http://dx.doi.org/10.5392/JKCA.2011.11.12.071

온라인 게임 악용 패턴 모니터링 방법의 성능 분석

Performance Analysis of an On-line Game Abuse Pattern Monitoring Method

노창현, 손한성
중부대학교 게임학과

Chang Hyun Roh(chroh@joongbu.ac.kr), Han Seong Son(hsson@joongbu.ac.kr)

요약

CEP(Complex Event Processing)는 대규모 정보시스템에서 발생하는 복잡한 이벤트 패턴을 발견하는 기법이다. 게임 사용자가 게임 서버에 접속하여 게임을 수행하는 과정에서 발생하는 이벤트들을 관찰하면서 규칙에 위배되는 행위를 검출하기 위하여 CEP 기법을 사용하는 방법이 제안된 바 있다. 본 연구는 실제 게임서버 DB를 이용하여 선행 연구를 통해 제안된 모니터링 방법에 적용하여 보았다. 이를 통해 CEP 기반의 온라인서비스 감시가 대규모 사용자들이 이용하는 온라인 게임의 부정한 사용자들을 찾아내고 감시하는 것에 효과적임을 관찰하였다.

■ 중심어 : | 온라인 게임 감시 | 사용자 악용 감시 | CEP | 성능 분석 |

Abstract

CEP(Complex Event Processing) is a technique to find complex event pattern in a massive information system. Based on CEP technique, an abuse pattern monitoring method has been developed to provide an real-time detection. In the method, the events occurred by game-play are observed to be against the rules using CEP. User abuse patterns are pre-registered in CEP engine. And CEP engine monitors user abuse after aggregating the game data transferred by game logging server. This article provides the performance analysis results of the abuse pattern monitoring method using real game DB. We results that the method proposed in previous study is effective to monitor abusing users

■ keyword : | Online Game Monitoring | Abuse Pattern Monitoring | CEP | Performance Analysis |

Ⅰ. 서 론

온라인 게임은 인터넷을 통해 게임 서버에 여러 사용자들이 동시에 접속하여 즐기는 게임을 말한다. 국내에서 가장 많은 사용자를 확보하고 있는 온라인 게임 장르는 MMORPG(Massively Multiplayer Online Role Playing Game)이다. MMORPG는 여러 사용자들이 가상 공간에서 다른 사용자와 협력하여 몬스터 사냥, 퀘스트 수행 등을 하고, 이를 통해 경험치를 얻고 게임머니(game money)를 벌어들이고 아이템을 획득하면서 자신의 캐릭터를 성장시키는 게임을 말한다[1].

온라인 게임 개발업체들은 개발된 게임 소프트웨어를 여러 대의 온라인 서버에 설치하고 주기적으로 업데이트하면서 게임 서비스를 제공한다[2]. 온라인 게임은

접수번호 : #111013-003
접수일자 : 2011년 10월 13일
심사완료일 : 2011년 11월 16일
교신저자 : 손한성, e-mail : hsson@joongbu.ac.kr

개발 프로그램이 방대하고 진행 과정이 매우 복잡하기 때문에, 게임 출시 이후에도 여러 가지 버그가 발생하는 경우가 많아 지속적으로 발견하여 수정해야 한다. 그러나 게임 개발자들이 인식하기 전에 발견된 버그를 사용자들이 자신에게 유리하도록 이용하는 경우가 종종 있으며, 이를 악용 또는 어뷰징(Abusing)이라고 부른다. 악용 방법이 사용자에 의해서 발견되면, 지인들을 통하여 게임 이용자들 사이에 급속도로 확산되는 양상을 보인다. 만약 악용에 대한 대응이나 프로그램 수정이 늦어지는 경우에는 정상적인 사용자들이 상대적인 피해를 입게 되어 게임에 대한 신뢰도가 하락하게 될 뿐만 아니라, 심각한 경우에는 사용자 이탈로 인한 게임의 존폐에 영향을 미치기도 한다. 이 때문에, 얼마나 빨리 프로그램 버그를 발견하고 사용자 악용을 감시하고 방지하느냐가 게임 서비스의 신뢰도 유지에 매우 중요한 이슈이다[3].

