이동 환경에서 인증된 사용자에게 선별적으로 데이터를 전송하는 브로드캐스팅 기법의 성능분석

임성화* 정승식** 김재훈*
*아주대학교 정보통신전문대학원
**Xapi 소프트웨어
e-mail : {holyfire, blueogre, jaikim}@ajou.ac.kr

Performance Analysis of Broadcasting Protocol Sending Information only to Authenticated Clients in Mobile Environment

Sung-Hwa Lim* Seunsik Jung** Jai-Hoon Kim*
*Graduate School of Information and Comminication, Ajou University
**Xapi Software

요 약

단말기의 컴퓨팅 능력과 이동 통신 기술이 발달함에 따라, 무선 이동망에서도 현재의 데스크탑에 버금가는 인터넷 컴퓨팅이 가능해 지고 있다. 브로드캐스팅(broadcasting)은 비대칭 통신 환경에서 정보를 효과적으로 전달하는 방법이다. 다수의 사용자가 요구하는 동일한 종류의 실시간 데이타를 전송할 경우, 무선 환경에서는 브로드캐스트 기법이 효과적이다. 그러나 유료 정보를 무선 망에 브로드캐스트 할 경우 허가되지 않은 사용자들도 해당 정보를 이용할 수 있는 문제가 발생한다. 그러므로 이 경우 기존의 브로드캐스트 기법을 사용하는 대신, 1:1 전송 방식 또는 멀티캐스트 방식을 사용해야 한다. 그러나 사용자의 수가 많을 경우와 전송할 데이터의 크기가 커질 경우 기존의 방식들은 통신 오버헤드를 증가시킬 수 있다. 그러므로 사용자가 많고 전송할 데이터가 큰 경우 효율적인 통신을 위해서는 특정 사용자들에게 선별적 전송이 가능한 브로드캐스트 기법이 필요하다. 본 논문에서는 공개키 암호화 기술을 사용하여 정보를 허가된 사용자에게만 전송하는 브로드캐스트 기법을 제안하고 그 성능을 분석한다.

1. 서론

이동컴퓨팅의 응용중 정보 송신측(위성 또는 기지국)으로부터 정보 수신측 (이동 컴퓨터 이용자들) 방향(downstream)의 통신량이 많고 반대 방향 (upstream)으로의 통신량은 상대적으로 적은 비대칭 통신 환경에서는 브로드캐스팅(broadcasting)이 정보를 효과적으로 전달하는 방법이 된다. 브로드캐스팅은 많은 사용자들이 공동으로 필요로 하는 정보를 동시에 전송할 수 있는 장점을 갖는다[3,9]. 무선망에서의 모든 통신은 브로드캐스트 기반으로 이루어 진다. 예를 들어 셀룰라 망에서 기지국과 이동 호스트간의 1:1 통신이 이루어질 때, 기지국은 이동 호스트으로의 전송을 위해 자신의 셀 지역으로 전송할 데이터를 브로드캐스트한다. 그러므로, 무선 망에서 브로드캐스트 기법을 적용할 경우 유선 망에서 보다 적은 대역폭 사용 오버헤드로 다수의 클라이언트에게 데이터를 전송할 수 있다. 현재는 이동 컴퓨팅 환경에서의 유료 컨텐트 서비스가 급증하고 있다. 사용자가 필요로 하는 정보를 가입된 사용자에게만 제공하는 서비스가 정보 제공 업체(ISP)들에 의해서 제공되고 있다. 단말기의 컴퓨팅 능력과 이동 통신 기술이 발달함에 따라, 무선 이동망에서도 현재의 데스크탑에 버금가는 인터넷 컴퓨팅이 가능해 질 전망이다. 다수의 사용자가 요구하는 동일한 종류의 실시간 데이타를 전송할 경우, 무선 환경에서는 브로드캐스트 기법이 효과적이다. 그러나 유료 정보를 무선 망에 브로드캐스트 할 경우 허가되지 않은 사용자들도 해당 정보를 이용할 수 있는 문제가 발생한다. 그러므로 이 경우 기존의 브로드캐스트 기법을 사용하는 대신, 1:1 전송 방식 또는 멀티캐스트 방식을 사용해야 한다. 그러나 사용자의 수가 많을 경우와 전송할 데이터의 크기가 커질 경우. 기존의 방식(1:1 전송)들은 통신 오버헤드를 증가시킬 수 있다. 또한 멀티캐스트의 경우 시스템 차원에서의 지원이 필요하다. 그러므로 사용자가 많고 전송할 데이터가 큰 경우의 효율적인 통신을 위해서는, 특정 사용자들에게 선별적 전송이 가능한 브로드캐스트 기법이 필요하다. 본 논문에서는 공개키 암호화 기술을 사용하여 정보를 허가된 사용자에게만 전

