WWW 환경에서의 안전하고 효율적인 사용량 측정 방안

이경현* · 신 원* · 신정화*

1. 시작하며

인터넷은 개방성과 표준화된 기술을 바탕으로 상상조차 할 수 없는 빠른 속도로 성장해왔으며, 1980년대 초 WWW(World Wide Web)의 등장으로 새로운 전환점을 맞이하여 기존의 방송 매체와 함께 일반 개인 생활뿐만 아니라 여러 주요 산업에 엄청난 영향력을 발휘하고 있다. WWW은 수많은 전세계의 네트워크를 바탕으로 함으로써 인터넷 사용인구의 폭발적인 증가를 가져오게 하였으며, 또한 상업화의 급진전에 의해 기업의 마케팅 전략에 따른 방송, 신문에 이은 기업 홍보와 제품 광고의 장으로써 널리 활용되기 시작하였고, 최근 전자상거래의 등장으로 인한 새로운 지불 및 유통 방식이 등장하고 있는 실정이다. 특히 WWW을 이용한 광고 시장이 엄청난 규모로 성장하고 있어 현 추세라면 2000년도에는 그 규모가 수십 억 달러에 이를 것이라고 예측하고 있다[4][7]<그림 1>.

최근 전세계의 수많은 기업들이 이를 위해 각자의 웹 페이지를 개설하는 것뿐만 아니라 TV, 라디오, 신문 등과 마찬가지로 상업적인 광고를 목적으로 광고 대행자를 두고 일반 고객들을 끌어들이기 위해 노력하고 있다.

그러나 WWW의 HTTP(HyperText Transfer Protocol)에서 동작하는 사용자의 클라이언트와 광고 회사의 서버 사이의 상호동작에 대한 효율적이고 안전한 측정 방법의 부재로 인하여 서버의 웹 페이지에 대한 인기도 및 사용량 등의 정확한 측정이 어려운 실정이다. 이들 서버 대부분이 자신들이 제공하는 웹 페이지에 대한 클라이언트의 방문 수를 세는 것을 목적으로 하는데, 이를 바탕으로 광고 수입이 책정되고 있다[9]. 그러므로 광고 회사 대부분은 상업적인 목적을 위하여 인터넷 광고의 집행기준이 되는 접속건수, 광고 전달 회수 등을 경쟁적으로 부풀리고 있다. 이러한 형태의 표준화되지 않은 인터넷 광고 가격 체계와 효과적인 측정 기준의 애매 모호함으로 광고주나 광고 회사 모두 직 · 간접적인 피해를 입을 수 있다. 또한 최근에는 웹 서버의 측정 과정을

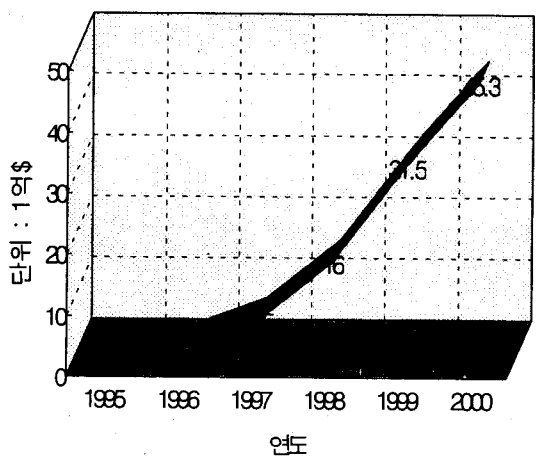


그림 1. WWW 광고 시장의 연도별 성장 규모

*부경대학교 전자계산학과

방해하려는 악의적인 클라이언트에 의한 서비스 거부 공격(Denial of Service Attack) 등도 등장하고 있다.

본 고에서는 WWW 환경에서 웹 페이지 사용량 또는 인기도 등을 측정할 수 있는 안전하고 효율적인 여러 방안을 살펴보는 것을 목적으로 한다. 이를 위해서 먼저 현재까지 사용되고 있는 광고의 여러 형태를 알아보고, WWW 광고 측정 방안에 대한 요구사항인 보안성(Security), 정확성(Accuracy), 효율성(Efficiency), 이동성(Turnover), 익명성(Anonymity), 표준화(Standardization) 등을 살펴본다. 또한 일반적인 측정 방안의 동작 방식을 살펴본 후 암호 기술 등을 이용한 측정 방안을 고려한다. 마지막으로 WWW 광고 측정 방안의 응용 기술과 그 미래를 전망한다.

