이동통신에서 단말기 불법 도용 탐지 및 관리 시스템

정윤경° 박형선 정문석
LG 정보통신(주) 중앙연구소 이동교환실

Fraud Detection & Management System in Mobile Communications

Yun Gyung Cheong° Hyoung Sun Park Moon Suk Chung
Mobile Switching Lab., R&D Center, LGIC Ltd.

요 약

이동통신 가입자의 폭발적인 증가에 따라 이동 단말기 정보의 불법 복제를 통한 이동 통신 서비스 도용의 사례가 증가하고 있다. 본 논문에서는 인증 센터와 연동하여 이동 단말의 불법 복제를 통한 이동 통신 서비스 도용을 탐지하고 이와 관련 정보를 저장 및 관리하는 시스템인 FDMS(Fraud Detection & Management Sytstem)를 제안한다.

1. 서론

일반적인 유선통신 서비스는 고정 위치에 설치된 전화기를 전화선으로 접속하여 통신 서비스를 제공하는 반면, 최근 이동통신 기술의 발전과 저렴한 서비스 가격으로 인해 그 이용도가 급격히 증가하고 있는 이동통신 서비스는 휴대용 이동 단말기를 이용하여 이동 교환기와 무선 인터페이스를 통해 정보 및 음성 전송 서비스를 제공한다.

그러나, 이동 단말기와 무선 전송이라는 특성상 간단한 장비만을 가지고 무선 통신 서비스를 쉽게 도용할 수 있는 가능성이 있으며 이러한 도용 사실을 탐지하고 방지하는 것이 어려워 실제로 이러한 사례가 빈번하게 발생하고 있다. 참고로, 미국의 경우 단말기 불법 복제에 의한 무선 통신 불법 도용의 비율은 전체 완료호 대비 5-30%로 추정되며 이러한 비용은 매년 수 천만에서 수 십억 달러로 추정되고 있다[1]. 이러한 불법 무선 통신 서비스 도용에 의해 이동 통신 서비스 품질 저하와 타 이동통신 서비스 제공 서비스나 육상라인 사용 등에 따른 운용 비용의 증가를 초래하고 불법 복제로 인한 피해 가입자는 서비스를 해지하는 등 이동 통신 서비스 공급자는 유지 비용의 증대와 가입자 감소라는 다중의 폐해를 겪게 된다. 따라서, 차세대 이동통신에서 이러한 단말기 불법 복제의 검출은 필수적인 기능으로 인식되고 있다[2].

본 논문에서 제시하는 FDMS(Fraud Detection & Management System)는 이러한 불법 도용의 예를 탐지 및 방지하고 관리하는 시스템으로서 인증센터와 연동되어 동작한다. 본 논문의 구성은 다음과 같다. 제 2 장에서 기존 연구에 대해 간략히 기술하며, 3 장에서 제안한 시스템에 대하여 설명한다. 마지막으로 4 장에서 본 구현에 대한 평가와 향후 연구과제를 기술한다.

2. 기존 연구 고찰

본 논문에서 “fraud”는 타인의 개인 정보 혹은 단말기 관련 정보를 취득하여 타인의 이동 통신 서비스를 사용하는 불법 가입자 혹은 사용자를 지칭한다. 이러한 “fraud”는 여러 종류가 있으나 본 논문에서는 두 가지로 분류한다. 첫 번째는 “subscription fraud”, 즉 타인의 정보를 사용하여 가입한 후 요금 미납으로 이동 통신 서비스가 정지될 때까지 사용하는 방식, 두 번째는 “cloning” 혹은 “tumbling”, 즉 이동 통신 서비스 사용시 정보가 무선을 통해 전송된다는 점을 이용하여 현재 이동 통신 서비스를 사용하고 있는 가입자의 MIN(Mobile Identification Number)과 ESN(Electronic Serial Number)을 특수 장치를 사용하여 취득한 후 해당 가입자에게 속하지 않은 단말기에 불법으로 취득한 정보를 입력하여 이동 통신 서비스를 사용하고 요금을 정상 가입자에게 부과하는 방식을 의미한다[3]. 본 논문에서는 “cloning” 방식을 이용한 불법 복제 단말기 사

용자를 탐지하는 방법에 대하여 기술한다.