송하는 브로드캐스트 기법을 제안하고, 그 성능을 분석한다.

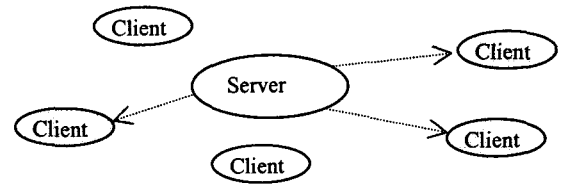
2. 관련연구

데이터 통신은 크게 유니캐스트, 브로드캐스트, 멀티캐스트 방식으로 나눌 수 있는데, 유선망에서 주로 사용되는 방식은 유니캐스트 방식을 사용하여 1:1 방식으로 데이터를 전송한다. 유니캐스트 방식은 목적지와 1:1 로 연결하여 데이터를 보내는 방식으로 전통적인 인터넷 기반의 데이터 전송 방식이다. 결과적으로 클라이언트의 수가 많아지면 동일한 정보를 동시에 전송하는 경우에도 개별적으로 서로 연결해야 하므로, 전송데이터의 중복으로 인한 사용량 증가로 네트워크상의 대역폭의 낭비를 초래하며, 네트워크에 혼잡이 발생할 우려가 있다. 멀티캐스트 방식은 송신자가 해당 데이터를 받기를 원하는 수신자들에게만 전달하는 방법으로, 데이터 송신자는 멀티캐스트 그룹으로 데이터를 보내면 받는 그룹에 포함된 호스트들에게만 데이터가 전송되는 방식을 취한다[4,5] 브로드캐스트 방식은 하나의 송신자가 네크워크의 모든 수신자들에게 데이터를 전송하는 방식으로 전송자는 하나의 데이터만 보내면 수신자들이 데이터를 받아볼 수 있는 방식이다. 따라서 유니캐스트와 비교하여 네크워크의 혼잡을 줄이거나 이용율을 높일 수 있지만 받기를 원하지 않는 호스트들도 데이터를 받게 된다.

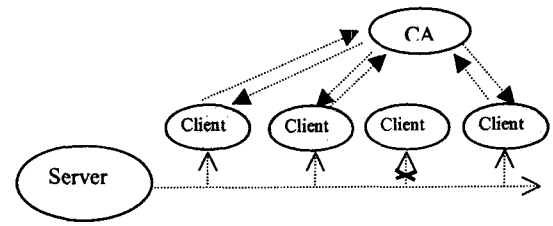
이동 컴퓨팅 환경에서는 단말기를 휴대할 수 있으므로 유선환경에 비해 파손이나 분실에 따른 물리적 보안 취약점을 갖는다. 이동 컴퓨팅 환경에서의 보안을 위해 RSA SecureID 나 RSA BSAFE 등의 상용 소프트웨어 솔루션들이 현재 제공되며, 최근에는 스마트 카드 등의 하드웨어 제품의 사용도 증가하고 있다. 많은 공개키 암호알고리즘이 제안되었으나 안전도 또는 실용적 측면에서 문제점이 야기되었으며 1978 년 소인수분해의 어려움에 기반을 둔 RSA 가 소개되어 지금까지 넓게 사용되고 있다.