2 WWW 광고의 형태

최근 인터넷이 기존의 TV, 라디오, 신문, 잡지에 이어 새로운 광고 매체로 등장하고 있다. 이러한 인터넷 광고는 그 특성상 기업의 마케팅이나 광고에 대한 전통적인 접근 방식을 크게 변화시키고 있다. 또 국내에서의 인터넷 광고는 단순 광고에서 벗어나 이벤트형 클럽 마케팅을 지향하는 데이터베이스 마케팅이 본격적으로 도입되고 있다.

현재까지 인터넷 광고 또는 WWW 광고는 단순히 특정 내용만을 전달하는 "수동적인 광고" 형태와 소비자들의 취향, 기호, 연령 등을 분석해 각 특성에 맞는 "능동적인 광고" 형태로 구현되어 왔으며, 이에 추가적으로 각종 애니메이션, 그래픽, 동영상까지 가미한 멀티미디어 광고가 늘어나고 푸시(Push) 기술 등을 적용한 강제형 광고도 등장하고 있다. 또한, 최근의 WWW 광고의 추세는 단독형 광고 형태에서 네트워크형 광고 형태로 변화하고 있음을 볼 수 있는데, 인터넷에 많은 광고의 등장으로 인해 하나의 웹사이트가 소비자들의 방문을 받을 확률이 낮아지는 추세이므로 여러 개의 웹사이트를 상호 연결하여 소비자들에 대한 메시지 전달 기회를 높이려는 것을 그 목적으로 하고 있다. 이와 같은 WWW 광고는 기존의 광고매체와는 달리 광고 그 자체로서 판매 경로를 확보할 수 있는 시장 역할을 수행할 뿐만 아니라 누가 광고를 보는가에 대한 정보도 전통적인 광고 매체에 비해 정확하게 제공해 줄 수 있는 장점을 가진다. 따라서 WWW 광고에서는 기존의 광고 매체와 달리 얼마나 많은 사람이 그 광고를 보았는지 알 수 있고, 서버에 있는 로그 파일 분석을 통해 특정 대상에 대한 광고를 구성할 수 있으며 광고 전달 회수와 클릭 회수를 계산해 광고에 대한 수요자 반응까지도 예측할 수도 있다. 이러한 특성을 기반으로 Chatterjee와 Patrali[3]은 현재까지 사용되고 있는 WWW 광고 형태를 "Banner advertisements"와 "Target advertisements"로 분류하였는데, 그 내용은 다음과 같다.

- 배너 광고(Banner ads.) - 수동적인 형태

  전통적인 광고 매체와 가장 유사한 특성을 가지고 있으며 현재 인터넷에서 가장 많이 사용되는 광고 형태이다. 웹 페이지내의 특정 위치에 작은 사각형 모양의 텍스트 및 이미지를 통한 광고를 말하는데, 사용자가 의도적으로 보려고 하는 것이 아닌 일방적인 형태의 광고이다. 일반적으로 사용자는 이를 클릭하여 해당 광고 메시지와 연결되는 목적 광고에 접근할 수 있게 된다.

  ◦ 고정형 배너 : 메시지나 이미지가 변화되지 않고 동일한 형태로 표현되는 것을 말한다.

그림 2. 고정형 배너를 이용한 광고 장면

◦ 애니메이션 배너 : 광고카피나 그림과 같은 배너 내의 표현요소들이 계속적으로 변화하면서 보여지는 형태를 말한다.

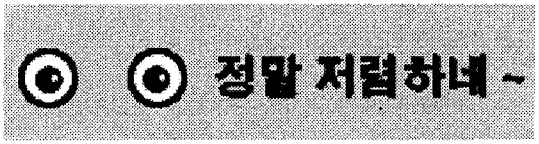


그림 3. 애니메이션 배너를 사용한 광고의 한 장면

이러한 형태는 소비자에게 광고 배너의 선택권이 있는 인터넷 광고의 특징에 따라 보다 주목률을 높일 수 있는 형태로 배너가 발전한 결과라고 할 수 있다. 현재 거의 대부분의 배너 광고가 주목률을 높이기 위해 애니메이션 형태를 띄고 있다. 애니메이션 배너가 고정형 배너보다 클릭률이 높다는 것은 이미 일반화되어 있는 사실이다.

● 목적 광고(Target ads.) - 능동적인 형태

WWW 광고를 전통적인 광고 매체와 확실하게 구분해 주는 광고 형태로, 방문자가 광고에 접근하기를 결정(주로 클릭)하여 적극적으로 광고를 접하는 형태인데 여러 가지 종류가 있다.