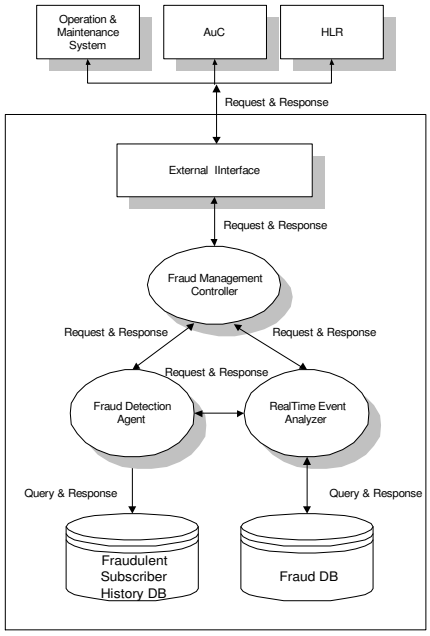
이러한 fraud 를 탐지하는 것을 Fraud Detection 이라 하며 구현 방식은 여러 기준을 이용하여 분류할 수 있는데, 일반적으로 rule-based 방식, data-mining 방식 및 neural network 방식으로 나눌 수 있다. 첫째, rule-based 방식은 absolute analysis 로서 모든 가입자의 호 사용 패턴에 대해 동일하게 적용할 수 있다. 이러한 구현 예는 둘 이상의 단말기가 동시에 발신/통화/착신하는 경우, 연속된 호 통화 사이의 위치 정보를 속도로 변환하였을 때 해당 가입자가 시간내에 이동하였다고 판단할 수 없는 경우, registration signal 이 불규칙하게 발생하는 경우 등이 있다[4][5]. 둘째, data mining 방식은 differential analysis 로서 가입자의 과거의 호 통화 패턴을 저장해 두고 새로이 발생하는 호 통화의 패턴이 기존의 가입자 패턴과 심하게 다른 경우 단말기 복제로 판단하는 것이다. 이러한 예로는 가입자의 호 통화량이나 국제 전화의 사용량이 급격히 증가하거나 사용자가 가입하지 않은 부가 서비스를 사용하려고 시도하는 경우 등을 이용하여 단말기 복제를 탐지할 수 있다[6]. 마지막으로, neural network 방식은 machine learning 의 한 분야로서 가입자 관련 정보를 입력 뉴런으로 이용하고 단말기 복제 여부를 출력으로 하여 과거의 자료를 반복 학습하고 새로운 규칙을 생성하여 적용함으로써 단말기 복제 여부를 판별한다[7][3].

3. 제안한 시스템

3.1 시스템 구조

본 논문에서 제안하고자 하는 FDMS(Fraud Detection & Management System)의 구조는 [그림 1]과 같다. 본 시스템은 인증 센터와 연동하는 것을 전제로 하고 있으며 External Interface, Fraud Management Controller, Real-time Event Analyzer, Fraud Detection Agent 및 Database 로 구성되어 있다. External Interface 는 연동된 시스템(즉, OMS 와 AuC)로부터 Fraud Event 와 운영자가 요구하는 명령을 수신하여 Fraud Management Controller 에 전송하고 그 결과를 OMS(Operation & Maintenance System)에 전송한다. Fraud Management Controller 는 External Interface 로부터 수신한 Fraud Event 를 적절한 기능 블록에 배분하고 각 블록이 수행한 분석 결과를 전송하는 전체 제어 블록이다. Real-Time Event Analyzer 는 Fraud Management Controller 에 의해 동작 개시되며 현재 발생한 Fraud Event 의 가입자가 Fraud DB 에 존재하는지 확인한다. 해당 가입자가 존재하는 경우 Fraud Management Controller 에 해당 가입자가 단말기 복제 가입자임을 알린다. 해당 가입자가 Fraud DB 에 존재하지 않는 경우는 현재 발생한 Fraud Event 분석만으로 해당 가입자가 단말기 복제 사용자인지 판단한다. 해당 이벤트만으로 단말기 복제 사용자로 판단하기 어려운 경우 Fraudulent Subscriber History DB 에 이벤트 정보를 저장한다. Fraud Detection Agent 는 Fraud Management Controller 나 운영 정책에 의해 주기적으로 혹은 최한시를 이용하여 동작 개시된다. Fraud Detection Agent 는 Fraudulent Subscriber History DB 의 첫번째 레코드부터 모든 레코드에 대해 순차적으로 검색하여 운영자가 지시한 단말기 불법 복제의 요건에 부합하는지 분석 및 판단한다. 단말기 복제 가입자로 판단된 경우 해당 가입자를 Fraud DB 에 저장하고 Fraudulent Subscriber History DB 에서 삭제한후 단말기 복제로 판단된 가입자에 대한 정보를 Fraud Management Controller 에 송신한다.

