 이러한 것이 가능한 이유는 기존의 회선교환 네트워크를 대신하여 디지털화된 정보가 IP 패킷 형태로 여러 계층의 컴퓨터로 구성된 패킷교환망을 통해 전달되기 때문이다. 반면에 이러한 형태의 시스템들이 기존 IP네트워크 환경에서의 취약점과 융합되어 발생되는 신규 취약점 등에 의해서 각종 Fraud가 발생하고 있다. 2012년 상반기 Fraud call의 46%가 VoIP 전화기에서 만들어지고 있다는 조사 결과도 있듯이 Fraud Call의 피해는 상당하다. 따라서 Fraud에 대한 손실예방을 위해 대책마련이 필요하다. 특히, Fraud Call의 피해는 주로 국제 통화를 이용할 때 과금 피해로 나타나고 있어, 이와 관련된 SIM Box에 의한 Toll Bypass Fraud에 대한 분석과 이를 검출할 수 있는 방안마련이 요구된다. 일반적으로는 DPI(Deep Packet Inspection)를 기반으로 주요 Signature 또는 통계정보를 이용한 다양한 검출 방안이 제안되었으나, Fraudster 역시 이를 회피하기 위해 다양한 방법을 사용하고 있다. 특히, VoIP에서 Call Setup과 Termination과정을 수행하는 SIP Signal을 암호화 하거나 여러 경로로 전송하는 방식을 사용함으로써 감지를 회피하고 있다. 본 논문은 Fraud call의 감지 회피를 효과적으로 방지할 수 있도록 VoIP 트래픽의 특성과 VoIP Fraud 중 SIM Box Fraud의 행위분석을 결합한 방법론을 제안한다. 또한 제안된 방법론을 적용하여 Toll Bypass Fraud와 관련된 VoIP 서비스 제공자의 장비를 검출하는 방법을 제시한다.

Key Words : Toll Bypass Fraud, SIM Box, Traffic Analysis, VoIP, VoIP Fraud Detection

ABSTRACT

Voice over IP (VoIP) is a technology for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks. Instead of being transmitted over a circuit-switched network, however, the digital information is packetized, and transmission occurs in the form of IP packets over a packet-switched network which consist of several layers of computers. VoIP Service that used the various techniques has many advantages such as a voice Service, multimedia and additional service with cheap cost and so on. But the various frauds arises using VoIP because VoIP has the existing vulnerabilities at the Internet and based on complex

※ 본 연구는 미래창조과학부 및 연구개발특구진흥재단에서 시행한 2014년 특구기술사업화사업으로 수행되었습니다.
• First Author : Creble Inc, jungwon.lee@creble.com, 정회원,
° Corresponding Author : Kyungpook National University School of Computer Science and Engineering, shkim@knu.ac.kr, 정회원
* Creble Inc, eom@creble.com, th.park@creble.com
논문번호 : KICS2015-07-208, Received July 2, 2015; Revised September 9, 2015; Accepted October 14, 2015

technologies, which in turn, involve different components, protocols, and interfaces. According to research results, during in 2012, 46 % of fraud calls being made in VoIP. The revenue loss is considerable by fraud call. Among we will analyze for Toll Bypass Fraud by the SIM Box that occurs mainly on the international call, and propose the measures that can detect. Typically, proposed solutions to detect Toll Bypass fraud used DPI(Deep Packet Inspection) based on a variety of detection methods that using the Signature or statistical information, but Fraudster has used a number of countermeasures to avoid it as well. Particularly a Fraudster used countermeasure that encrypt VoIP Call Setup/Termination of SIP Signal or voice and both. This paper proposes the solution that is identifying equipment of Toll Bypass fraud using those countermeasures. Through feature of Voice traffic analysis, to detect involved equipment, and those behavior analysis to identifying SIM Box or Service Sever of VoIP Service Providers.

Ⅰ. 서 론

VoIP는 다양한 부가서비스와 저렴한 통신비용 등의 장점으로 인해 나날이 발전하고 있으며, 사용자도 전 세계적으로 증가하고 있다. 그러나 기존의 IP 네트워크 환경에서 발생되는 보안의 위협뿐만 아니라 서비스를 제공하기 위한 여러 가지 기술이 융합됨으로 인해 드러난 신규 취약점을 활용한 다양한 VoIP Fraud가 발생하고 있다.

CFCA(Communications Fraud Control Association)의 2013년도 Worldwide Telecom Fraud Survey 보고서[1]에 따르면, VoIP Fraud로 인해 2013년 한 해에 발생된 Global Fraud Loss의 추정치는 약 $46.3 Billions (USD) [한화 약 47조원]이며, 피해금액이 매년 증가 추세를 보이고 있다. 그 중 Toll Bypass Fraud는 약 $2.0 Billons(USD)[한화 약 2조]로 추정되고 있으며, 이 역시 지속적으로 증가 추세에 있다. 그러나 정작 큰 문제점은 각 국가의 VoIP 서비스 사업자가 실제로 해당 Fraud에 당하고 있는 것을 모르거나 그 피해액을 정확히 파악하지 못하고 있는데 있다[2]. 한국정보통신진흥협회(KAIT)의 통계 결과에 의하면 국내의 국제 전화 시장은 약 7231억 원에 달한다고 한다[3]. 여기서 약 1%만 VoIP Fraud가 점유한다고 가정할 경우 연간 약 100억 원의 손실이 발생한다고 추론할 수 있다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 주요한 VoIP Fraud 유형별로 상세히 설명하고, Ⅲ장에서는 그중 SIM Box에 의한 Toll Bypass Fraud가 발생하는 경우에 대해 패킷 분석 및 시나리오를 설명하고, 그 특징을 이용하여 이를 검출하는 방법론을 제시한다. 그리고 마지막으로 Ⅳ장에서는 제안된 모델을 구현 및 검증하고 Ⅴ장의 결론으로 마무리 짓는다.

Ⅱ. VoIP Fraud 정의 및 분류

2.1 Fraud 정의

일반적으로 Fraud란 개인적인 이익 또는 다른 사람에게 해를 끼치기 위해 행해지는 모든 행위를 일컫는다. 그림 1과 같이 개인적인 이익의 획득을 위해 행해지는 Fraud 중에는 금융사기(Financial Fraud)와 통신사기(Communications Fraud)가 큰 부분을 차지하고 있으며, 점차 개인화/지능화/조직화 되어 가고 있다.

첫 번째로 Financial Fraud란 금융 조직이 가지고 있거나 유지하고 있는 돈, 자산, 또는 다른 사람의 재산 등을 획득하기 위해 잠재적으로 불법적인 방법을 사용하거나, 또는 은행 또는 금융 기관으로 사칭하여 예금자의 돈을 획득하는 것을 말한다. 가장 대표적인 예로 보이스 피싱(Voice Phishing)을 들 수 있다.