◦ 컨텐트형 광고 : 소비자들이 주로 찾고 많은 시간을 보내는 정보나 컨텐트를 활용해 브랜드 인지도를 강화하고자 하는 형태의 광고이다. 이 광고는 특정 사이트에 대해 스폰서를 제공하는 형태로 이루어지는데 기존 협찬 광고와 동일한 개념이다. 이 광고는 보다 세분화하기도 하는데 단순 협찬식 이외에 게임이나 채팅과 같은 컨텐트를 이용하는 상품배열(Product Placement), 관련업계 기사나 사설 등을 이용하는 기사 형식 광고(Advertorial)등이 있다. 컨텐트형 광고는 배너 광고 그 자체가 광고물이라는 상업성을 떨쳐버릴 수 없기 때문에 소비자의 관여도를 얻는데 제약이 있을 수 있다. 또한 광고에 따라 소비자에게 전달되는 위치나 시점이 고정되기 때문에 네티즌을 따라다니며 광고 메시지를 전하기란 불가능한 일이다. 이와 같은 단점을 보완하기 위해 개발된 광고 형태이다.

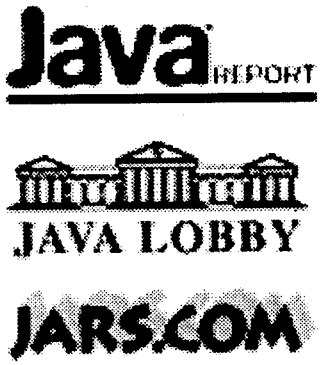


그림 4. Java site에서 제공하는 컨텐트형 광고

◦ 틈새형 광고 : WWW의 HTTP의 특성상 클라이언트가 서버에게 정보를 요청한 후 그 결과를 확인하고 다시 새로운 정보를 요구하는 행위를 반복하게 되는데 이 과정에서 생기는 정보 전달의 틈새를 이용해서 광고화면을 표출시키는 형태의 광고이다. 이 광고는 인터넷 회사들의 입장에서는 새로운 광고 공간의 확장이라는 점에서, 광고를 집행하는 기업의 입장에서는 사용자의 주목을 높일 수 있다는 점에서 활성화될 것으로 보

인다.

틈새형 광고는 배너 광고나 컨텐트형 광고에 비해 주목률이 상대적으로 높은 것이 사실이다. 하지만 사용자의 작업에 시간만 낭비하게 되는 형태로 진행될 때 광고를 하는 기업은 물론, 해당 웹사이트도 외면을 당하게 되므로 사용자에게 역효과를 불러올 가능성도 가지고 있으므로 조심스러운 접근이 필요한 광고이다.

◦ 푸시형 광고 : 소비자가 이미 설정한 환경에 따라 선택된 내용을 컨텐트와 함께 제공하는 광고형태이다. 이미 등록되어 있는 사용자 정보에 의해 정확한 목표 고객 선정이 손쉽고 멀티미디어형 광고물 제작이 가능하다. 그 반면 등록된 사용자만을 대상으로 하기 때문에 도달 범위에 제한을 받을 수 있다.

◦ 인터넷 액세스형 광고 : 사용자들에게 인터넷 서비스를 무료로 제공하고, 이에 대한 비용을 광고주로부터 받음으로써 사용자와 ISP(Internet Service Provider)가 모두 이득을 볼 수 있는 광고 형태이다. 사용자의 등록정보를 이용하므로 정확한 목표 고객에 접근할 수 있기 때문에 광고를 하는 기업도 효과를 얻을 수 있다.

3. WWW 측정 방안의 요구사항

WWW을 이용한 광고가 제대로 이루어지는지 확인하기 위해서는 광고주 자신들의 광고에 대한 그 효과를 측정하는 방법이 필수적이다. 인터넷 광고는 아직 표준화가 이루어지지 않은 부분이 많으며 특히 측정 분야는 그 정도의 폭이 크다. 그러므로 이러한 측정법을 통하여 광고주는 전통적인 TV나 신문과 같은 형태로 웹 광고에 대한 비용을 책정하게 된다. 그러므로 WWW 광고는 안전하고 정확하게 측정될 수 있어야 하고, 시스템에 무리를 주지 않도록 효율적으로 수행되어야 한다. 부가적으로 클라이언트의 이동성(Turnover)을 측정할 수 있어야 하고 익명성을 보장해주어야 한다. WWW 측정 방안의 요구사항을 살펴보면 다음과 같다.

● 보안성(Security)

WWW 광고는 대부분이 방문한 클라이언트의 수에 의해 광고비가 책정되므로 광고 회사에서는 이러한 상업적인 목적으로 인하여 자신의 웹 서버를 방문한 클라이언트의 수를 부풀리려 한다. 올바른 WWW 광고 측정을 위하여 어떤 서버가 자신에게 방문했다고 주장하는 클라이언트의 수를 조작하는 것이 사실상 불가능해야만 한다. 즉, 서버는 클라이언트 방문 수를 수학적으로 증명할 수 있어야 한다. 또한 서비스 거부 공격 등을 통하여 측정 과정을 방해하려는 악의적인 클라이언트로부터 보호되어야 한다.