운영자는 단말기 복제로 보고받은 가입자에 대한 확인 및 처리 절차를 진행한다. 해당 가입자에게 직접 전화를 하거나 메시지를 남겨 가입자가 정상사용중임을 확인하면 Fraud DB 에서 해당 가입자를 삭제하고 해당 가입자에 대한 Fraudulent Subscriber History DB 에서 가입자 의심도를 초기화하도록 한다. 단말기 복제로 판명된 가입자에 대해서는 서비스 이용을 금지하거나 제한하는 등의 해당 조치를 취한다.



[그림 1. Fraud Management System Architecture]

3.2 DB 구조

기존의 Fraud Detection 시스템에서 가입자 정보를 하나의 DB 로 관리하였던 것에 비하여 FDMS 에서는 단말기 도용 가입자와 도용의 가능성이 있는 가입자의 DB 를 분리하여 저장한다. Fraud DB 와 Fraudulent Subscriber History DB 는 배타적이다. 즉, Fraud DB 에 저장된 가입자는 Fraudulent Subscriber History DB 에 속하지 않으며 그 반대의 경우도 같다. Fraud DB 는 해당 가입자가 "fraud"로 판명된 시점의 시각, 식별자, 제한 서비스의 종류를 나타내는 필드를 가지고 있다. Fraudulent Subscriber History DB 는 인증 관련 이벤트 메시지가 발생한 가입자에 대한 이벤트 발생 정보 및 의심도를 가지고 있으며 Fraud Detection Agent 에 의해 fraud 로 판명된 경우 Fraudulent Subscriber History DB 에서 삭제된다. DB 의 자세한 속성은 [표 1]와 [표 2]을 참조한다.

이와 같은 방법으로 분리하여 저장하는 경우 저장 공간을 절감할 수 있으며 여러 프로세서가 동시에 접근하지 않으므로 접근 속도를 향상시키고 DB 의 안정화를 꾀할 수 있다.

[표 1 Fraud DB]

MIN	Restriction	IsFraud	TIME
0708180000	No Outgoing Call	Y	1998/11/02/14:40
0702741436	No International Call	N	1999/01/01/12:11
0703840002	No International Call	Y	1998/12/04/17:22
……	……		……
0705320092	Barring All Calls	Y	1998/12/11/18:20
0704569823	No Incoming Call	Y	1999/01/07/05:05

[표 2. Fraudulent Subscriber History DB]

MIN	ESN	MSC ID	TIME	EVENT			Suspect Level
				E1		En	
0708180001	C9000010	7	98/12/1	12	…	2	304
0708180004	C9000013	1	98/10/2	0	…	4	150
0708180235	C9000016	2	99/3/2	1	…	3	142
……							
0708180476	C9000201	3	99/5/31	4	…	1	50
0708180871	C9000243	2	97/12/3	6	…	0	100
0708180901	C9000274	4	98/11/1	1	…	4	72

3.3 불법 복제 단말기 탐지

제안한 FDMS 은 [표 3]와 같은 인증 실패 메시지가 발생한 경우 이를 Fraud Event 로 사용한다. 단말기 불법 복제 여부 분석 동작이 개시된다. 아래 [표 3]의 Fraud Event 는 인증 실패 메시지로서 TIA/EIA/IS-41.C 에 대부분 정의되어 있다[8].