두 번째로 Communications Fraud는 광의와 협의 두 가지로 나누어 정의할 수 있다. 광의의 사기전화란 전화통화의 비용을 지불하는 것을 회피하기 위해 관련 시스템을 사용하는 모든 행위를 말한다. 협의의 사기전화는 타인의 전화번호를 도용하거나 요금체계를 회피하여 전화를 거는 행위를 말할 수 있다. 형태는 행위자를 중심으로 가입자가 전화회사를 사취, 전화회사가 가입자를 사취, 또는 제 3자가 가입자나 전화회사를 사취하는 세 가지로 나누어진다. 유선전화 기반의 사기전화는 개인적으로 요금을 내지 않고 전화를 거는

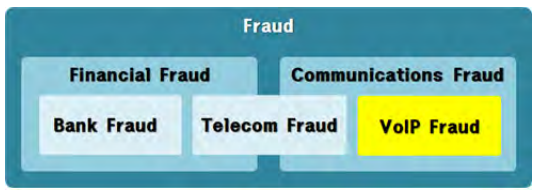

그림 1. Fraud의 구분
Fig. 1. Classification of Fraud

표 1. VoIP Fraud 분류
Table 1. Type of VoIP Fraud

Fraud	Fraudster	Victim	Description
Arbitrage	VoIP Service Provider	Network Service Provider	비용이 싼 회선을 통해 국제전화를 라우팅하는 행위
Toll Bypass Fraud	VoIP Service Provider / SIM Box operator	Mobile operator / Government	VoIP Gateway/SIM Box를 이용하여 국제전화를 국내전화로 위장하는 행위
Location Routing Number (LRN) Fraud	Hacker	Operator	통신 사업자들이 LRN dip 요금 절약을 위해 이를 회피하는 속성을 사용한 장거리 전화 요금을 회피하는 행위
Roaming Fraud	Malicious user	Operator	사용자가 자국이 아닌 타국의 무선통신 사업자의 전화를 통신 요금을 지불할 의사가 없이 사용하는 행위
Shell Companies	Malicious user	Operator	일반적인 사기 수법으로 허위의 회사 명의로 전화 서비스를 받는 행위
Buffer Overflow	Hacker	VoIP Service Provider	Fraud를 위해 VoIP 장비의 취약점을 해킹하는 행위
Call Transfer Fraud	Hacker	User / Operator	IP-PBX 해킹을 통한 제어 권환 획득과 Blind Transfer(REFER) 기능을 이용한 불법 통화 행위
Domestic &International Revenue Share Fraud	Hacker / Operator	User / Operator	사업자간 상호접속 협약을 악용할 목적으로, 트래픽 양을 부풀리거나 Premium Rate Service 로 착신하게 하여 요금을 비싸게 부과하여 자신에게 정산요금이 거의 부과되지 않게 하거나 낮추는 행위
False Answer Supervision	Operator /Carrier	Operator / Originating call user	장거리/해외 통신 사업자가 착신을 요구하는 호에 대해 비정상적 과금을 하는 행위
PBX Hacking	Hacker	User / Operator	IP-PBX 해킹을 통해 불법적으로 전화 서비스를 사용하는 행위
Phreaking	Hacker	User and Operator	장거리 전화를 무료로 사용하거나 도청을 위해서 전화기에 인가되지 않는 액세스나 제어 하는 행위
Subscription Fraud	Malicious user	Operator	타인의 명의를 도용하여 전화 서비스를 받는 행위
Toll Fraud	Malicious user / Malicious Service Provider	User	장거리 전화를 사용할 목적으로 기업의 VoIP 네트워크에 침투하여 전화선이나, 장비, 또는 서비스를 불법으로 사용하고 과금은 사용자에게 전가시키는 행위
Unallocated Number Fraud	Malicious operator	User	악의적인 중계업자가 Premium Rate Service의 회선으로 호를 중계하여 비정상적인 과금을 하는 행위

사기수법이 주류로 손해의 크기가 상대적으로 작다.

그러나 이동통신 전화 기반의 사기전화는 상대적으로 비싼 요금을 회피하는 형태이며, 예를 들어 국제전화 요금을 회피하는 사기전화나 사용자에게 통화시간보다 더 많은 과금을 하는 형태의 사기과금이 주를 이루고 있다. 게다가, 현재 VoIP 기술의 보편화로 해킹을 통한 사기전화 기술이 늘어나고 있으며 정당한 가입자와 서비스 사업자들에게 악의적인 손해를 끼치는 형태로 발전하고 있는데 이를 VoIP Fraud라고 한다. 특히 근래에 들어서는 국제적인 테러 조직과의 연계 등으로 세계적인 테러 범죄의 범위로까지 확대되고 있다.

2.2 VoIP Fraud

VoIP Fraud란 요금 지불을 회피할 목적으로 VoIP 전화망을 사용하는 것을 총칭한다[4]. 요금 지불 회피에는 요금이 부정확하거나, 전화기록을 완전히 삭제하거나, 다른 사람에게 부과시키는 것이 모두 포함된다. 또한 VoIP 통신 프로토콜이나 시스템의 취약점을 이용한 불법적인 활동 또는 기술적으로는 합법이지만 전화회사에 손실을 끼치는 모든 활동을 VoIP Fraud로 간주할 수 있다. VoIP Fraud 중에서 통신사업자나 기업에 악영향을 미치는 대표적인 행위는 Toll Bypass Fraud, Toll Fraud, False Answer Supervision, Call Transfer Fraud, 그리고 PBX Hacking등이 있다. VoIP 기술의 보편화에 따라 기업 및 교회와 같은 사설 조직들의 독자적인 IP-PBX(Internet Protocol-Private Automatic Branch eXchange)의 운용이 점차 늘어가고 있으며, 이에 따

른 VoIP 해킹과 같은 보안 문제점[5,6]에 대한 대응 능력이 점차 필수적인 것으로 자리 잡아 가고 있다. 표 1은 다양한 VoIP Fraud의 분류를 정리하였다. 각 Fraud는 하나의 Fraud로 구성되기 보다는 두어 가지의 Fraud가 혼합되어 발생되는 경우가 대부분이다. 주요한 VoIP Fraud 에 대한 상세한 설명은 다음 장에서 기술한다.

2.3 VoIP Fraud 타입별 분석

2.3.1 Toll Bypass Fraud

Toll Bypass Fraud[7]는 장거리 사업자 망에 불법적으로 트래픽을 유입시키는 행위로 다른 용어로 SIM Box Fraud, Interconnect Fraud, GSM Gateway Fraud로 불린다. Fraudster는 최신 기술을 사용하여 국제전화를 값싼 국내전화로 보이게끔 하므로, 정상적인 국제전화 요금 시스템을 “bypassing” 시킨다. Fraudster는 주로 해외 장거리 Calling Card를 팔아서 수익을 얻는데, 고객이 카드의 번호로 전화를 걸면 SIM Box 운용자는 이 전화를 착신 측에서 국내호 같이 보이게끔 만든다. 여기서 사용된 SIM Box는 VoIP Gateway 장치로써 VoIP 인터넷 전화를 SIM Box에 삽입된 USIM(Universal Subscriber Identity Module)에 있는 수신자의 정보를 사용하여 해당 국가의 이동통신 사업자의 지역 통화로 변환시켜주는 기능 수행한다.

2.3.2 Toll Fraud

장거리 전화를 사용할 목적으로 기업의 VoIP 네트워크에 침투하여 전화선이나, 장비, 또는 서비스를 불법으로 사용하고 과금은 사용자에게 전가시키는 경우를 말한다. 장거리 전화를 사용하기 위해 주로 해킹된 PBX[8]를 사용한다. Toll Fraud는 Mobile Phones, Calling Cards, Pay Phones, Long-distance Fraud등 다양한 형태의 Fraud를 포함한다. VoIP 인프라 내 주요 해킹 대상은 설치 과정에서 기본 관리자 패스워드를 변경하지 않는 경우, 충분한 길이의 암호화된 패스워드를 사용하지 않는 경우, 내부 통신에서 암호화 기능을 사용하지 않는 경우가 된다. 국내에서 발생되는 대부분의 과금 폭탄과 관련 된 경우는 이와 같은 경우로 인해 발생된다. 또한, 분실된 USIM을 사용하거나 또는 사용자 정보를 도용해서 발급한 USIM을 SIM Box에 사용한 경우도 있다[9].