3. 제안 브로드캐스팅 프로토콜

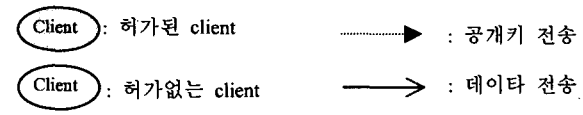
무선환경에서 허가된 클라이언트에게만 데이터를 전송할 경우, 1:1 로 전송하는 것이 가장 안정적이다. 그러나 주가, 날씨, 스포츠중계와 같은 실시간 데이터들은 다수의 클라이언트가 공통적으로 요구하는 정보이다. 이동 컴퓨팅이 발달함에 따라 가까운 미래에는 무선망에서 동영상을 통한 스포츠 중계와 같은 용량이 큰 데이터를 실시간으로 여러 명의 사용자들에게 동시에 전송하는 서비스가 예상된다. 이렇게 용량이 큰 정보를 다수의 클라이언트들에게 전송하는 경우 브로드캐스트 기법이 효과적이다[1,2]. 그러나 유료 컨텐트의 경우 사용료을 지불한 허가된 클라이언트들에게만 정보를 전달해야 하므로 일반적인 브로드캐스트 기법은 사용할 수 없다. 만약 유료 정보를 브로드캐스트 할 경우 허가되지 않은 클라이언트도 억세스가 가능할 수 있기 때문이다. 그러므로 유료 컨텐트의 선별적 전송을 위해서는 다수의 클라이언트가 요구하는 실시간 데이터라 하더라도 1:1 로 전달할 수 밖에 없다. 그러나 1:1 전송의 경우 클라이언트가 증가함에 따라 연결의 수가 증가하므로 통신 오버헤드가 증가한다. 또한 전송할 데이터의 크기가 증가할 경우의 통신 비용은 급수로 증가하게 된다. 또 다른 방법으로는 전송하는 데이터에 허가된 클라이언트의 목록을 실어서 멀티캐스트 하는 방법이 있으나 전송할 클라이언트의 수가 많아지면 클라이언트 정보 목록의 추가로 인해 데이터의 크기가 증가하는 단점이 있다. 본 논문에서 제안하는 기법은 유료 컨텐트 정보를 서버의 Private Key 로 암호화하여 브로드캐스트 하고, 허가된 클라이언트들은 브로드캐스트되는 정보를 읽은 후 인증된 클라이언트들만 CA 에서 서버의 공개키를 받아서, 받은 공개키를 이용하여 복호화해서 사용하는 방식이다. 공개키를 얻어야 수신한 정보를 복호화 할 수 있으므로 허가되지 않은 클라이언트는 CA 에서 서버의 공개를 주지 않기 때문에 브로드캐스트 되는 정보를 수신하여도 사용할 수 없다. 그러므로 본 논문의 브로드캐스트 기법을 적용할 경우 선별적인 데이터 전송이 가능하면서도 브로드캐스팅을 통해서 통신 비용의 절감을 예상할 수 있다. [그림 1]은 무선환경에서 허가된 클라이언트에 대한 실시간 정보를 전달하는 기법들 중 1:1 전송기법과 본 논문에서 제안하는 선별적 브로드캐스트 기법을 설명한다. [그림 2]는 본 논문에서 제안하는 공개키 기반의 선별적 브로드캐스트 알고리즘을 나타낸다.



