(t, n) 쓰레시홀드 크립토그래피를 이용한 안전한 멀티캐스트 방안

조성호[0] 김종권
서울대학교 컴퓨터공학부
{shcho, ckim}@popeye.snu.ac.kr

Secure Multicast with the (t, n) Threshold Cryptography

Seongho Cho[0] Chong-kwon Kim
School of Computer Science and Engineering, Seoul National University

요 약

멀티캐스트는 수신자 그룹이 명확하지 않고 데이터 전송 중에 수신자가 그룹에 가입하고 탈퇴하는 것이 가능하다. 수신자가 그룹에 가입하고 탈퇴할 때마다 멀티캐스트 그룹의 키를 바꿔야 할 필요가 생기게 되는데, 이 때 키를 효율적으로 바꾸기 위한 멀티캐스트 구조로써 (t, n) 쓰레시홀드 크립토그래피를 응용한 구조를 제안한다. 이 경우 서브그룹을 관리하는 서버가 없이도 수신자 그룹에 의해서 안전한 멀티캐스트를 할 수 있다.

1. 서론

인터넷이 널리 보급됨에 따라서 인터넷을 이용한 응용프로그램들이 많이 사용되고 있다. 그런 응용프로그램들 중에는 하나의 데이터를 여러 사용자가 공유하게 되는 멀티캐스트를 필요로 하는 경우가 있다. 예를 들어 화상 회의, 분산처리용 응용프로그램, 데이터 캐스팅과 같은 것이 그런 예이다. 이런 응용프로그램들은 송신자가 데이터를 한 번 전송하더라도 네트워크를 통해서 그 데이터가 복제되어 모든 수신자가 데이터를 받음으로써 각각의 수신자에 대한 유니캐스트에 통한 네트워크의 부하와 서버의 부하를 줄임으로써 전체적인 성능 향상을 꾀할 수 있다.

이러한 멀티캐스트에서도 보안 문제를 해결할 필요가 생기게 되었다. 제한된 그룹의 사용자에게만 데이터를 전달하고 그 외의 사용자는 데이터가 무엇인지 알 수 없도록 하는 응용이 그런 예이다. 가령 인터넷을 통한 재판, 한정된 그룹에 대한 데이터 전송, 지적재산권 보호와 같은 목적을 위한 응용프로그램들은 보안을 필요로 하게 된다. 그러나 유니캐스트와 다르게 멀티캐스트 환경은 수신자가 불명확하기 때문에 보안 문제를 해결하는 것이 어렵다. 또한 멀티캐스트는 사용자가 데이터 전송 중에 그룹에 참가하고 탈퇴하는 것이 자유롭기 때문에 사용자의 수가 증가함에 따라서 안전한 멀티캐스트를 위한 효율적인 방법들이 필요로 하게 된다.

본 연구는 한국과학재단 특정기초연구(KI.06852) 지원으로 수행되었음

우리는 이 논문에서 멀티캐스트에서 보안에 대한 요구사항들을 분석하고 그에 대한 기존의 연구들을 살펴 보기로 한다. 그리고 수신자의 동적인 참가와 탈퇴에 따른 안전한 멀티캐스트의 효율적인 구조를 (t, n) 쓰레시홀드 크립토그래피[8, 9, 10, 11, 12] 를 이용하여 제안하고자 한다. 이 방법을 통해서 우리는 기존의 Iolus[2] 방법에서 제안한 계층적인 구조에 비교하여 서브 그룹을 관리하는 서버가 없고 수신자 그룹에 의해서 수신자의 참가와 탈퇴가 가능한 구조를 제안하고자 한다.