2.3.3 Roaming Fraud

Roaming Fraud는 통신 요금을 지불할 의사가 없이 사용자의 자국이 아닌 타국의 무선통신 사업자의 전화를 사용하는 것을 말한다. 주로 이런 형태의 Fraud는 거짓 신분을 사용하여 서비스를 가입하는 Subscription Fraud(대포폰)를 사용하는 누군가에 의해서 수행된다. 로밍 사업자간의 CDR(Call Detail Record)의 전달 지연 때문에 홈 네트워크에서 CDR이나 Fraud 통보를 수신하는데 수일 또는 수주가 걸릴 수도 있는 것을 악용하여 발생한다. Fraud 과정은 우선 불법으로 사업자 서비스 가입, 가입된 전화기를 가지고 해외 사업자 지역으로 로밍, 고액의 전화 요금 발생, Fraud 검출 시까지 사용한다.

2.3.4 Call Transfer Fraud

Call Transfer Fraud는 IP-PBX Hacking을 통한 제어 권한을 획득한 후에 착신전환(Blind transfer, REFER) 기능을 이용한 불법 통화를 말한다. 이는 Three way calling과 유사한 형태로써 IP-PBX Hacking이 전제되어야 한다. 그림 2는 Call Transfer Fraud의 시나리오를 기술하였다. 해킹 된 IP-PBX에 해커가 호 생성을 명령한다. 해킹된 IP-PBX는 목적지로 Call Setup 메시지를 전송하고 호가 연결 되면, 해커는 또 다시 IP-PBX에게 REFER을 사용하여 착신 전환을 한다. 이때 Fraud의 목적에 따라 해커 자신이나 자신의 서비스를 사용하는 사용자에게 전환 시킬 수 있다.

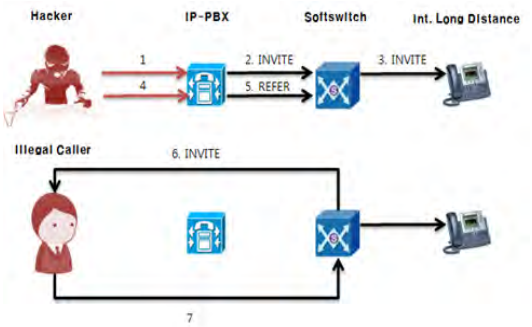

그림 2. Call Transfer Fraud
Fig. 2. Call Transfer Fraud

2.3.5 Domestic & International Revenue Share Fraud(IRSF)

IRSF는 사업자간 상호접속 협약을 악용하는 목적으로, 요금을 비싸게 부과하거나 트래픽 양을 부풀려서 자신에게 상호접속협약 정산요금이 거의 부과되지 않게 하거나 낮추는 것이다. 이러한 Fraud는 국내 사업자간 또는 국제간 사업자 사이에 발생 가능하다.

비록 기술적으로 합법적일 수도 있으나, 주로 불법적으로 PBX Hacking을 하거나 다른 형태의 Fraud를 사용하여 가공의 트래픽을 발생시킨다. 일반적으로 상호접속요금 정산에서 자신에게 유리하도록 착신호 트래픽을 부풀리는 형태인 Traffic Pumping 또는 Switch Access Stimulation을 사용한다. 그리고 CNAM(Caller ID Name)Revenue pumping 혹은 Dip pumping(CNAM dip fee를 악용한 과금 및 이익 갈취), Premium Rate Services를 제공한다는 빌미로 일반 전화보다 훨씬 비싼 요금을 부과하는 Fraud를 예를 들 수 있다.

2.3.6 Location Routing Number (LRN) Fraud

Location Routing Number (LRN) Fraud는 사업자들이 LRN dip 요금을 절약하기 위해 이를 회피하는 속성을 이용하여 요금을 낮추는 방법이다. 대부분의 사업자들은 착신번의 정확한 LRN을 결정하기 위해 LRN dip을 수행한다. 그러나 일부 사업자들이 SIP 메시지 안에 LRN이 이미 존재하면 LRN dip을 수행하지 않는다. Fraudster는 이를 이용해 SIP 메시지 안에 가짜의 LRN을 삽입한다. 예를 들면 비교적 요금이 비싼 지역으로 착신할 때 LRN에는 저렴한 지역의 LRN을 넣어, Fraudster에게 싼 요금으로 과금이 되게 만든다. 어떤 경우는 5배까지 요금 차이가 나게 된다.

2.3.7 Unallocated Number Fraud

Unallocated Number Fraud는 번호 영역에는 속해 있으나 합법적인 국가 번호 할당 기관에서 할당된 적이 없는 번호를 이용하는 Fraud를 말한다. 일반적으로 Unallocated Number는 라우팅이 되지 않는다. Unallocated Number Fraud는 호의 라우팅에서 투명성 부족으로 인해 발생된다. 장거리 사업자 내부에 존재하는 Fraud 사업자나 개인 또는 그룹이 존재하지 않는 번호에서 주로 다른 나라에 있는 실제 번호로 불법으로 호를 재라우팅 할 수 있다. 이런 호의 실제 최종 목적지는 주로 Premium Rate Service Number가 된다. 네트워크에서 발신하는 Unallocated Number Fraud는 모든 네트워크와 과금 시스템에서 존재하지 않는 번호로 기록되게 된다.

2.3.8 False Answer Supervision

False Answer는 장거리 사업자가 실제로는 착신되지 아니한 호에 대하여 고의적으로 연결 기간에 대한 요금을 부과할 때 발생한다. 잘못된 연결 기간은 호 설정시(Early Answer)나 종료시(Late Disconnect)에 수초간일 수도 있고, False Answer 메시지나 false ring tone 사용으로(False Answer) 통화시간이 완전히 거짓일 수도 있다. 통상 통신 사업자는 이러한 Fraud가 발생하는 것을 인식하지 못하고 있어, 장거리 사업자에게 요금 정산 후에 가입자로부터 클레임을 받을 수도 있다. 이로 인해 발신측 통신 사업자의 재정 손실 및 회사 평판이 나빠진다. 해당 Fraud 의 특징은 짧은 음성 통화, 발신측에서 거의 100% 호를 종료, 높은 착신 응답율을 들 수 있다.