● 정확성(Accuracy)

최근 클라이언트와 서버의 성능을 향상하기 위해 도입하는 캐쉬 기술 및 프록시 서버 등은 정확한 광고의 측정을 방해하거나 사용자의 성향을 파악할 수 없도록 하는 단점이 있다. 이에 대하여 객관적이고 과학적인 방법을 통하여 측정 방안의 결과는 가능한 한 정확해야 한다. 서버가 증명하는 방문 수에 대해서 허용될 수 있는 작은 오차 범위를 가져야만 한다.

● 효율성(Efficiency)

측정 과정은 주로 서버에서 일어나며 수많은

클라이언트와 직접 통신하며 HTML 문서를 통한 광고를 전달하고 있다. 따라서 HTTP에 기반한 많은 통신량과 시스템 부하를 감당하고 있으므로, 측정 과정이 포함됨으로 인하여 시스템에 많은 부하를 주지 않도록 하고 가능한 한 통신량은 작도록 설계되어야 한다. 특히, 광고 측정은 서버와 클라이언트의 상호 작용으로 이루어지므로 사용자 입장에서 클라이언트의 계산량과 메모리 사용량은 최소이어야 한다.

- 이동성(Turnover)

서버를 방문했던 과거 어느 시점의 클라이언트와 현재 시점의 클라이언트 사이에 대한 비율을 측정할 수 있어야 한다. 즉, 어느 기간 동안 서버를 방문한 대부분의 클라이언트들이 그 이전에 서버를 역시 방문했는지 아닌지를 설명할 수 있어야 한다. 이동성을 분석하여 사용자의 성향, 사용 시간대, 이동량 등을 측정할 수 있으며 이를 기반으로 앞으로의 광고 방향을 수립하고 특정 사용자를 대상으로 마케팅을 펼칠 수 있도록 해준다.

- 익명성(Anonymity)

측정 과정의 상호동작에서 클라이언트의 정보가 쿠키나 에이전트 등을 통하여 서버로 전송되는데 이 때 클라이언트의 프라이버시가 누출된다. 서버가 이를 악의적인 목적으로 사용할 수도 있으므로 측정 과정 중 클라이언트의 프라이버시를 침해하지 않도록 익명성을 허용해주어야 한다. 보다 강력한 성질은 같은 클라이언트에 의해 발생하는 서로 다른 방문을 서버가 구분할 수 없도록 하는 비연결성을 제공하는 것이다.

- 표준화(Standardization)

Novak과 Hoffman[9]은 웹 측정에 있어 현실정을 살펴보고 웹 측정 과정을 표준화하는 것이 중요하다고 논의하였다. 특히, 시장의 방향성을 제시한다는 측면에서 가장 민감한 부분인데 WWW 광고는 아직 표준화가 이루어지지 않은 부분이 많으며, 광고 효과 측정 부분에서는 광고 회사의 측정 기준에 따라 그 결과가 서로 다르게 나올 수 있다. 측정 수단, 사용되는 단위의 통일, 결과 보고 형태 등이 이 부분에 속하는데 단순한 광고 효과 측정의 객관성 확보뿐만 아니라 광고 비용 산출, 다른 광고 매체에 대한 비교 등을 제공해주어야 한다.

4. 동작 방식

다른 광고 매체인 TV, 신문, 잡지와 마찬가지로 WWW 광고도 객관적인 인증 데이터가 요구된다. 그러므로 독립적인 제 3의 기관에 의한 인증 데이터는 하나의 광고 매체로써 인식하게 하고 일반적으로 인정받는 데이터로써 사용될 수 있다. 따라서 인증기관은 웹사이트가 제시하는 사용자 방문 정보를 기반으로 웹사이트의 측정 과정과 그 결과를 검증하는 절차를 거쳐 정확한 데이터로써 인증하게 하므로 제 3의 인증기관의 역할은 매우 중요하며, 광고 회사의 웹사이트에서 제공되는 데이터에 대해 객관성과 신뢰성을 더해준다.

측정 방안이 동작하는 환경은 사용자의 클라이언트(C), 광고 회사의 웹 서버(S), 제 3의 인증기관(CA)으로 구성된다. 일반적으로 사용자의 클라이언트와 WWW 광고를 위한 서버 사이에 어떤 상호동작이 이루어지고, 인증기관이 이 상호동작에서 측정에 대해 책임을 가진다. 클라이언트와 서버는 서로 신뢰할 필요는 없지만 올바른 측정을 위해 인증기관은 반드시 신뢰해야만 한다. 경우에 따라서는 방문 수를 부풀리기 위해 부

정한 서버끼리 또는 부정한 서버와 부정한 클라이언트끼리 공모도 존재할 수 있다.