그런데, 온라인 게임에서는 사용자 수가 워낙 많고 게임 진행 과정도 매우 복잡하기 때문에 실시간 감시 기능을 구현하기가 쉽지 않다. 또한 게임 실행 결과가 주기적으로 저장되는 데이터베이스도 분석하기 매우 방대하며, 매일 대규모 데이터가 누적되기 때문에 설령 분석한다고 하더라도 즉각적인 조치를 취하기가 어렵다[3].

따라서 온라인 서비스의 감시 도구는 넘쳐나는 데이터 속에서도 각종 서비스 장애 상황을 가급적 신속(Early Warning)하게 알려주는 기능을 갖추어야 한다. 또한 비정상적인 상황이 나타나더라도 이것이 타당한 원인이 있기 때문에 그런 것인지, 아니면 불법적인 방법에 의해 나타난 현상인지를 판단할 수 있는 방법도 온라인 서비스 감시 장치는 갖추고 있어야 한다[3].

이를 위해서 본 연구진은 선행 연구를 통해, CEP(Complex Event Processing)엔진을 사용하여 온라인 서비스 중에 온라인 게임 사용자들의 악용(Abuse) 패턴을 감시하는 방법을 제안한 바 있다[3]. CEP는 대규모 정보시스템에서 발생하는 복잡한 이벤트 패턴을 발견하는 기법이다[4]. 이 연구에서는 게임 사용자가 게임 서버에 접속하여 게임을 수행하는 과정에서 발생하는 이벤트들을 관찰하면서 규칙에 위배되는 행위를 검출하기 위하여 CEP 기법을 사용하였다. 이는 사용자들이 자주 악용할 가능성이 있는 이벤트 패턴을 미리 복합 이벤트로 설정하여 CEP 엔진에 등록해 두고, CEP 엔진은 게임 서버에서 발생하는 이벤트를 실시간에 필터링하여 사용자 악용을 감시하는 방법이다.

선행 연구를 통해 제안된 CEP 기반 온라인 게임 악용 패턴 모니터링 방법[3]은 사용자 악용패턴을 감시하는데 실제 효과적이라는 구체적인 증거를 제시하지 못했다. 그러므로, 본 연구에서는, 실제 게임 서버 DB를 활용하여 제안된 방법이 산업 현장에서 사용 가능한지에 대한 성능 분석을 하였다. 이를 통해서 온라인 게임에 대한 사용자 악용 패턴 모니터링 전략 수립에 도움을 얻을 수 있을 것이다.

II. 온라인 게임 감시 방법

1. 악용 패턴 (Abuse Pattern)

온라인 게임의 악용 패턴은 게임의 종류에 따라 다를 수 있지만 MMORPG의 경우 게임머니, 아이템 취득 과 관련하여 악용 사례가 많다. 이와 같은 악용 형태를 나름대로 정형화 할 수 있다면, 게임 관리자는 이처럼 잠재적인 악용을 탐지할 수 있는 패턴을 지정함으로써 사용자들의 악용을 실시간에 감지하여 사용자들의 악용 위험에 빠르게 대응할 수 있다[3].

2. 감시 과정

선행 연구에서 제시한 악용 감시 과정은 그림 1과 같다. 먼저 관리자는 악용 패턴을 미리 정의하여 CEP 엔진에 등록하고, 실시간에 사용자들의 게임 실행 이벤트를 수집하여 CEP 엔진에게 전달하면, 악용을 감지하여 관리자에게 보고하는 과정으로 구성된다.