Ⅲ. SIM Box에 의한 Toll Bypass Fraud 검출

SIM Box에 의한 Toll Bypass Fraud는 통신 사업자들의 주요한 수입 손실과 통화 품질 저하의 원인이 되고 있다. SIM Box는 일종의 VoIP Gateway로써 불법적인 장비가 아니라 일반적으로 사용되는 장비이다. 그러나 이를 불법적으로 사용함으로써 정상적인 국제 통화 요금에 비해 획기적으로 싼 요금으로 국제 통화를 제공할 수 있고, Calling Card를 일반 사용자에게 판매한 금액에서 차액이 Fraudster의 수입된다. 더욱이 관련 지식을 가지고 있는 경우 수개월 내에 SIM Box와 관련 장비를 사용하여 손쉽게 큰 수입을 얻을 수 있다[10]. 특히, 아직 통신회사를 국가에서 운영하는 캄보디아, 베트남, 미얀마 등에서는 세금 자체가 매년 손실되기 때문에 심각한 문제로 대두되고 있다[11]. 국내 역시 다양한 국가에서 들어온 인력들이 보다 싼 가격으로 자국의 친지들과 통화하기 위해 사용되고 있다. 이로 인해 해당국가의 통신사와 국내 통신사 역시 정확하게 파악은 못하고 있으나 피해액은 상당할 것으로 추측 된다. Toll Bypass Fraud를 검출하기 위해 다양한 방법이 시도되고 있으나, Fraudster 역시 다양한 방법을 사용하여 이를 회피하고 있다. 일반적으로 TCG(Test Call Generation) 와 FMS(Fraud Management System) 두 가지 방식으로 나눠진다. 우선 TCG은 각 국가에 테스트 스테이션을 두고 실제로 Calling Card 등을 구입하여 테스트 호를 생성한다. 이때 발신측의 정보와 수신측의 정보가 다른 경우 SIM Box Fraud 라고 판별하기 때문에 상당히 정확성이 높다. 그러나 서비스 형태의 방식으로 이루어지기 때문에 지속적인 비용이 든다.[12] 그리고 FMS는 DPI(Deep Packet Inspection)를 통해 트래픽을 분석하고, 추출된 SIP를 분석해서 Signature와 통계 정보, CDR정보 분석을 이용한 검출 방법이다. 초기 투자비

용이 들지만 유지비면에서 효율적이다. 그러나 지속적으로 검출 방법에 대한 연구와 업그레이드가 필요하다. Fraudster은 해당 검출 방식을 회피하기 위해 IX(Internet eXchange) 구간 즉 Bypass Operator의 IP-PBX와 SIM Box 의 구간을 암호화 하거나 우회 경로를 사용하여 Call Setup 또는 Termination Signal을 전송함으로써, DPI를 기반으로 한 Fraud 검출 장비를 무력화 하고 있다. 따라서 본 장은 암호화와 관계없이 VoIP 음성 트래픽이 가진 특성을 사용하여 음성 트래픽을 검출한다. 그리고 검출된 장비간의 행위 정보 분석을 수행하여 정상적인 VoIP 서비스를 제공하는 장비와 Toll Bypass Fraud를 생성하는 장비를 분류하여 해당 정보를 제공해 주는 방법에 대해 기술한다.

3.1 환경 분석

SIM Box에 의한 Toll Bypass Fraud는 그림 3과 같이 발생한다. 해당 방식은 SIM Box를 통해 해외에서 발신된 VoIP 통화를 지역 이동통신 통화로 전환하여 국제 요금이 아니라 지역 이동통신 통화 요금이 과금 되도록 하여 정상적인 국제 요금보다 낮은 금액으로 통화를 가능하도록 한다. 이로 인해 불법적인 트래픽이 유입되어 통화 품질 저하와 통화에 대한 과금 수입 손실이 발생되며, 이동통신 업체는 비정상적인 VoIP 통화로 인한 서비스 제공으로 통화품질 저하와 과금 손실이 발생된다. SIM Box에 의한 Toll Bypass Fraud를 수행하기 위해서는 크게 두 가지가 필요한데 첫 번째는 발신국에서 발신자들의 PSTN, 인터넷 전화, 이동통신 전화 등으로 Bypass Operator 에게 접속하는 IVR과 VoIP 서비스 인프라인 구성하는 IP-PBX 등의 장비가 필요하다. PBX는 일반 상용서버에 오픈소스인 Asterisk[13]를 일반적으로 사용한다. 그리고 수신국에는 VoIP 제어 신호/음성을 해당 지역의 이동통신 통화로 전환시키는 SIM Box가 필요하다. 일반적으로 SIM Box에는 한 개 또는 최대 수십 개의 USIM를 삽입할 수 있다. 따라서 동시에 많은 사용자들에게 불법 서비스를 제공할 수 있다. 정상적인 국제통화(또는 장거리 통화)와 SIM Box를 사용한 Toll Bypass Fraud의 On-Net SIM Box와 Off-Net SIM Box에 대한 자세한 시나리오는 그림3과 같다. 정상적인 과금이 발생하는 국제 통화인 경우에 Caller Alice는 PSTN, 이동통신, 인터넷 전화 등 다양한 방법을 통해 수신국 B국의 Callee Bob에게 발신한다. 그리고 발신국의 통화망 사업자, 중계자, 수신국 통화망 사업자를 통해 통화하게 되고, 각각 과금된 요금이 분배된다. 예시 상으로 과금 단위 시간당 총 0.8$ 과금된다.

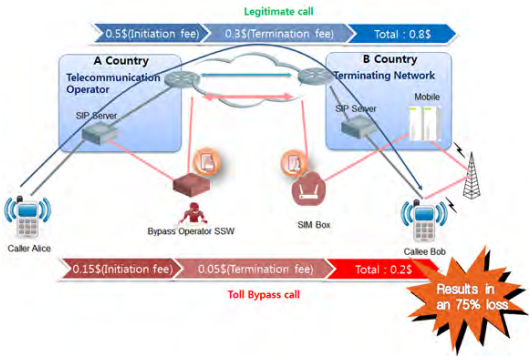

그림 3. SIM Box를 사용한 Toll Bypass Fraud 환경 및 시나리오
Fig. 3. Toll Bypass Fraud Using SIM Box

반면, SIM Box를 사용한 Toll Bypass Fraud중 하나인 On-Net SIM Box로 장거리 사업자 망에 불법적으로 트래픽을 유입시키는 과정은 그림 3의 하단에 적색으로 기술된 바와 같다. 수신국 B에 설치된 SIM Box는 해당 장비에 삽입된 USIM의 정보를 기반으로 발신국의 Bypass Operator의 IP-PBX로 등록한다. 발신국 A의 Caller Alice는 Bypass Operator가 판매한 Calling Card에 기입된 IVR 번호 또는 Soft phone으로 통화를 시도한다. 사용자는 Bypass Operator의 IVR(Interactive Voice Response)을 통해 카드 번호와 수신국 B의 User Bob의 정보를 입력하고 Bypass Operator는 수신국의 SIM Box를 통해 수신국의 로컬 이동통신 망을 통해 수신국의 Callee Bob과 국내 통화로 음성을 주고받는다. 예시 상으로 발신국의 이동통신 사업자는 과금 단위 시간당 약 75%인 0.6$를 금전적 손실을 보게 된다. 이와 유사한 경우로 Off-net SIM Box에 의한 Toll Bypass Fraud가 발생할 수 있다. 이는 특정 국가나 다른 통신업자 간의 협약을 통해 일반적인 통화 금액 보다 싸게 책정한 경우 최초 발신국의 발신자가 Bypass Operator를 통해 협약된 국가의 네트워크의 SIM Box를 통해 실제 수신국의 수신자에게 통화하는 방식이다. 해당 Fraud의 주요한 특징 중 하나로 SIM Box에 삽입 된 USIM은 서비스 제공을 위해서 Bypass Operator가 운용하는 IP-PBX로 등록을 수행해야 한다. 또한, 제어/음성 트래픽은 추가적인 조작이 없는 한 IP-PBX와 SIM Box와 직접적으로 주고받는다. 정상적인 서비스를 제공하는 통신업자 역시 최종적으로 국제 통화 시 사용되는 SSW (Soft Switch)와 제어 신호/음성 트래픽을 주고받게 된다. 실제 국제 관문국 구간의 트래픽을 분석하고,

SIM Box와 IP-PBX를 사용하여 테스트 베드를 구성한 후 수집한 트래픽들을 그림 4와 같이 분석하였다.