기본적으로 측정 시스템은 서버가 받아들이는 클라이언트의 방문 수를 측정한다. "무엇을 방문하는가"하는 것은 WWW 광고에서 쓰이는 단순한 HTML 문서이거나 동영상, 이미지, 사운드, 텍스트 등 어떠한 정보도 될 수 있다[3]. 일반적인 측정 방식의 동작은 <그림 5>와 같은 구조를 가지도록 구성된다[8][10].

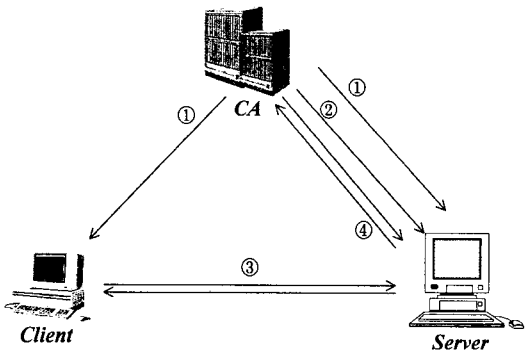


그림 5. 측정 방안의 동작 방식

① 초기화 :

$CA \rightarrow S : f_{CA1}(\alpha, S)$

$CA \rightarrow C : f_{CA1}(\alpha, C)$

시작 단계에서 단방향으로 단 한번 수행되는 과정으로 인증기관 CA는 임의의 비밀키 α를 선택하고, 각 클라이언트 C와 각 서버 S에 대해 초기화 메시지(α와 수신측 식별자의 함수)를 생성하여 안전한 채널을 통하여 전송한다. 이 메시지는 측정결과에 대한 증명에서 사용하므로 클라이언트와 서버에서 각각 비밀로 유지되어야 한다.

② 측정 시작 :

$CA \rightarrow S : h_{S,t} = f_{CA2}(\alpha, S, t)$

측정 방안의 목적은 어떤 단위 시간 t내에 각 서버를 방문하는 여러 클라이언트의 수를 측정하는 것이 목적이다. 어떤 시작 시점에서 CA는 각 S에게 challenge $h_{S,t}$를 생성하여 안전한 채널을 통하여 전송한다. 이 challenge는 서버에 대해 단위 시간을 결정하고 클라이언트로 전송하여 돌아오는 response로 측정을 증명할 때 사용하므로 역시 비밀로 유지되어야 한다.

③ 상호동작 :

$S \rightarrow C : f_S(h_{S,t}, f_{CA1}(\alpha, S), C)$

$C \rightarrow S : f_C(f_S(h_{S,t}, f_{CA1}(\alpha, S), C), f_{CA1}(\alpha, C))$

C가 S를 방문했을 때, S는 $h_{S,t}$, S의 초기화 메시지, C의 식별자를 인자로 함수값을 계산하여 C에게 전송하고, C는 받은 값과 자신의 초기화 메시지를 인자로 함수값을 계산하여 이것을 response로 S에게 전송한다. 이 response가 C의 방문에 대한 증거가 되므로 S는 잘 보관해야 한다.

④ 측정 끝 :

$CA \rightarrow S : h_{S,t} = f_{CA2}(\alpha, S, t)$

$S \rightarrow CA : f_S(f_C(f_S(h_{S,t}, f_{CA1}(\alpha, S), C), f_{CA1}(\alpha, C)), f_{CA1}(\alpha, S))$

CA는 단위 시간 t시간 후에 새로운 challenge $h_{S,t}$를 생성하여 안전한 채널을 통하여 각 S에게 전송한다. 이 때 S는 t시간 동안 각 C에서 받은 response와 자신의 초기화 메시지를 사용하여 응답함으로써 자신이 가지는 C의 방문 수를 제시한다. CA는 각 클라이언트에게 나누어준 초기화 메시지와 각 클라이언트에서 받은 서버의 response를 각각 비교함으로써 S가 주장하는 방문 수를 확인할 수 있다.

위와 같은 측정 방안이 가장 일반적인 형태인데, 여기서 사용되는 함수 f는 각 인증기관, 서버,

클라이언트에 의해 정의되는 일방향 함수이다. 각 서버에게 전송되는 challenge 메시지를 수신 측에서 직접 계산할 수 있다면 이를 생략하여 통신량을 줄일 수도 있다.