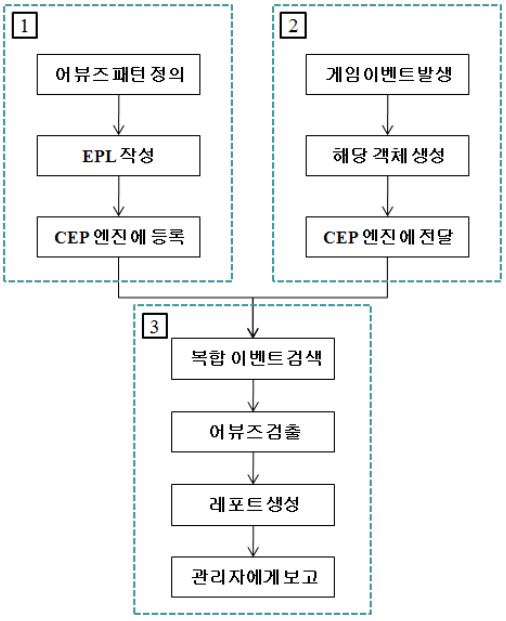

그림 1. 온라인 게임 감시 과정 [3]

III. 온라인 게임 감시 시스템 구현

온라인 게임 감시 방법에 대한 성능 분석을 수행하기 위하여 다음과 같이 시스템을 구현하였다. 일반적으로 온라인 게임들은 여러 대의 게임 서버를 운용하는데, 이 게임 서버들은 개별적으로 사용자들의 게임을 실행시키고 상황을 전개한 후, 중요한 사용자 데이터 및 현황 정보를 로깅 서버를 통하여 데이터베이스에 저장한다[2]. 게임 서버에서 발생하는 이벤트들은 실시간의 상세한 정보를 포함하고 있지만, 게임 서버에 저장되는 정보는 불필요할 정도로 세부적인 데이터들이 많을 뿐만 아니라, 게임 서버의 이벤트를 직접 전달받는 것은 게임 서버의 속도 및 성능에 영향을 줄 수 있다.

그러므로 본 연구에서는 게임 서버로부터 직접 이벤트를 수집하는 것이 아니라, 게임 서버들이 주기적으로 로깅 서버에게 전달하는 이벤트를 분석함으로써, 게임 서버의 실행과는 완전히 분리된 구조로 이벤트를 수집하도록 감시 시스템을 구현하였다.

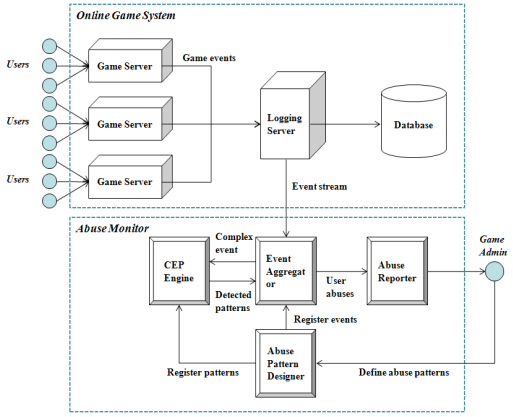

그림 2. 온라인 게임 감시 시스템 구조 [3]

[그림 2]는 본 연구에서 구현한 온라인 게임 감시 시스템의 구조를 보여준다. 온라인 게임 서버는 주기적으로 중요한 게임 사용자 데이터를 저장하기 위하여 로깅 서버로 데이터를 전달하는 데, 감시 시스템은 이 로깅 서버로부터 이벤트를 수집하여 이벤트 처리를 작동한다.

게임 관리자는 미리 Abuse Pattern Designer를 통하여 감시 대상이 되는 악용 패턴을 정의하면, 이는 실시간 이벤트를 수집하는 Event Aggregator에 이벤트를 등록하고, CEP 엔진에 추출할 이벤트 패턴을 등록한다. CEP Engine은 Event Aggregator로부터 전달받은 이벤트들을 감시하여 악용을 추출한 후, Abuse Report를 생성하여 관리자에게 전달한다.

CEP 엔진으로는 Esper[5]를 사용하였으며, 개발 언어는 Java를 사용하였다. 개발된 시스템의 주요 컴포넌트를 설명하면 아래와 같다[3].