최초 사용자는 Soft phone을 통해 수신지 번호로 통화를 시도한다. Call Setup Signal은 Soft phone에 미리 설정된 Bypass Operator가 구축한 VoIP 서비스 인프라로 전달된다. 그리고 이를 IX구간을 지나 수신 국가에 설치된 SIM Box가 수신하고, 삽입되어 있는 USIM 정보를 바탕으로 이동통신 망의 Call Setup Signal로 변환되어 해당 지역 이동통신 망으로 전달된다. 그리고 최종적으로 호가 성립되고 음성을 주고받게 된다. 제어 신호의 경우 반드시 Bypass Operator의 IP-PBX를 경유하여 SIM Box로 전달되지만, 음성인 경우 상황에 따라 모두 경유하거나, 최소한 SIM Box는 반드시 경유하게 된다. 왜냐하면, VoIP 통화를 위한 제어 및 음성을 이동통신 망에 맞게 변환 시켜야하기 때문이다. 또한 정상적인 서비스를 제공하는 경우에도 위와 동일한 이유와 각국의 통신사업자 간의 상호 정산 협약을 통해 과금하게 되기 때문에 정확한 정산과 관리를 위해 특정 SSW를 통해 주고 받는다. 따라서 SIM Box에 의한 Toll Bypass Fraud를 검출하기 위해서는 IX구간에 해당하는 위치에 제안된 시스템을 위치 시켜야 한다. 그림 5는 본 논문에서 제안하는 시스템 구조이다.

해당 시스템은 크게 세 가지 단계로 구성된다. 우선 IX구간의 대용량 트래픽을 손실 없이 수집하기 위해 NPU(Network Process Unit)기반으로 패킷을 수집하고, 이를 기반으로 Flow를 생성한다. 그리고 각 Flow

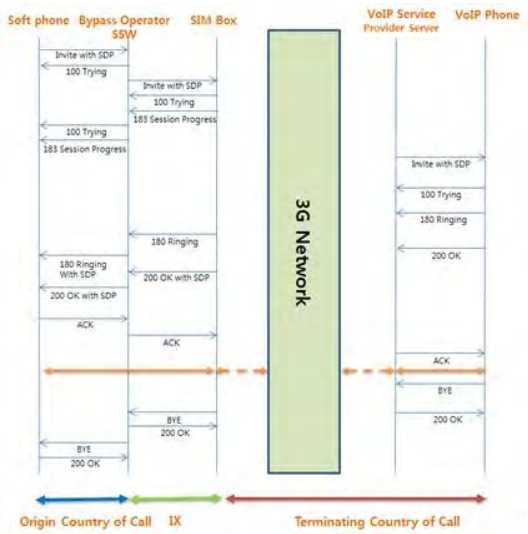

그림 4. SIM Box에 의한 Toll Bypass Fraud의 Call Flow
Fig 4. Call Flow of Toll Bypass Fraud Using SIM Box

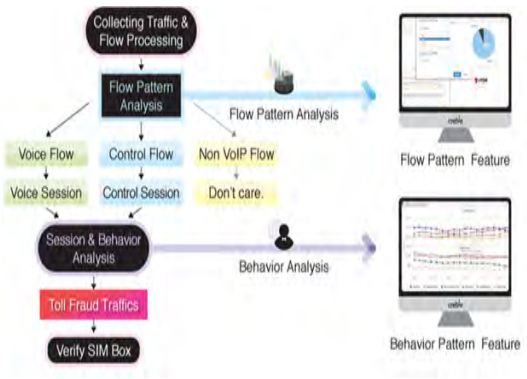

그림 5. 제안하는 SIM Box 기반 Toll Bypass Fraud 검출 방법
Fig. 5. Proposed Toll Bypass Fraud Detection Method

기반으로 트래픽 분석을 통해 Voice Flow를 검출한다. 해당 정보를 바탕으로 VoIP서비스를 제공하는 장비들의 IP Pair를 검출한다. 그리고 검출된 IP Pair간의 행위 정보를 분석하여 정상적인 서비스를 제공한 장비와 비정상적인 서비스를 제공하는 장비의 IP Pair Set 리스트를 검출한다[14].

3.2 검출 과정

3.2.1 Flow 생성

대용량의 트래픽을 처리하기 위해 기본적으로 Flow 기반으로 트래픽 분석을 수행한다. Flow의 정의는 동일한 5 튜플(source address, source port, destination address, destination port, transport protocol)을 가지고 이전의 패킷 과 새로운 패킷과의 시간차가 T 시간 이내인 패킷들의 집합이다. 수식 1과 같이 정의 된다. Flow 기반의 트래픽 분석을 위해 Flow의 Packet Count, Size, Inter-arrival-time 에 대한 평균, 표준편차, 최빈값 등을 생성 및 유지 한다.

$$
\begin{aligned}
&f = \{P_0, P_1, \ldots\ldots, P_{i-1}, P_i\},\\
&\text{if } |T_{p_{i+1}} - T_{p_i}| \le T_{th}\\
&where\ P_i\ is\ Sequence\ Arrived\ Packets.\\
&T_{p_i}\ is\ arrival\ time\ of\ Packet\ ith \in Flow(f).\\
&T_{th}\ is\ threshhold\ of\ time.
\end{aligned}
\tag{1}
$$

3.2.2 Flow 기반 VoIP Traffic Detection

본 장은 생성된 Flow 중 Voice Flow의 특성을 가진 Flow 후보군을 추출한다. 음성은 샘플링이 필수적이다. 나이키스트(Nyquist) 원리로 4Khz의 전화선상의 음성을 2배인 8천 번 샘플링 하는 것으로 64kbps

로 만든다. 코덱 마다 차이가 있으나 동일한 코덱 내에서는 일정한 주기와 크기로 음성 트래픽이 전송된다. 주요 파라미터는 Inter-arrival-time, Packet Size Average와 Packet Size Variant(Flow 내의 Packet size 별 개수)이다[15]. 실험 결과 및 표준 분석 결과에 의해 표 2와 같이 Voice Flow의 특성을 생성한다. 네트워크 상황 및 코덱의 설정 또는 환경에 따라 변동이 발생할 수 있다. 따라서 Inter-arrival-time와 Packet Size Average는 그 평균을 기준으로 특정 임계치 내로 만족하는 경우 Voice Flow로 판단한다.