5 측정 방안

5.1 기존 방안의 고찰

3장에서 언급한 요구사항을 가능한 한 만족하도록 측정 시스템을 단순하게 구현하려면 인증기관 *CA*가 각 클라이언트에게 인증된 서명키를 미리 제공한 후 클라이언트가 서버를 방문할 때마다 서명하도록 하면, 서버는 방문의 증거로써 클라이언트가 서명한 리스트를 제시하여 인증기관이 클라이언트 서명을 확인하도록 함으로써 서버가 주장하는 방문을 증명할 수 있다. 그러나 이 시스템은 매우 정확하지만 방문했을 때 서명과 그 확인에 따르는 계산량과 메모리 사용량이 아주 비효율적이고, 서명을 통해 클라이언트의 신분이 노출될 수 있으므로 각 클라이언트의 프라이버시도 지킬 수 없다는 단점이 있다.

Franklin과 Malkhi[6]는 서명을 생성하고 확인하는 노력을 줄이기 위해 "lightweight security"만을 제공하여 간편하게 구현함으로써 정확한 방문 수를 보다 효율적으로 측정하는 방안을 제안하였다. 이 방안은 사용자 클라이언트가 서버에 접속할 때 Java 애플릿을 전송받은 후 사용자의 사용시간을 입력으로 하여 해쉬값을 반복적으로 계속해서 계산하고 그 결과를 서버로 전송하는 형태로 동작한다. 그러나 클라이언트가 Java 애플릿이 동작하는 동안 실수 또는 악의적인 목적으로 서버가 방문을 측정하는 것을 방해할 수 있고, 사용자의 사용 시간만을 입력으로 해쉬값을 계산하므로 서버가 클라이언트 방문 수를 생성시켜 부풀리는 것이 가능하기 때문에 WWW 광고에 실제 적용하기에는 다소 무리가 있다.

Shamir[1]의 k-out-of-n 비밀 분산 방안은 측정 방안을 위해 많은 요구사항을 만족시킨다. 이를 이용한 측정 방안은 인증기관이 비밀(여기서는 어떤 단위 시간당 방문 수)을 n개의 분할로 나누어 각각을 클라이언트에게 배분한 후 서버를 방문할 때마다 서버에게 자신의 분할을 전송하도록 한다. 서버는 k개의 서로 다른 분할을 얻었을 때에만 비밀을 재구성할 수 있고 이를 인증기관에게 증명할 수 있다. 만약 $k-1$개 이하의 분할을 가진다면 비밀에 대한 어떠한 정보도 서버는 알아낼 수 없다. 그러나 방문 수를 부풀리기 위해 부정한 서버와 클라이언트 사이의 공모를 염두에 둔다면 단 1회만 사용한 후 계속해서 갱신하도록 해야한다. 또한, 실수든 의도적이든 하나의 분할이라도 잘못된 경우 비밀을 복구할 수 없기 때문에 잘못되거나 부정한 분할을 서버가 미리 인식할 수 있는 방법이 요구된다.

최근 전자상거래가 부상함에 따라 온라인 출판, 온라인 정보검색, 온라인 데이터베이스 서비스 등에 "micropayment"가 새로운 지불방식으로 등장하고 있는데[11], 상업적인 온라인 서비스를 위한 대안이고 작업량보다 오버헤드를 줄이기 위해 매우 효율적으로 설계되었다. WWW 광고에 적용하기 위해 이것을 변형하여 방문 수 측정에 사용할 수 있는데, 방문시 클라이언트가 서버에게 자신의 "money"를 전송하고 서버는 이들 합계를 은행에 다시 전송한다. 은행은 서버가 보내온 합계가 각 클라이언트에게 발행한 money의 합계와 서로 일치함을 확인함으로써 서버가 주장하는 방문 수를 확인하는 방식이다. micropayment를 기반하는 모든 측정 방안은 서버가 받았던 순서대로 money를 다시 은행(또는 *CA*)으로 전송해

야만 하지만 실제 지불 방식과는 달리 은행의 클라이언트 계좌에서 money를 공제할 필요가 없기 때문에 측정 방안에서는 보다 효율적으로 구성할 수 있는 장점이 있다.

Naor와 Pinkas[8]는 비밀 분산 방안(Secret Sharing Scheme)을 수정하여 이변수 다항식을 이용한 측정 방안을 제안하였다. 이 방안은 클라이언트 측면에서 작은 계산량만이 필요로 하는 다항식을 비밀 분산 방안에 적용하여 안전하고 효율적인 측정에 초점을 두었다. 그러나 제안 방안에서 별도로 견고성, 효율성, 익명성 등을 부가하기 위해서는 기본 방안에서 새로운 수정이 필요하므로 모든 요구사항을 만족하는 일반적인 목적의 측정보다는 각각의 요구사항이 필수적인 특수한 환경에서의 측정에 유용하다.