- 게임 로그 시뮬레이터 (Game Log Simulator)
  - 사용자 n명과 아이템 m개를 가정하고 거래를 가상으로 수행한다.
  - 일부 거래에 확률적으로 abuse를 포함시킨다.
  - 거래 시 거래이벤트(TradingEvent)와 골드이벤트(GoldEvent)를 발생시킨다.

- 게임 이벤트 (TradingEvent, GoldEvent)
  - 모니터링할 거래이벤트과 골드이벤트를 정의한다.
  - 거래이벤트는 거래수행내역을 인스턴스화한다.

(buyerID, sellerID, itemName)
- 골드이벤트는 사용자의 골드양을 인스턴스화한다.(userID, gold)

- 이벤트 리스너 (Game Listener)
  - 거래이벤트와 골드이벤트를 모니터링한다.
  - 이벤트 패턴을 지정하여 해당되는 패턴을 추출한다.

- 테스트 (TestGameEvent)
  - 시뮬레이션을 실행시키고, 리스너를 생성하여 패턴을 추출하는 테스트를 실행한다.

- 이벤트 로그 해석기 (Event Log Parser)
  - 실제 게임에 직접 테스트해볼 수 없기 때문에, 실제 게임업체에서 획득한 게임로그 파일을 파싱하여 실제상황과 유사하게 이벤트를 발생시키도록 로그를 해석한다.

- 이벤트 어뷰즈 패턴 (Game Abuse Patterns)
  - 감시할 사용자 어뷰즈를 감지할 유형들을 다양하게 설정하여, 시스템에 반영시킨다.

- 게임 리포터 (Game Reporter)
  - 모니터링 결과를 보여주기 위한 감시보고서를 작성하여 보여준다.

IV. 성능 분석

1. 성능 분석 과정

성능분석을 위해 국내 M사에서 서비스 중인 MMORPG의 로깅 서버 DB를 이용하였다. 확보된 DB에서 감시 변수만을 추출하여 주기적으로 로깅 서버 시뮬레이터를 통해 게임 감시 시스템에 이벤트 데이터를 전송하였다.

또한. 악용 패턴에 대한 감시 환경을 설정하고 결과를 보여주기 위해 다음과 같은 사용자 인터페이스들이 구현되었다.

[그림 3]은 금일 불법거래 현황으로 금일에 해당하여 실시간으로 불법거래가 이루어진 데이터를 확인 가능하다.

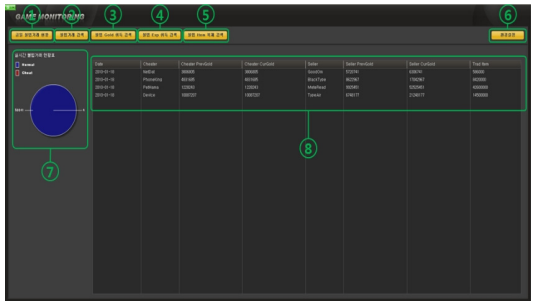

그림 3. 금일 불법거래 현황(실시간 아이템 트랜잭션 감시)

①~⑥은 감시항목별 메뉴이며 각각 금일 불법거래 현황, 불법거래 검색, 불법 Gold취득 검색, 불법 경험치(Exp)취득 검색, 불법 Item 복제 검색, 환경설정 순으로 구성되어 있다. ⑦은 일반적인 거래횟수와 악용에 의한 불법거래 횟수를 각각 파랑색과 빨간색으로 표시한 원형 그래프로 거래 규모와 불법거래의 발생 빈도를 통해 빠른 대처가 가능하다. ⑧은 불법거래를 한 사용자의 정보를 확인할 수 있다. 거래 날짜, 악용 유저, 악용 유저의 판매전후 금 보유량, 구입자, 구입자의 구입전후 금 보유량, 아이템의 가격 정보를 제공한다.