표 2. Voice Traffic Flow 주요 특징 파라미터
Table 2. Feature Parameters of Voice Traffic Flow

CODEC	Size Avg	Inter-arrival -time Avg:	Packet Size Variant
G.711	214 byte	20msec	1(2)
G.723	74/78byte	30 msec	1(2)
G.729	74 byte	20 msec	1(2)

3.2.3 VoIP Traffic session 검출

VoIP Traffic Session 검출 과정에서는 Flow 기반 VoIP Traffic Detection 단계에서 검출된 Voice Traffic Flow 후보군으로부터 실제 Voice Flow를 검출하고 이를 주고받는 IP Pair를 검출한다. VoIP 통화 음성 트래픽은 크게 두 가지 특성을 가진다. 첫 번째로 양방향성으로 Flow가 동시간대에 동일한 IP pair에서 생성되어 주고받는다. 두 번째로 음성이기 때문에 양방향 Flow의 Total packet size 비율이 5:5, 6:4, 4:6을 가진다. 따라서 IP Pair로 검출된 Flow에 대해 수식 2와 같이 양방향 Flow의 비율인 $Bidriection_{Ratio}$를 구하고, 임계치 값 BDR_{low-th}는 4, $BDR_{high-th}$는 6 인 조건에 만족할 경우 최종적으로 VoIP Traffic session으로 판단한다.

$$Bidriection_{Ratio} = \frac{BIG(FTS(f_i), FTS(f_j))}{FTS(f_i)+FTS(f_j)} \times 100,$$
$$where\ f_{i,j}\ is\ flow\ set\ of\ voice\ session,$$
$$FTS\ is\ Flow's\ total\ packet\ size.$$
$$\text{if} \begin{cases} Bidirection, \\ \quad \text{if } BDR_{low-th} \le Bidirectoin_{Ratio} \le BDR_{high-th} \\ Non\ Bidirection,\ Othrewise \end{cases}$$
$$where\ BDR_{low-th}\ is\ Bidirection_{Ratio}{}'s\ lower\ threshold,$$
$$BDR_{high-th}\ is\ Bidirection_{Ratio}{}'s\ higher\ threshold \quad (2)$$

2.3.4 Behavior Pattern Analysis

VoIP Traffic session을 검출 후 해당 IP Pair의 Traffic의 행위 분석을 통해 정상적인 VoIP 서비스를 제공하는 서비스 사업자의 장비인지, SIM Box를 사용한 불법적인 VoIP 서비스 인지를 판단하기 위해 정상적인 VoIP 서비스를 제공하는 트래픽의 특징을 정의한다. 정상적인 VoIP 서비스를 제공하는 서비스 사업자의 장비 간에 발생되는 트래픽 특징은 다음과 같다. 첫째 가장 주요한 특징으로 각 VoIP 서비스 사업자의 서비스는 24시간 동안 운용된다. 각 국가의 생활 습관에 따라 VoIP Call Volume의 형태가 약간 차이가 날수가 있지만, 무시할 만한 공백 기간을 포함하여, 24시간 중 약 22시간이상 유지된다. 두 번째로 국가별로 Call Volume은 업무 패턴에 따라 아침, 점심, 저녁, 그리고 심야를 기준으로 4번 변동된다. 국가별 업무 패턴에 따라 유동적일 수도 있으나 대부분 유사한 패턴을 가진다. 그림 6은 국내 VoIP 서비스를 제공하는 업체의 실제 24시간 Call Volume을 나타낸다. 그림 6에 따르면 업무가 시작되는 8~9시 사이부터 급격히 Call Volume이 증가하기 시작하고, 12시에 최대치를 기록한다. 그리고 점심시간 구간인 12~14시에 급격히 감소하였다가 오후 업무시간인 18시까지 일정 수준을 유지하다가 그 이후 급격하게 감소한다.

업무 패턴을 분석하기 위해 수식 3의 1차 미분을 사용한다. 1차 미분은 영상 처리에서 엣지를 검출하는데 주로 사용되는 도구로써, 밝기 값이(Intensity) 평탄한 영역에서는 그 값이 0을 유지하고, 급격하게 밝기 값이 증가할 때는 그 값이 0이상의 값을 유지하고 밝기 값이 감소할 경우 0이하 값을 유지하는 특성을 가진다[16]. 그림 6의 적색 그래프는 Call Volume 그래프를 1차 미분한 결과를 나타낸다.

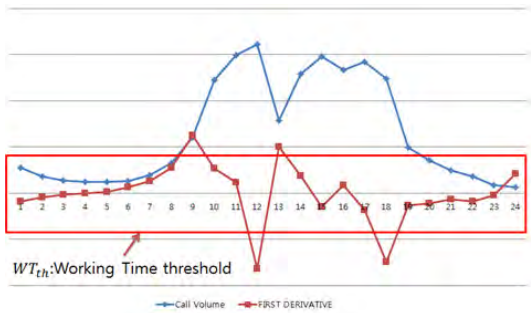

그림 6. 국내 24시간 Call Volume 과 업무 패턴 분석 예시
Fig. 6. Call Volume of operations around the clock & Analysis of working pattern

$$Working\ Pattern(T_i) = \frac{\partial f}{\partial x} = f(x+1) - f(x)$$
$$where\ x\ is\ call\ Volume\ of\ time\ T_i,$$
$$\text{if}\begin{cases} Working\ On\ Time, \\ \quad \text{if}\ |Working\ Pattern(T_i)| > WT_{th} \\ Working\ Off\ Time, otherwise \end{cases} \quad (3)$$

그림에서 확인할 수 있듯이 Call Volume이 변동이 없는 영역에서는 거의 0에 가까운 값을 유지 한다. 그러나 변동이 큰 영역에서는 1차 미분한 영역이 특정 임계치(Call Volume의 최대치와 비례함)이상 변동된 구간을 인식할 수 있다. 이를 기반으로 Call Volume의 변화 패턴을 인식하여 업무 패턴을 분석한다.

Ⅳ. 실 험

본 논문에서 제안된 SIM Box Fraud Detection System의 기능 시험을 위해서는 크게 세 분야를 나누어 실험하였다. 첫째 IX구간의 대용량 트래픽을 처리할 수 있도록 NPU(Network Processing Unit) 기반 단독형 시스템으로 개발된 SIM Box Fraud Detection System의 10G급 트래픽 수집 및 처리 기능, 두 번째로 VoIP 음성 트래픽 판별 기능, 마지막으로 정상적인 VoIP 서비스를 제공하는 장비와 SIM Box Fraud를 발생하는 장비 판별 기능이다. 첫 번째 실험은 TTA의 실험 의뢰를 통해 확인하였다. 그림 7은 패킷 처리 성능 측정 시험 구성도이다.

트래픽 생성 및 계측을 위해 'Spirent' 사의 'SPT-2U'를 사용하였다. 해당 트래픽 장비를 제안된 SIM Box Fraud Detection System 으로 연결하고 탭핑 장비를 연결하여 다시 계측기로 연결 한 후 계측된 결과와 제안된 장비 상에서 처리된 결과를 비교하였다. 실험은 무손실 패킷 수집 및 처리 성능에 대한 실험을 진행하였다. 실험 환경 및 실험 결과는 표 3과

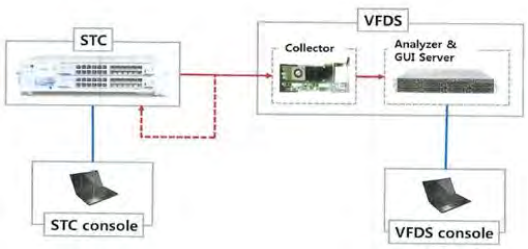

그림 7. SIM Box Detection System 의 10G급 트래픽 수집 및 처리 Test Bed 환경
Fig. 7. Test Bed of 10Gbps traffic collection & processing of SIM Box Detection System

표 3. 패킷 수집에 대한 실험 환경 및 결과
Table 3. Test Environment & Summary of Packet Collection

Packet Type	Packet Size	Traffic Load	Test Duration
UDP	300~500 Byte	2,400,000 pps	60 sec
Tester		SIM Box Fraud Detection System	
# of Packets		# of Packets	Processing Rate(pps)
144,000,0001		144,000,0001	2,400,002.373

같이 500byte의 패킷을 약 9.6Gbps의 처리량으로 손실 없이 2,400,000 PPS를 처리하는 것을 확인하였다.