(a) 1:1 전송 기법



(b) 공개키 기반의 선별적 브로드캐스트 기법

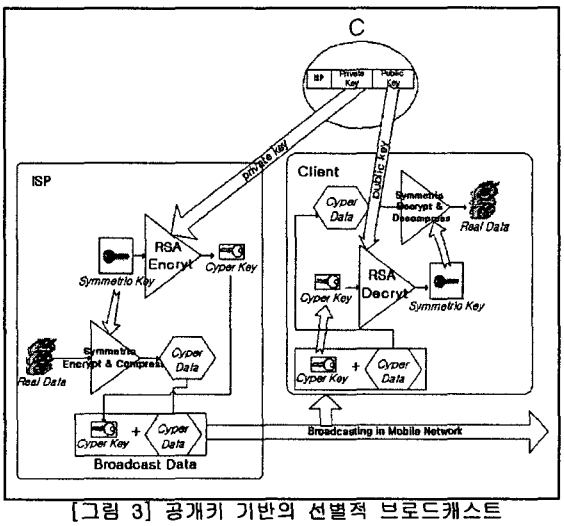


[그림1] 1:1 전송 기법과 제안된 브로드캐스트 기법

Step 1. 정보 제공자(ISP)는 CA 로부터 얻은 PrivateKey 를 사용하여, 다수의 클라이언트가 요구하는 실시간 데이터를 선정 후 암호화한다.
Step 2. ISP 는 암호화된 실시간 데이터를 무선 망을 통해 브로드캐스트 한다.
Step 3. ISP 에 가입한 클라이언트들은 브로드캐스트되는 데이터 중, step2 에서 브로드캐스트 된 데이터를 읽어 들인다. (가입되지 않은 클라이언트들도 브로드캐스트 된 데이터를 전송 받을 수 있다.)
Step 4. Step3 의 클라이언트는 CA 와의 연결을 개설하고 통신을 하여 ISP 의 공개키를 얻어온다.
Step 5. Step4 에서 얻은 공개키를 이용해 클라이언트는 해당 데이터를 복호화 한다.

[그림 2] 공개키 기반의 선별적 브로드캐스트 알고리즘

[그림3]는 [그림2]에서 설명한 알고리즘을 확장해서 전송자와 수신자가 세부적으로 데이터를 주고 받는 것을 나타내었다. RSA 기반의 알고리즘은 암/복호화에 많은 컴퓨팅이 필요하다. 암호화는 전송자가 한번만 수행하면 되므로 커다란 오버헤드는 없지만 수신측인 클라이언트 쪽에서 받은 데이터의 전체를 RSA 알고리즘을 통해서 복호화 하는 것은 매우 어려운 일이다. 따라서 [그림3]에서와 같이 실제 데이터에 대한 암호화 및 압축은 대칭키 방식을 사용하고 이때 사용된 키를 RSA 방식을 통해서 암호화 하여 단일키 방식으로 암호화/압축된 데이터와 함께 전송한다. 수신자측에서는 우선 RSA기반으로 암호화 된 키를 CA로부터 받은 전송자의 공개키로 복호화하여 키를 얻고, 그 키를 이용해서 단일키 방식으로 암호화/압축된 데이터를 복호화하는 방식을 취하면 클라이언트에 많은 오버헤드 없이 복호화가 가능하다.



[그림 3] 공개키 기반의 선별적 브로드캐스트

$$C_{p\_to\_p} = n \times Data$$

$$C_{bcast} = n \times (2C_{pk}) + \left[\left\lceil \frac{Data}{block} \right\rceil \times \alpha \right] \times block$$

n : 이동 클라이언트의 수
Data : 전송받을 데이터의 전체 크기
Block: 전송 받을 데이터의 블록 개수
C_{pk} : CA와 통신하여 공개키를 가져오는 비용
α : 복호화에 따른 오버헤드

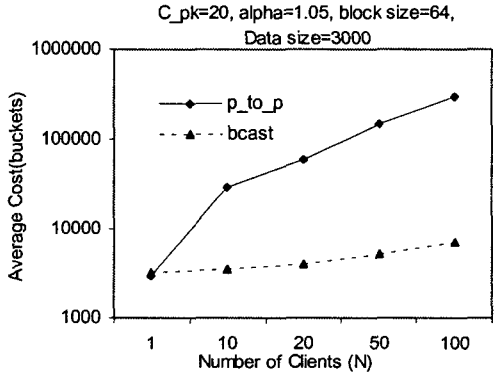
[그림 4] 각 기법에 따른 평균 통신비용

[그림 4]는 n명의 허가된 클라이언트의 수에게 같은 종류의 실시간 데이터를 전송하는 경우 1:1 전송기법과 제안된 브로드캐스트 기법에 따른 평균 통신비용을 나타내고 있다. $C_{p\_to\_p}$ 는 1:1전송에서의 평균 비용, 그리고 C_{bcast}는 본 논문에서 제안하는 브로드캐스트 기법의 평균비용을 나타내었다. 1:1전송의 경우 클라이언트의 수에 따라 각각 전송이 이루어져야 하므로, 통신비용은 데이터와 클라이언트 수의 곱으로 나타낼 수 있다. 브로드캐스트의 경우 클라이언트가 CA를 통한 인증작업을 통하여 공개키를 받아야 하므로 $2*C_{pk}$의 추가 비용이 추가되며, 암호화된 정보를 공개키를 이용하여 복호화해야 하는 오버헤드 α 가 추가되지만, 전송할 데이터의 양은 클라이언트의 수에 영향을 상대적으로 작게 받는다.