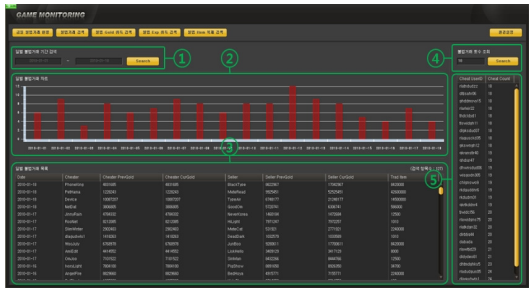

그림 4. 불법거래 검색(아이템 트랜잭션 감시)

[그림 4]는 불법거래 검색으로 기간을 지정하여 해당하는 기간의 불법거래 데이터를 확인 가능하다.

①은 텍스트 박스를 클릭하면 나타나는 달력을 이용해 날짜를 등록할 수 있고 Search버튼으로 ②, ③에 정

보를 호출한다.

②는 ①에서 지정한 기간 내에서 악용 횟수를 표현한 막대그래프이고, ③은 악용 날짜를 기준으로 내림차순 하여 유저의 데이터를 제공한다. 유저 데이터는 금일 불법거래 현황과 같다.

④는 텍스트박스에 임의의 수를 입력하고 Search버튼으로 입력한 수이상의 불법거래 유저의 정보를 ⑤에 호출한다. ⑤에는 악용 횟수를 기준으로 오름차순 하여 유저 ID와 악용 횟수가 표시된다.

[그림 5]는 불법 Gold 취득 검색으로 불법 Exp 취득 검색과 같은 인터페이스를 제공한다.

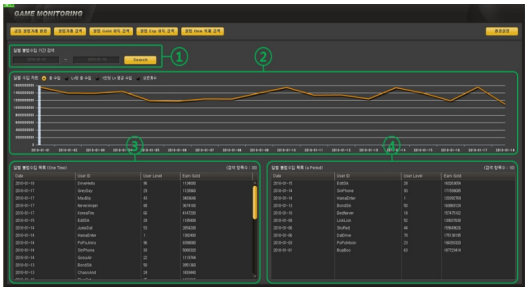

그림 5. 불법 Gold취득 검색 (골드 및 경험치 증가량 감시)

①은 불법거래 검색과 같은 기능을 하며 ②, ③, ④에 각각의 정보를 호출한다. ②는 ①에서 지정한 기간 내에서 총 수입, Lv당 총 수입, 1인당 Lv 평균 수입과 최근 일주일간의 상관계수를 선택하여 볼 수 있는 그래프이다. 그래프의 데이터를 이용하여 Gold량의 변화 추이를 파악할 수 있다.

③, ④는 일별 불법수입 목록으로 각각 ①에서 지정한 기간 내에서 악용 가능성이 있는 유저의 정보를 제공한다. 정보의 내용은 해당날짜를 기준으로 내림차순 하여 해당날짜, 유저 ID, 유저 Lv, 획득한 Gold이다. ③은 한 번의 획득 골드가 설정된 수치를 넘었을 경우에 해당하고, ④는 설정된 시간 동안 설정된 수치를 넘었을 경우에 해당된다. 각 수치는]그림 7]의 환경설정에서 설정이 가능하다.

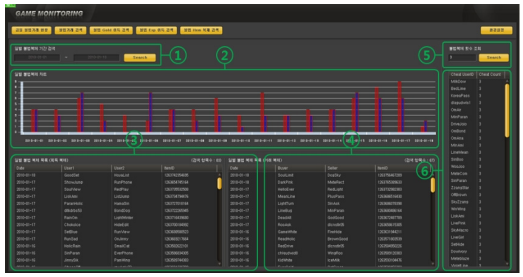

그림 6. 불법 Item 복제 검색

[그림 6]은 불법 Item 복제 검색으로 ①은 기존의 날짜 검색과 같은 기능을 하며, 기본 인터페이스는 불법 Item 복제에 대하여 [그림 5]의 불법거래 검색과 같은 기능을 한다. 불법 Item 복제는 획득 복제와 거래 복제 2가지로 구성되며, ②의 막대그래프는 지정 기간 내의 획득 복제와 거래 복제 횟수를 표시한 것이다. 각각 빨간색과 파란색으로 표시된다. ③, ④는 각각 획득 복제에 대한 유저 데이터, 오른쪽이 거래 복제에 대한 유저 데이터를 표시한 것이다. 데이터는 악용 날짜를 기준으로 내림차순하여 악용 날짜, 복제 아이템을 획득 혹은 거래한 User 2명의 ID, Item ID를 제공한다. ⑤, ⑥은 불법 Item 복제에 대하여 [그림 3]의 불법거래 검색과 같은 기능을 한다.