두 번째와 세 번째의 기능을 확인하기 위해 그림 8과 같이 테스트 베드를 구성하였다. 실망에서 수집한 TEST pcap 셋들을 트래픽 재생기와 VoIP 계측기를 사용하여 트래픽을 생성하고, SIM Box Fraud Detection System통해 계측기 상의 정보 또는 WireShark로 확인된 pcap 셋의 내용과 비교하여 정확하게 Voice Flow를 검출함을 검증한다. 그리고 트래픽 재생기에서 정상적인 VoIP 서비스 사업자가 서비스하는 장비의 트래픽을 수집한 pcap 셋들을 재생하고, SIM Box와 IP-PBX를 사용하여 SIM Box Fraud 트래픽을 생성한다. 생성된 트래픽을 트래픽 집선 스위치로 유입하고 이를 미러링 하여 SIM Box Fraud Detection System으로 보낸다.

VoIP 트래픽의 생성을 위해 'Shenick'사의 'diversifEye 8400'장비를 사용하였다. diversifEye는 음성 부터 IPTV같은 영상(video) 트래픽의 생성뿐만 아니라, IP기반 전 범위의 멀티미디어에 대해 Testing/Monitoring이 가능한 소프트웨어를 제공한다. 두 번째 Voice Traffic Flow 인식 기능을 확인하기 위해 표 4와 같이 DiversifEye 8400 소프트웨어에서는 1개의 UAS(User Agent Server)와 1000개의 UA간에

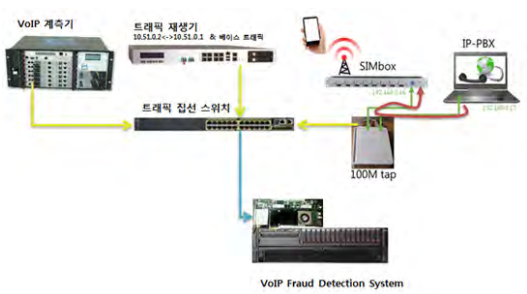

그림 8. SIM Box Detection System Test Bed 환경
Fig. 8. Test Bed of SIM Box Detection System

표 4. 코덱 별로 생성된 Traffic 인식 실험 결과
Table 4. Identified Experiment Results Of The Generated Traffic By Each Voice CODEC

CODEC	VoIP Tester	The number of Identified Voice Flow at SIM Box Fraud Detection System
g.711	1000 call/sec (BHCA:360000, AHTime:5sec)	2000 flows
g.723	1000 call/sec (BHCA:360000, AHTime:5sec)	2000 flows
g.729	1000 call/sec (BHCA:360000, AHTime:5sec)	2000 flows

시간당 총 360,000개의 통화가 발생하도록 하되, 통화는 각 코덱별로 5초간만 유지되도록 설정했다. 결과적으로 1000call / 10sec 에 해당하는 VoIP 트래픽들이 SIM Box Fraud Detection System으로 유입되도록 설정하였다. SIM Box Fraud Detection System에서 인식된 Voice Flow 수는 10 Sec 주기로 확인한 결과 정확하게 2000 flow로 음성을 인식할 수 있었다.

세 번째 정상적인 VoIP 서비스를 제공하는 장비와 SIM Box Fraud를 발생하는 장비의 IP Pair 정보 검출 기능을 확인하기 위해 그림 8의 테스트 환경에서 트래픽 재생기에서는 VoIP 서비스 사업자의 장비에서 주고받는 트래픽을 가정하여 10.51.0.2<->10.51.0.1사이에 주고받는 트래픽을 생성하고, SIM Box Fraud를 발생하는 환경으로 SIM Box(192.168.0.16)와 IP-PBX(192.168.17)는 IP-PBX를 통해 주기적으로 통화를 발생 시켰다. 이를 SIM Box Fraud Detection System으로 유입시켜 정상적인 Plain Traffic과 SIM Box Fraud의 Gray Traffic으로 분류하는 것을 확인하였다. 그림 9는 SIM Box Fraud Detection System의 GUI 화면으로 좌측 상단은 모니터링 트리, 하단은 분류된 트래픽을 5분단위로 보여준다. 그리고 우측은 상/하단은 모니터링 트리 상의 Flow, Session 등의 정보를 각각에 맞게 디스플레이 한다. 그림 9에서는 제안된 시스템의 SIM Box검출 결과로 Gray Traffic으로 판별된 SIM Box(192.168.0.16)와 IP-PBX(192.168.17)의 정보를 확인할 수 있다. 또한 정상적인 VoIP 서비스를 제공한 장비인 10.51.0.2<->10.51.0.1는 Plain Traffic으로 분류된 결과를 확인할 수 있다. 그림 9의 각 테이블에서 4, 5 번째 항목인 'Incoming/Outgoing Percentage of Bidirection Ratio'는 수식 2로 얻어지는 결과로써 거의 5:5를 유지하는 것을 알 수 있다. 표 2의 조건과 이를 통해 해당 세션들이 음성 트래픽임을 확인할 수 있다. 그리고 발/수신 횟수를 나타내는 6, 7번째 항목인 'Incoming/Outgoing Voice Session Count'에서는 Plain Traffic인 경우 둘 다 비슷한 횟수로 발생되지만, Gray Traffic인 경우 Outgoing Voice session이 많은 것을 확인할 수 있다. 11번째 항목인 'Session Activity Time'인 경우 Voice session이 발생된 시간의 총합을 나타낸다. Plain Traffic인 경우 실험 시간동안 지속적으로 통화가 발생하였고, 이에 비해 Gray Traffic은 Plain Traffic에 비해 약 5분의 1 정도 유지된 것을 확인할 수 있다.

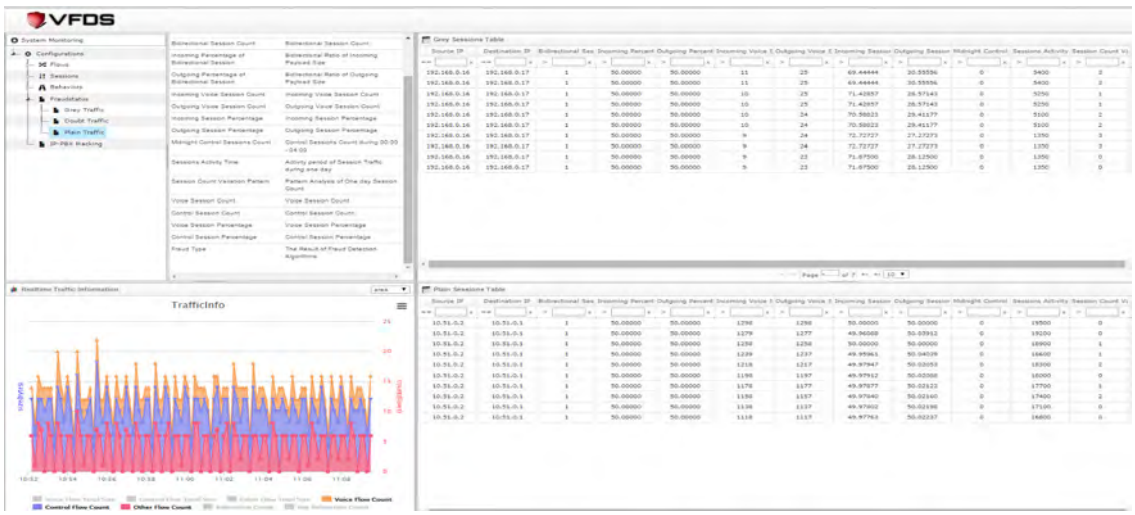

그림 9. SIM Box Fraud Detection System의 GUI 화면
Fig. 9. SIM Box Fraud Detection System GUI