4. 시스템 모델링 및 성능분석

성능분석을 위한 Assumption 및 시스템 파라메터는 다음과 같다.

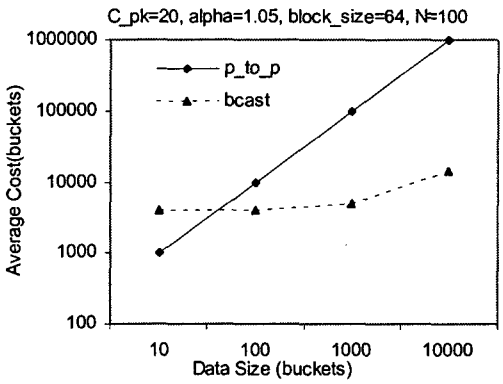
- 특정 시스템에서 독립적으로 적용하기 위하여, 데이터 크기의 단위는 버켓이라는 단위 길이로 가정한다. 평균 비용의 단위도 버켓으로 가정한다.
- 하나의 데이터는 여러 개의 블록으로 나누어져 브로드캐스트 되며, 블록은 고정길이를 갖으며 하나의 블록 내에 남은 공간이 발생할 경우 패딩을 통해 길이를 맞춘다.
- 클라이언트가 공개키를 얻기 위해 CA와 통신하여 공개키를 얻는 비용은 2 * C_{pk}로 가정하며, 복호화 오버헤드는 α 로 가정한다.
- 통신 비용은 데이터의 길이만큼 전송 또는 수신하는 비용이며, 무선환경에서의 경우만 고려한다.
- 통신 비용은 무선환경에서 전송되는 데이터 양만을 고려한다.
- 통신 비용은 클라이언트가 데이터를 받거나 보내는 경우 만을 고려한다.



[그림 5] 클라이언트 수(N)에 따른 각 기법의 평균 비용

[그림 5]은 클라이언트의 수(N)에 따른 1:1기법과 제안된 브로드캐스트 기법의 평균 통신 비용을 나타낸다. 클라이언트가 CA를 통해 공개키를 얻는 비용과 한 블록의 크기의 비율, 그리고 전송할 실시간 데이터의 전체 크기의 비율을 20:1:64:3000으로 가정하였다. 결과에서 볼 수 있듯이, 클라이언트의 수가 적은 경우(n=1)는 1:1 방식의 성능이 우수하나, 클라이언트의 수가 증가함에 따라 제안된 브로드캐스트 기법이 적은 비용을 나타내었다. 제안된 브로드캐스트 기법의 경우 공개키를 얻는 과정에서의 오버헤드 때문에 클라이언트의 수가 적은 경우에도 일정량이상의 비용이 소요되나, 클라이언트의 수가 증감함에 따른 비용의 증가가 선형에 가까우므로, 클라이언트가 많은 환경에서는 가장 좋은 성능을 나타내었다. [그림 6]은 클라이언트의 수가 일정

한 환경에서 전송할 실시간 데이터의 크기가 변할 때에 각 기법의 평균 비용을 나타내었다. 역시 데이터의 크기가 작은 경우에는 공개키를 습득하는 프로세스의 오버헤드의 비율이 상대적으로 커짐으로 다른 기법에 비해 제안 브로드캐스트 기법은 높은 비용을 나타내었다. 그러나 데이터의 크기가 커져도 공개키를 습득하는 프로세스의 오버헤드의 양은 일정하므로, 제안 브로드캐스트 기법은 1:1 통신 기법보다 적은 비용을 소요한다. 전송하는 데이터가 스포츠 중계 동영상과 같은 대용량 멀티미디어 데이타일 경우 제안 브로드캐스트 알고리즘이 높은 성능을 나타낼 것으로 예상된다.