2. 멀티캐스트를 위한 보안 요구사항

양단 간의 데이터 전송과는 다르게 멀티캐스트에서는 보안과 관련된 요구사항이 응용에 따라 달라질 수 있다[1]. 데이터 방송과 같이 한 개의 송신자 혹은 소수의 송신자가 불특정한 다수의 수신자에게 데이터를 전송하는 경우를 1 대 n 멀티캐스트라고 하고, 화상회의와 같이 소수의 노드가 그룹에 참여하여 데이터를 서로 주고 받은 경우를 m 대 n 멀티캐스트라고 한다. 각각의 경우에 따라서 인증(Authentication)과 보안 정도에 대한 요구사항이 서로 다르다. 하지만 공통적으로 이루어져야 하는 보안 요구사항에 대해서 살펴 보면 다음과 같다.

인증(Authentication)은 데이터를 전송받은 것이 원래 받아야 하는 데이터와 같고, 데이터를 보낸 송신자가 수신자가 송신을 받아야 하는 노드인지 확인할 수 있어야 하는 것을 의미한다. 무결성(Integrity)은 송신자로부터 수신자

에게 전송되는 과정에서 데이터가 변경되거나 손실되지 않고 전송되는 것을 확인할 수 있는 것을 의미한다. 기밀성(Confidentiality)은 데이터를 받을 수 있는 수신자만 데이터의 내용을 알 수 있고, 그렇지 않은 그 외의 수신자는 데이터의 내용을 알 수 없는 것을 의미한다.
인증은 MAC(Message Authentication Code) 나 전자서명(Digitial Signature) 과 같은 방법을 이용하여 송신자의 인증을 처리할 수 있다. 무결성은 데이터에 대한 해쉬 함수를 이용한 다이제스트(Digest)를 이용하여 데이터가 전송되는 과정에서 변하지 않았다는 것을 보장할 수 있다. 기밀성은 암호화 기법을 이용하여 송신자와 수신자만 알고 있는 키를 이용하여 데이터를 받을 수 있는 수신자만 데이터를 받고 그렇지 않은 수신자는 데이터를 받을 수 없고, 또 그 내용을 알 수 없는 것을 보장할 수 있다.

3. 관련연구

멀티캐스트와 관련된 보안과 관련된 연구는 송신자의 인증, 수신자의 그룹에 참가와 탈퇴를 효율적으로 처리하기 위한 멀티캐스트 구조, 그에 따른 효율적인 키 분배 방법을 들 수 있다. 이와 관련된 연구들로는 효율적인 멀티캐스트 구조를 위해서는 Mittra 가 제안한 Iolus[2]와 Nortel이 제안한 방법이 있고 멀티캐스트 보안 정책에 대한 설정 등을 고려한 구조로서 Honeyman 등이 제안한 Antigone [3]등이 있다.

4. (t, n) 쓰레시홀드 크립토그래피

4.1 쓰레시홀드 크립토시스템

Shamir[7]가 비밀 공유 기법을 제안한 이후, 쓰레시홀드 크립토시스템은 발전하였다. 쓰레시홀드 크립토시스템은 공개키와 비밀키 쌍을 이용하는데, 공개키는 한 개만 존재하는 반면에 비밀키는 n개의 노드로 이루어진 그룹에 의해 비밀 정보가 일부분씩 공유된다. 비밀키는 쓰레시홀드값 t 이하의 노드는 원문을 복구해 내지 못하고 t+1 이상의 노드가 모여야만 비밀키를 얻어낼 수 있는 크립토시스템이다.
이 시스템에서는 송신자가 메시지를 수신자에게 전송하고자 하는 경우, n group 의 공개키를 가지고 원문을 암호화하여 전송한다. 수신자는 각자가 가지고 있는 비밀 정보를 믿을 수 있는 노드(trusted party)에게 안전한 채널을 통해 전송한다. 트러스티드 파티는 t+1 이상의 비밀 정보를 모아서 비밀키를 만들어낸 다음에 원문을 구하여 각각의 수진자에게 데이터를 전송한다.

4.2 제 삼자가 없는 쓰레시홀드 크립토시스템

위에서는 믿을 수 있는 제 3의 노드가 있어야만 암호화된 데이터의 원문을 구해낼 수 있었다. Pedersen은 이런 단점을 보안하여 트러스티드 파티가 없는 (t, n) 쓰레시홀드 크립토시스템[8]을 제안하였다.