V. 결 론

본 논문에서는 VoIP 네트워크상에서 발생하고 있는 다양한 Fraud에 대해 알아보고, 그 중에서 국제 통화 상에서 과금 관련 피해가 주로 발생하고 있는 SIM Box에 의한 Toll Bypass Fraud에 대해 분석하고, 이를 검출할 수 있는 방안을 제안하였다. 이를 검증하기 위해 실망에서 수집된 트래픽을 기반으로 검증된 테스트 장비를 사용하여 테스트 환경을 구성해서 실험을 진행 하였다. 그러나 보다 정확한 검증을 위해서는 실제 IX구간에 해당 장비를 설치해서 다양한 트래픽이 포함된 대용량 트래픽을 실시간으로 음성 트래픽 및 SIM Box에 대한 검출을 검증해야 한다. 일반적으로 트래픽 분석 기반의 FMS(Fraud Management System)와 테스트 전화 기반의 TCG(Test Call Generation)으로 크게 두 가지 방안으로 SIM Box를 검출하는 방식이 제안되고 있다. 그러나 FMS의 경우 본 논문에서 언급한 회피방안을 사용할 경우 성능이 급격이 저하되며, TCG 방식의 경우에는 비교적 정확도는 높으나 비용 등 환경상의 문제로 지속적으로 사용하기 어렵다. 따라서 본 논문에서는 FMS의 방식을 따르면서 VoIP Call Setup/Termination을 수행하는 SIP Signal을 암호화 등의 회피 방안을 해결할 수 있는 음성 트래픽의 특성을 기반으로 관련 장비를 검출하고 행위분석을 통해 Toll Bypass Fraud와 관련된 장비를 검출하는 방법을 제안하였다. 그러나 Fraudster 역시 지속적으로 회피 방안을 연구 개발하기 때문에 국제 통화 비용이 급격히 하락하기 전까지는 끝임 없이 새로운 Fraud가 생겨날 것으로 예상된다. IX구간에서 트래픽의 특성만으로 다양한 Fraud를 검출하기에는 역부족이다. 이를 해결하기 위해서는 VoIP 서비스 사업자의 내부에 위치한 DPI 기반 분석 시스템과 제안된 시스템의 연동이 필요할 것으로 예상된다. 따라서 대용량 트래픽을 손실 없이 수집 할 수 있는 트래픽 수집 기술과 DFI/A, DPI/A 기술과 대용량 데이터를 저장 및 분석할 수 있는 BigData 기술이 융합되어야한다. 그러고 각 분야 별로 심도 깊은 연구가 필요하기 때문에 지속적인 관심과 연구, 지원이 필요하다.

References

[1] Communications Fraud Control Association (CFCA), *Global Fraud Loss Survey Report*(2013), Retrieved Aug. 2014.

[2] S. S. Kim, "*Provider and consumers Unknown International Fraud calls*," Retrieved Mar. 19, 2014, from http://www.etnews.com/201305270513

[3] KAIT, *Trends on policy and technology of S&T and ICT*, no. 4, 2013, Retrieved Mar. 19, 2015, from http://www.kait.or.kr/notice/board_view.jsp

[4] TransNexus, *INTRODUCTION TO VOIP FRAUD*, 2012.10.18., Retrieved May 24, 2014, from http://transnexus.com/resources/telecom-industry-topics/fraud-detection/download-voip-fraud-white-paper/

[5] J. T. Ryu, K. Y. Ryu, and B. Roh, "A SIP INVITE flooding detection algorithm considering upperbound of possible number of SIP messages," *J. KICS*, vol. 34, no. 8, pp. 797-804, Aug. 2009.

[6] Y. H. Jung, K. M. Yang, J. W. Park, and K. C. Kim, "Denial of service detection on SIP-based VoIP client," in *Proc. KICS Int. Conf. Commun.*, pp. 706-710, Korea, 2008.

[7] J. W. Lee, H. J. Kim, J.-H. Eom, and S. H. Kim, "A study on toll bypass fraud and detection method of VoIP," in *Proc. KICS Winter Conf. Commun.*, pp. 728-729, Korea, 2015.

[8] D. Hoffstadt, A. Marold, and E. P. Rathgeb, "Analysis of SIP-Based threats using a VoIP honeynet system," *IEEE TrustCom*, pp. 541-548, Liverpool, Jun. 2012.

[9] I. Murynets, M. Zabarankin, R. P. Jover, and A. Panagia, "Analysis and detection of SIMbox fraud in mobility networks," *IEEE INFOCOM*, pp. 1519-1526, 2014.

[10] meucci, "*SIM Box Detection-Service Description,*" 01, Mar. 2012, Retrieved Mar. 19, 2014,

[11] metfone, *ILLEGAL BYPASS FOR INTERNATIONAL CALLS: INDUSTRY POSITION*, 2013.07. Retrieved Mar. 19, 2014, from http://www.slideshare.net/firdausf1/sim-box-issue

[12] http://www.meucci-solutions.com/

[13] http://www.asterisk.org/

[14] J. W. Lee and J. H. Eom, *APPARATUS OF DETECTING Toll Bypass Fraud,* Patent applied for 2015.

[15] T. Okabe, T. Kitamura, and T. Shizuno, "Statistical traffic identification method based on flow-level behavior for fair VoIP service" *IEEE Workshop VoIP MaSe*, pp. 35-40, Apr. 2006.

[16] Rafael C. Conzalez and Richard E. Woods, *Digital Image Processing,* 3rd Ed., Prentice Hall Press, 2008.

[17] J. Rosenberg, et al., *RFC 3261-SIP: Session Initiation Protocol*, 2002.

이 정 원 (Jung-won Lee)

2004년 2월 : 경성대학교 컴퓨터과학과 졸업
2006년 2월 : 경북대학교 컴퓨터 공학과 석사
2008년 3월 : 경북대학교 컴퓨터 공학과 박사 수료
2010년~현재: ㈜크레블 재직
<관심분야> 트래픽 분석, 멀티미디어통신, VoIP 등

엄 종 훈 (Jong-hoon Eom)

1986년 2월 : 경북대학교 전자공학과 졸업
1992년 2월 : 경북대학교 전자공학과 석사
1993년~2009년 : 한국통신(KT) 수석연구원
2004년 8월 : 경북대학교 전자공학과 박사
2010년~현재 : (주)크레블 대표이사
<관심분야> 통신공학, 광통신, VoIP 등

박 태 흠 (Ta-hum Park)

1987년 2월 : 경북대학교 전자공학과 졸업
1993년 2월 : 경북대학교 컴퓨터공학과 석사
2012년 ~2014 7월 : ㈜드림시큐리티 기술연구소 팀장
2014년 8월~현재 : ㈜크레블 기술 연구소 팀장
<관심분야> 통신공학, 멀티미디어, VoIP 등

김 승 호 (Sung-ho Kim)

1981년 2월 : 경북대학교 전자공학과 졸업
1983년 2월 : 한국과학기술원 전산학과 석사
1994년 2월 : 한국과학기술원 전산학과 박사
1985년~현재 : 경북대학교 컴퓨터학부 교수
<관심분야> 알고리즘, 멀티미디어통신 등