[표 3. Fraud Event]

Index	Fraud Event Message
0x01	AUTHR mismatch
0x02	COUNT mismatch
0x03	SSD Update fail
0x04	Unique Challenge fail
0x05	SSD Update not attempt/no response
0x06	Unique Challenge not attempt/no response
0x07	COUNT Update not attempt/no response
0x08	SSD Update retry
0x09	COUNT Update retry
0x0A	RANDC mismatch
0x0B	Count Request Error
0x0C	Count Request Ack without Count

[표 4. 의심도 설정 분류기준]

	ATTR1	ATTR2	ATTR3
0	clear	Nothing	Nothing
1	normal	RANDC	Retry
2	noticeable	SSD	no response
3	critical	Count	Fail
4		Unique	Mismatch
5		AUTHR	Error

[표 4]에서는 [표 3]에서 정의한 Fraud Event 에 대한 의심도 설정을 일관성있게 하기위해 고안된 의심도 결정함수의 분류 항목을 제시한 것이다. 각 Fraud Event 는 항목별로 분류될 수 있으며 이러한 항목의 속성을 조합하여 의심도를 설정할 수 있다. 발생 이벤트에 대한 분석을 N 개의 속성 항목으로 분류할 경우 발생 이벤트에 대한 i 번째 속성의 값은 x_i 으로 나타낼수 있고, 이에 대한 의심도 설정은 $f(x_1, x_2, ..., x_N)$ 으로 나타내어진다. 이를 [표 3]의 AUTHR Mismatch 이벤트의 예로 들어 설명하면 [표 4]의 ATTR1 항목은 severity 를 나타내는 항목으로 발생한 이벤트에 대한 fraud 정도를 나타내는 항목이다. 이러한 항목 분류를 따를 때, AUTHR Mismatch 이벤트는 운영자가 판단하기에 severity 가 높다고 판단되어 critical 로 분류되며 해당값은 3 이 된다. ATTR2 항목은 이벤트가 발생한 operation 의 종류를 나타내고 AUTHR Mismatch 이벤트는

AUTHR 에 포함되므로 해당값은 5 가 된다. ATTR3 항목은 발생한 실패의 종류로 AUTHR Mismatch 이벤트는 mismatch 에 해당하므로 해당값은 4 가 된다. 따라서, AUTHR Mismatch 이벤트는 운영자가 정의한 의심도 결정 속성 벡터 (3,5,4)로 재정의될 수 있으며 이러한 값은 의심도 결정함수의 입력이 되고 출력결과는 이벤트의 의심도로 사용된다. 즉, 의심도 결정함수를 [수식 1]로 정의했을 때, 의심도는 [수식 2]에서 보는 바와 같이 56 으로 결정된다. 여기서 의심도 결정함수는 운영자 혹은 시스템 설계자에 의해 다른 함수로 변경될 수 있다. [수식 3]은 이러한 의심도 결정함수 정의의 다른 예를 나타낸다.

$$f(x_{attr1}, x_{attr2}, x_{attr3}) = x_{attr1}{}^3 + x_{attr2}{}^2 + x_{attr3} \quad \text{[수식 1]}$$

$$f(3,5,4) = 3^3 + 5^2 + 4 = 56 \quad \text{[수식 2]}$$

$$f(x_{attr1}, x_{attr2}, x_{attr3}) = 10^2 \times x_{attr1} + 10 \times x_{attr2} + x_{attr3} \quad \text{[수식 3]}$$

위에 기술한 방식으로 설정된 각 Fraud Event 에 대한 의심도는 발생시마다 해당 가입자의 Fraudulent Subscriber History DB 의 Suspect Level 필드에 누적되어 저장된다. 의심도 수치가 시스템에서 미리 설정한 임계치를 넘어서거나 특정 이벤트가 반복하여 발생하면 시스템은 해당 가입자를 “fraud”로 판단하고 운영자에게 이를 통보한다.

4. 결론 및 향후 연구과제

본 논문에서는 급격히 확대되는 이동통신 서비스의 문제점으로 부각되는 단말기 불법 복제를 탐지 및 관리 하는 FDMS 를 제안하였다.