[그림 6] DataSize에 따른 각 기법의 평균 비용

5. 결론 및 향후과제

다수의 사용자가 요구하는 동일한 종류의 실시간 데이타를 전송할 경우, 무선 환경에서는 브로드캐스트 기법이 효과적이다. 그러나 사용자가 필요로 하는 정보를 가입된 사용자에게만 제공하는 유료 컨텐츠 데이터 서비스에서는, 무선 망에 유료데이터를 브로드캐스트 할 경우 허가되지 않은 사용자들도 해당 정보를 이용할 수 있는 문제가 발생한다. 그러므로 이 경우 기존의 브로드캐스트 기법을 사용하는 대신, 1:1 전송 방식 또는 멀티캐스트 방식을 사용해야 하지만 사용자의 수가 많을 경우와 전송할 데이터의 크기가 커질 경우 기존의 방식들은 통신 오버헤드를 증가시킬 수 있다. 사용자의 수와 데이터의 용량이 큰 상황에서의 효율적인 데이터 전송을 위하여, 본 논문에서는 공개키 기반의 암/복호화 기술을 이용하여 특정 사용자들이 선별적 데이터 접근이 가능한 브로드캐스트 기법을 제안하고 성능을 분석하였다. 사용자의 수가 많고, 전송할 데이터의 용량이 큰 경우 본 논문에서 제안한 브로드캐스트 기법의 성능이 높음이 나타났다. 특히 향후 스포츠 중계와 같은 데이터의 용량이 큰 멀티미디어 서비스가 많이 제공될 것으로 예상되므로, 본 논문의 제안 브로드캐스트 기법을 적용하였을 때, 많은 효과가 예상된다. 또한 공개키 기반의 암/복호화 알고리즘을 사용하므로, 높은 수준의 보안성을 제공한다.

향후 연구 과제로는 실제 환경의 고려를 위하여 특정 무선 통신망에 접목시켜 이동 컴퓨팅 환경의 응용에 이용할 수 있도록 연구할 예정이다.

참고문헌

[1] T. imielinski, S. Viswanathan, B.R. Badrinath, "Energy efficient indexing on air," ACM SIGMOD 94-5/94 Minneapolis, Minnesota, USA, pp 25-36. 1994.

[2] E. Pitoura, G. Samaras, "Data management for mobile computing," Kluwer Academic Publishers, 1998.

[3] S. Hameed and N. H. Vaidya, " Efficient Algorithms for Scheduling Data Broadcast, " ACM/Baltzer Wireless Networks (WINET), May 1999.

[4] Zimmermann, Phillip, "A Proposed Standard Format for RSA Cryptosystems," Advances in Computer Security, Vol III, edited by Rein Turn, Artech House, 1988

[5] Charles P. Pfleeger, "Security in Computing," second edition, published by Prentice Hall PTR, 1997, pp 91-96.

[6] http://www.rsa.com/solutions/wireless/

[7] M. Satyanarauanan, "Fundamental challenges of mobile computing," ACM Symposium on Principles of Distributed Computing, 1995 (PODC'95 invited lecture).

[8] G. H. Forman and J. Zahorjan, "The Challenges of Mobile Computing," IEEE Computer, V 27, N 4, April 1994, pp. 38-47.

[9] M. Franklin, S. Zdonik, "A Framework for Scalable Dissemination-Based Systems," University of Maryland.

[10] 원유헌,"이동컴퓨팅 보안기술," 정보과학회지, 제18권 제1호, 2000년.

[11] C. Cordeiro, D. Sadok and J. Kelner, "Establishing a Trade-Off between Unicast and Multicast Retransmission Modes for Reliable Multicast Protocol," Proc. 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 1999.

[12] D. Waitzman et al, "Distance Vector Multicast Routing Protocol," RFC1075, Nov. 1988.

[13] A. Ballardie, "Core Based Trees Multicast Routing Architecture," IETF RFC2201, Sept. 1997.

[14] J. Moy, "Multicast Extensions to OSPF," IETF RFC 1584, Mar. 1994.

[15] D. Estrin et al, "Protocol Independent Multicast Sparse Mode(PIM-SM):Protocol Specification," IETF RFC 2117, June 1997.

[16] S. Deering, "Host Extensions for IP Multicasting." IETF RFC 1112, August 1989.

[17] B. On and M. Park, "A Reliable Multicast Protocol in Networks with Mobile Hosts," Proc. The International Symposium on Distributed Objects and Applications, 1999.