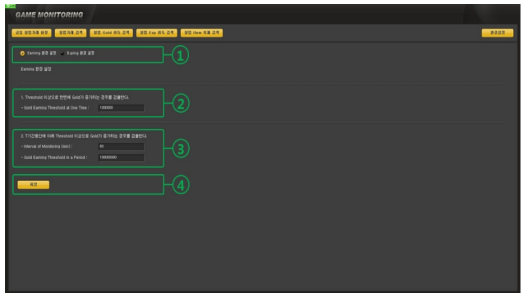

그림 7. 환경설정(불법 Gold 취득 설정, 불법 Exp 취득 설정)

[그림 7]은 [그림 5]에서 설명한 악용 가능성이 있는 유저를 검색하기 위하여 Gold 취득과 Exp 취득에 관련하여 설정할 수 있다. 두 가지 경우 모두 인터페이스는 같으며 ①로 설정항목을 선택한다. ②는 Threshold 이상으로 한번에 Gold 및 Exp를 획득하는 경우의 수치를 1 Gold 단위로 설정하고, ③ T기간 동안에 아래

Threshold 이상으로 Gold 및 Exp를 획득하는 경우의 수치를 분 단위와 1 Gold단위로 설정 가능하다. ④를 통해 설정된 수치를 저장할 수 있다.

2. 성능 분석 결과

위와 같은 과정을 통해 본 연구에서 개발한 CEP 기반의 악용 패턴 모니터링 방법에 대한 성능을 분석한 결과 다음과 같은 결과를 도출할 수 있었다.

과거 발생된 악용 유형을 지속적으로 패턴으로 추가 등록할 수 있기 때문에 확장성이 높으며, 일단 등록된 악용 패턴은 룰 기반으로 처리되기 때문에 이론적으로는 정확성을 보장할 수 있다. 단, 온라인 서비스에서 이벤트 발생 시점에서 네트워크 지연으로 인한 시간적 순서가 변경되는 경우에 악용 패턴에서 벗어날 가능성이 있지만, 네트워크 지연으로 인하여 시간적 순서가 변경되는 경우는 매우 드물다. CEP를 활용함으로써 방대한 이벤트가 들어오는 경우에도, 대용량 이벤트 스트림 처리를 위하여 특화된 CEP 엔진을 사용하기 때문에 데이터 누락이 없고, 스트림 처리 방식이기 때문에 저장 용량에 대한 한계도 없으므로 신뢰성이 매우 높다.

기존의 방법들이 데이터베이스에 저장된 실행 결과를 분석함에 비하여, 개발 기술은 이벤트 스트림을 직접 처리하는 엔진을 사용하기 때문에 발생되는 악용을 거의 실시간에 감시할 수 있다. 단, 이벤트를 엔진으로 배치 처리하는 경우에는 이벤트 전달 주기만큼의 지연이 발생할 수 있다. 예를 들어, 본 기술이 적용된 온라인 게임 감시의 경우, 게임서버에서 로그서버로 전달되는 주기만큼의 지연만이 발생 가능할 뿐, 거의 실시간 악용 모니터링이 가능하다.

본 결과를 요약하면 감시신뢰도는 사전 등록된 사용자 악용 패턴에 대하여 99.9%를 나타냈다. 또한, 온라인 게임의 로그 서버에 연결하고 로그 DB를 24시간 이내에 옮겨온다고 가정하면, 24시간 이내에 사용자 악용패턴을 찾아 낼 수 있다.