5 . 키 분배 방법

5.1 키 생성 프로토콜

하나의 수신자 그룹에 속해 있는 각각의 수신자는 임의의 비밀정보 $x_i \in Z_q$를 생성하고 이와 동시에 임의의 문자열 r_i를 생성한다. 그리고 r_i에서 $C(r_i, x_i) \in \{0, 1\}$를 생성하고 $h_i = g^{x_i}$를 생성하여 브로드캐스트한다. 이 때 대표 수신자는 Πh_i를 구하여 그룹에 대한 공개키를 생성한다.
여기서 각각의 수신자는 자신이 생성한 비밀정보 x_i와 r_i를 새로 생성하기만 하면 그룹에 대해서 새로운 키를 생성할 수 있다.
멀티캐스트가 이루어질 때 원문을 얻어 내기 위한 비밀키 생성 프로토콜은 각각의 사용자는 다음과 같은 임의의 t+1 차 방정식을 만든다.

$$f_i(z) = f_{i0} + f_{i1}Z + \cdots + f_{ik-1}z^{k-1} \bmod , \ f_{i0} = x_i$$

생성된 $f_i(z)$로부터 $f_i(j) = s_{ij}$를 생성하여 각각의 j 노드에게 안전한 채널을 통한 유니캐스트를 한다. 각 수신자는 $s_i = \Sigma s_{ji}$를 구하여 $x = \Sigma s_i$인 비밀키를 생성한다.

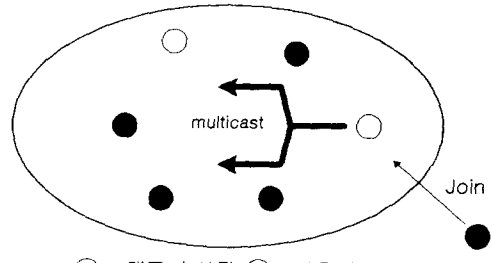

그림 1 그룹 참가 시 키 생성 방법

5.2 그룹에 참가 시 키 생성 방법

수신자는 데이터를 전송받고자 하는 경우에는 IGMP[14] 와 같은 프로토콜을 이용하여 그룹에 참여하는 메시지를 전송한다. 가장 가까운 멀티캐스트 수신자 그룹 중에 수신자는 IGMP 를 전송한 수신자에게 그룹에 참여하라는 메시지와 안전한 유니캐스트 채널을 통해서 p, q, g 를 전송한다. 그리고 수신자 그룹에게 새로운 수신자가 참여했다는 메시지를 멀티캐스트를 통해서 전송한다. 각 수신자는 자신이 가지고 있는 키를 바꾸고 키생성 프로토콜에 의해서 새로운 그룹키를 생성한다.

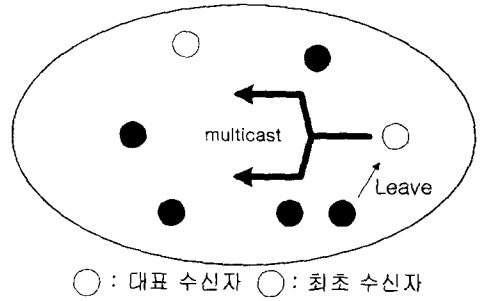

그림 2 그룹 탈퇴 시 키 생성 방법

5.3 그룹에 탈퇴 시 키 생성 방법

수신자가 멀티캐스트 그룹에서 탈퇴하고자 하는 경우에는 수신자 그룹에게 탈퇴 메시지를 전송한다. 그러면 그룹의 수신자는 탈퇴 메시지를 받는 즉시 그룹에 멀티캐스트하여 모든 수신자에게 한 수신자가 탈퇴했음을 알린다. 멀티캐스트를 받은 모든 수신자는 키 생성 프로토콜에 의해 자신의 키를 바꾸고 새로운 그룹키를 생성한다.