제안한 FDMS 의 장점은 다음과 같다. 첫째, 기존의 연구에서는 인증 센터를 대체하는 개념으로 단말기 불법 복제 탐지 시스템을 구현하였으나 제안한 FDMS 는 인증 센터와 연동하여 가입자 정보를 저장, 분석 및 관리하므로 상호 보완적으로 동작하면서 불법 단말기 복제자를 보다 정확하게 탐지하도록 한다. 둘째, 가입자의 정보를 저장하는 데이터베이스를 그 특성에 따라 분리하여 관리함으로써 정보 관리의 효율성을 높였다. 셋째, 기존의 운영자 의존적인 의심도 설정을 보완하기 위하여 의심도 설정 함수를 제안함으로써 의심도의 일관성을 보장하였다. 넷째, 가입자 정보 분석 방법으로 Agent 를 제시함으로써 이동통신의 특성인 이동성과 정보의 분산성 및 운영자의 다양한 분석 요구에 적합하도록 설계하였다.

그러나, 본 논문에서 제시한 FDMS 는 현재 인증 센터에서 제공하는 인증관련 정보로 한정되어 있다. 따라서, 향후 HLR 과 AuC 에 선택적으로 연동하여 동작할 수 있는 유연한 시스템으로의 개발이 요구된다. 또한, 제시한 Fraud Detection Agent 는 현재는 이동 단말기 불법 복제 정보 분석 기능만 구현되어 있으므로 추후 Agent 로서의 이동성 및 사용자 인터페이스 측면이 보완되어야 한다.

[참고문헌]

[1] Melissa Vadman, Mobile Radio Technology, Intertec Publishing Corporation, pp.36 – 38, March 1997.

[2] Susan M. Ahimovic, Joan M.Michaels, “Services for Tommorow’s PCS,” Universal Personal Communications Personal Communications: Gateway to the 21st Century, Vol.1, pp. 222-227, 1993.

[3] P Burge, J Shawe-Taylor, C Cooke, Y Moreau, B Preneel, C Stoermann, “Fraud Detection and Management in Mobile Telecommunications Networks,” European Conference on Security and Detection, Conference Publication No. 437, pp. 91-96, 1997.

[4] Cooper John R., Sonberg Kenneth W., Eletronic Data Systems Corporation, “Apparatus for detecting and preventing subscriber number cloning in a cellular mobile telephone system”, US Patent US5335265, 1994.

[5] Umesh J., Redmond, Lorin B., Russell, John, AT & T Wireless Services, INC., WO98/3340 Detection of Fraudulently Registered Mobile Phones, 1997.

[6] Johnson Eric A., Liss Michael D., Jensen Flemming B.,Coral Systems, “Apparatus and method for detecting fraudulent telecommunication activity”, US Patent US5345595, 1994.

[7] Michiaki Taniguchi, Michael Haft, Jaakko Hollmen, Volker Tresp, “Fraud Detection in Communication Networks Using Neural and Probabilistic Methods,” Proceedings of the IEEE Internatinal Conference on Acoustics, Speech, and Signal Proc., Vol.2, pp.1241-1244, 1998.

[8] TIA, “TIA/EIA/IS-41.C Cellular Radiotelecommunications Intersystem Operations”, 1996.

저자 연락 정보

1. 논문제목

이동통신에서 단말기 불법 도용 탐지 및 관리 시스템

Fraud Detection & Management System in Mobile Communications

2. 저자명 : 정윤경 (Yun Gyung Cheong), 박형선(Hyoung Sun Park),
정문석(Moon Suk Chung)

3. 논문분야 : (12) 이동통신, (21) 통신소프트웨어,
(22) 초고속정보통신, 기타 통신관련분야

4. 주소 : 431-080 경기도 안양시 동안구 호계동 533 LG 제 1 연구단지
LG 정보통신 교환연구소 이동교환실

5. 전화/팩스 : 회사: 0343)450-7134, 집: 0343)383-1436 팩스 : 0343)450-7104

6. 전자우편 : ykj@lgic.co.kr parkhs@rex.lgic.co.kr mschung@rex.lgic.co.kr