V. 결론 및 토의

본 연구는 온라인서비스 감시의 어려운 점을 효과적으로 해결해 줄 수 있는 방법으로서 CEP(Complex Event Processing, 복잡 이벤트 처리) 기법을 채택하여, 게임 사용자가 게임 서버에 접속하여 게임을 수행하는 과정에서 발생하는 이벤트들을 관찰하면서 규칙에 위배되는 행위를 검출하는 시스템을 개발하고 그 성능을 분석하였다. 현재 게임을 운영하고 있는 게임사로부터 제공된 실제 온라인서비스 데이터를 일부 분석하여, 그 속에 내재된 이벤트 패턴을 분석하였으며, 여기에서 도출된 패턴은 복합 이벤트로 설정하여 CEP 엔진에 등록해 두고, CEP 엔진은 게임 서버에서 발생하는 이벤트를 실시간에 필터링하여 온라인서비스의 불법적 사용을 방지할 수 있음을 확인하였다.

개발된 온라인서비스 감시 시스템의 로그 서버, CEP 엔진, 그리고 사용자 인터페이스가 통합 구현된 상태에서 성능 평가를 수행하여, 목표한 성능 수준을 만족하는지를 확인하였으며, 이를 통해 CEP 기반의 온라인서비스 감시가 대규모 사용자들이 이용하는 온라인 게임, 온라인 쇼핑, 온라인 커뮤니티 사이트의 부정한 사용자들을 찾아내고 감시하는 것에 효과적임을 관찰하였다. 향후 이러한 시스템의 기능을 확장하고 보안과 시스템 안정성을 향상시킨다면 실제적인 산업계 적용이라는 성과도 가능할 것으로 사료된다.

본 연구는 미리 입력된 패턴을 통해 사용자 행위를 감시하므로, 새롭게 방식의 불법행위 등을 찾아내는데에는 한계가 있다. 추후 새로운 방식을 스스로 학습하여 새로운 사용자 악용 패턴을 등록할 수 있도록 한다면 좀 더 효과적인 방법론이 될 것으로 생각된다.

참 고 문 헌

[1] 한국게임산업개발원 산업정책팀, *대한민국 게임백서 2008,* 한국게임산업진흥원, 2008.

[2] 최용준, “온라인게임 서비스 안정화”, 전자통신동향분석, 제22권, 제4호, pp.43-44, 2007(8).

[3] 노창현, “CEP 기반 온라인 게임 악용 패턴 모니터링 방법”, 한국콘텐츠학회논문지, Vol.10 No.1, pp.113-121, 2010(1).

[4] 손성호, “프로세스 기반 이벤트 분석을 이용한 비즈니스 활동 모니터링”, 한국전자거래학회지, 제12권, 제2호, pp.219-231, 2007.
[5] http://esper.codehaus.org

저 자 소 개

노 창 현(Chang Hyun Roh) 종신회원

- 1993년 2월 : KAIST 원자력공학과(공학사)
- 1995년 2월 : KAIST 원자력공학과(공학석사)
- 2001년 2월 : KAIST 원자력공학과(공학박사)
- 2006년 3월 ~ 2007년 2월 : 엠게임 정보기획실장, 엠게임 USA 개발 이사
- 2007년 3월 ~ 2007년 6월 : 엔트리소프트 미국지사 자문위원
- 2002년 3월 ~ 현재 : 중부대학교 게임학과 교수

<관심분야> : 가상세계, 온라인게임, 게임기획, Interactive Media

손 한 성(Han Seong Son) 정회원

- 1993년 2월 : 서울대 원자핵공학과(공학사)
- 1995년 2월 : KAIST 원자력공학과(공학석사)
- 2000년 2월 : KAIST 원자력공학과(공학박사)
- 2002년 4월 ~ 2004년 7월 : 한국원자력연구원 선임연구원
- 2008년 3월 ~ 현재 : 중부대학교 게임학과 전임강사

<관심분야> : 소프트웨어 신뢰도, 게임 소프트웨어공학, 소프트웨어 분석 및 설계