5.2 요구사항에 따른 확장 방안

3장에서 논의했던 측정에 있어 중요한 요구사항들을 확장할 수 있는 여러 가지 방안들을 암호 기술을 중심으로 살펴보기로 한다.

먼저 안전성 및 정확성에 있어서 측정 방안의 성질에 가장 적당한 방안이 바로 "비밀 분산 방안"이다. 서버가 방문 수를 부풀리는 것을 막아주고, 좀 더 보완하면 클라이언트의 측정 방해도 막을 수 있다. 다항식을 이용한 k-out-of-n 비밀 분산 방안은 클라이언트에 있어 계산량 및 메모리 사용량을 줄여주므로 실제 사용에 적당하다 할 수 있다. 또한, 부정한 클라이언트나 잘못된 클라이언트에 의해 하나의 분할이라도 이상이 있다면 비밀을 복구할 수 없기 때문에 이를 미리 대비하는 견고성을 보장해 주어야 하는데, 이것은 자기 인증(Self-authenticating) 코드, 증명 가능한 비밀 분산(Verifiable Secret Sharing), 법 위에서의 다항식 연산 등을 이용하여 가능하다. 또한 micropayment를 WWW 광고에 맞도록 변형하여 사용하는 방안도 고려해 볼 수 있다.

서버는 언제 얼마만큼의 클라이언트들이 방문할지 알 수 없을뿐더러 WWW 특성상 수많은 클라이언트들이 서버를 매일 방문하고 있다. 이러한 상황에서 측정 방안의 효율성을 증가시키는 방법으로는 여러 클라이언트들을 같은 성질을 가지는 몇 개의 클래스로 분할하여 클라이언트 단위로 측정하는 것이 아니라 클래스 단위로 측정함으로써 가능하다. 각 클라이언트는 자신이 어떤 클래스에 속하는지 알 수 있지만 서버는 그것을 알 수 없도록 한 상태에서 측정을 한다면 서버가 특정 클래스를 사용하여 부풀리는 것을 방지하면서 효율성을 보다 높일 수 있는 두 가지 이점이 있다.

실제 측정 과정 동안 클라이언트의 정보가 누출될 수 있는 가능성이 많으므로 클라이언트의 프라이버시를 보호하는 방법이 필요하다. 이를 위한 클라이언트에 대해 익명성을 허용하는 방법은 역을 계산하기 어려운 일방향 함수의 성질을 이용하여 서버가 어떤 특정한 방문과 그 때 방문한 클라이언트를 서로 연결시킬 수 없도록 하는 방법이 있다. 이 방법은 서로 다른 클라이언트 각각의 방문인지, 같은 클라이언트의 반복된 방문인지를 알 수 없도록 하여 클라이언트의 프라이버시를 보호할 수 있다. 그러나 인증기관은 이 사실을 모두 알 수 있으며 각 클라이언트의 방문을 서로 연결시킬 수 있다.

WWW 광고 측정에 대한 표준화는 측정 방법상의 표준화뿐만 아니라 객관적이고 신뢰성 있는 WWW 광고 효과를 산출하도록 해주기 때문에 광고주와 광고회사를 끌어 모을 수 있도록 하므로 해외에서는 이미 많은 노력과 투자가 이루어지고 있다. 특히 미국에서는 여러 인터넷 광고 회사를 중심

으로 구성된 컨소시움인 IAB(Internet Advertising Bureau)[5]와 AAAA(American Association of Advertising Agencies)[2]를 중심으로 구체적인 표준화 사례가 나오고 있는 실정이다.

6. 끝내며

인터넷 환경에서 최근 상업적인 목적으로 가장 각광 받고 있는 분야는 바로 WWW 광고이다. 그러나 현재의 WWW 광고는 정확하고 안전한 측정 방법의 부재로 인해 그 인기도라든지 사용량을 단지 히트 수 및 클릭 수만으로 측정하고 있어 그 측정 결과를 보편적으로 판단하기 어렵다. 이를 해결하기 위한 몇몇 방안들이 제안되어 왔지만 측정 과정에서 있어 요구사항을 모두 만족하지는 못하고 있다. 본 고에서는 안전하고 효율적인 측정 방안을 구현하기 위하여 필수적인 보안성, 정확성, 효율성, 익명성, 이동성, 표준화 등에 대하여 논의하였다. 그리고, 일반적으로 구현되는 웹 측정 시스템에서 클라이언트, 서버, 인증기관에서의 상호동작을 살펴보고, 필수적인 요구사항을 만족시키기 위한 여러 방안을 살펴보았다.

이러한 측정 방안은 인터넷 및 WWW 환경에서의 보편적인 광고를 위한 시스템에 적용할 수 있으며, 특히 암호 기술과 결합하여 보다 안전하고 보다 견고하게 설계된다면 WWW 광고 측정을 위한 한 분야로써 자리잡게 될 것이다. 특히, 광고주 입장에서는 신뢰성 있는 측정 자료를 바탕으로 광고비를 책정할 수 있게 되고 이동성을 이용하여 사용자 집단의 특성, 취향 등을 파악하여 서비스의 차별화를 꾀할 수 있고, 사용자들은 익명성을 통하여 개인의 프라이버시를 보호받으며 안전한 양질의 서비스를 제공받을 수 있을 거라 예상된다.

WWW 광고를 위해 적용되는 여러 가지 방안들은 WWW 광고를 전통적인 광고와 마찬가지로 인식하도록 해주는 것은 물론 WWW의 특성을 이용하여 능동적인 사용자의 참여를 유도하는 새로운 광고 매체로서의 가능성을 보여주고 있다. 이를 이용하여 일반적인 WWW 광고 시스템뿐만 아니라 네트워크 가입자를 위한 한정 광고 시스템, 특정 라이선스에 따르는 소프트웨어나 정보 서비스 등의 응용 분야에 활용할 수 있고, 또한 보안 단계에 따른 계층적인 키분배 방안, 저작권 보호를 위한 디지털 워터마킹 기술들과 결합한다면 이를 응용한 새로운 활용 분야도 등장할 수 있을 것으로 예상된다.

참 고 문 헌

[1] A.Shamir, "How to share a secret", Comm. ACM vol.22 no.11, pp.612-613, 1979

[2] AAAA(American Association of Advertising Agencies), "http://www.commercepark.com/AAAA/", 1998

[3] Chatterjee, Patrali, "Modeling Consumer Network Navigation in World Wide Web Sites: Implications for Advertising," Dissertation proposal, Owen Graduate School of Management, Vanderbilt University, 1996

[4] CyberAtlas, "http://www.cyberatlas.com", 1996

[5] IAB, "http://www.iab.net", 1998

[6] M.K.Franklin and D.Malkhi, "Auditable metering with lightweight security", Financial Cryptography '97, 1997

[7] M.Kinsman, "Web advertising 1997 : market analysis and forecast", Cowles/Simba Information, Stanford, Connecticut, May 1997

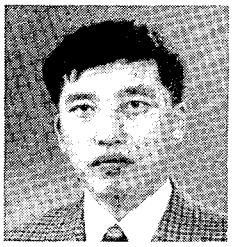
[8] M.Naor and B.Pinkas, "Secure and Efficient Metering", EuroCrypt '98, 1998

[9] T.Novak and D.Hoffman, "New metrics for web media: toward the development of web

measurement standards", http://www2000.ogsm.vanderilt.edu/novak/web.standards/webstand.html

[10] 신원, 이경현, "WWW 환경에서의 안전한 측정 방안", 한국정보처리학회 '98 추계학술발표논문집, pp.757-760, 1998

[11] 한국전산원, "전자 상거래 환경을 위한 기술 조사 연구", http://ncalib.nca.or.kr/HTML/1996/96070/96070. htm

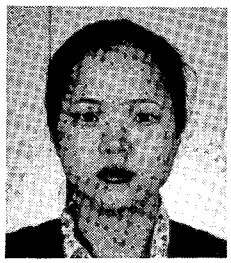


이 경 현

- 1982년 경북대학교 사범대학 수학교육과 졸업(이학사)
- 1985년 한국과학기술원 응용수학과 졸업(이학석사)
- 1992년 한국과학기술원 수학과 졸업(이학박사)
- 1985년 2월~1993년 2월 한국 전자 통신 연구소 연구원, 선임 연구원
- 1993년 3월~현재 부경대학교(구 부산수산대학교) 전임강사, 조교수
- 1995년 7월~1996년 7월 Univ. of Adelaide, 응용수학과, Australia 방문교수
- 관심분야 : 정보보안, 멀티미디어 통신 및 성능분석, 암호이론, 재시도 대기체계론

신 원

- 1996년 부산수산대학교(현 부경대학교) 전자계산학과 졸업(이학사)
- 1998년 부경대학교 전자계산학과 대학원 졸업(이학석사)
- 1998년~현재 부경대학교 전자계산학과 박사과정
- 관심분야 : 정보보안, 멀티미디어 통신 및 성능 분석, 암호이론, 재시도 대기체계론



신 정 화

- 1997년 한국방송대학교 전자계산학과 졸업(이학사)
- 1998년~현재 부경대학교 전산정보학과 석사과정
- 관심분야 : 정보보안, 멀티미디어 통신, 암호이론