5.4 재 그룹핑 시 키 생성 방법

수신자 그룹이 n 보다 작은 경우에는 그룹의 보안을 위해서 n 이상이 되도록 재그룹핑 해야 한다. 이 경우에는 가장 가까운 그룹 간에 재그룹핑을 해서 그룹의 크기가 n 이상이 되도록 그룹을 생성하고 대표 수신자를 선정한 후 대표수신자가 멀티캐스트를 통해서 새로운 그룹키를 다시 생성하도록 한다.

5.5 주기적인 키 생성

(t, n) 쓰레시홀드 크립토시스템은 주기적으로 키를 재생성하는 경우 안전도가 더 증가하는 것으로 알려져 있다.[11, 12] 수신자 그룹에 새로운 참가나 탈퇴가 없는 경우 주기적으로 키를 생성 메시지를 대표 수신자가 전송하여 새로운 그룹키를 생성할 수 있다.

6. 안전한 멀티캐스트를 위한 구조

송신자가 멀티캐스팅을 하는 경우 그룹을 생성하고 수신자는 그룹을 만들어 키를 생성한다. 대표수신자는 자신이 속해 있는 서브그룹과 상위 그룹에 속한다. 그리고 공개키를 수신자 그룹의 한 수신자가 대표로 생성한다. 그리고 대표 수신자는 서브 그룹의 키로 데이터를 암호화해서 전송한다. 수신자는 키 생성 프로토콜을 통해 생성한 키를 이용하여 원문을 구해 낸다.
이 방법을 통하면 (t, n) 쓰레시홀드 크립토시스템의 공개키/비밀키 암호체계가 안전하다면 기밀성과 무결성을 보장할 수 있게 됨을 알 수 있다.

7. 결론

우리는 이 연구를 통해서 네트워크 상에 Iolus 에서 제안된 GSA 와 같은 중앙집중식 서버를 통하지 않고 안전한 멀티캐스트를 할 수 있는 방법을 제안하였다. 앞으로 키 생성 프로토콜에 따른 오버헤드를 줄일 수 있는 방법에 대해서 연구해야 할 것이다.

8. 참고문헌

[1] Ran Canetti, Juan Garay, Gene Itkis, Daniel Micciancio, Moni Maor, Benny Pinkas, "Multicast Security : A T axonomy and Some Efficient Constructions", INFOCOM `99

[2] Suvo Mittra, "Iolus : A Framework for Scalable Secure Multicasting", ACM SIGCOMM `97

[3] Patrick McDaniel, Atul Prakash, and Peter Honeyman, "Antigone : A Flexible Framework for Secure Group Communicatio n", Proceedings of the 8 th USENIX Security Symposium, Washington D.C., USA, August 23-26, 1999

[4] M. J. Moyer, J.R. Rao, P. Rohatgi, "Maintaining Balanced Key Trees for Secure Multicast", SMuG draft, 25 June, 1999

[5] H. Harney,C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC 2094

[6] D.M. Wallner, E. J. Harder, R. C. Agee, "Key Management for Multicast: Issues and Architectures", RFC 2627, June 1999

[7] Douglas, R. Stinson, Cryptography - theory and Practice, CRC Press, 1995.

[8] Torben Pryds P edersen, "A Threshold Cryptosystem without a Trusted Party", In Advances in Crytology -Eurocrypt '91, pages 522-526, 1991

[9] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin, "Robust Threshold DSS Signature", Eurocrypt '96

[10] Y. Desmedt, Y. Fra nkel., "Threshold crypto-systems". In: Advances in Cryptology - Crypto '89, Proceedings, Lecture Notes in Computer Science 435 (G. Brassard, Ed.), Springer-Verlag, 1990, pp. 307-315.

[11] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive public -key and signature scheme s", In proceedings of the Fourth Annual Conference on Computer Communications Security", ACM, 1997, pp. 100-120.

[12] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage", Advances in Cryptology - Cryto '95, Santa Barbara, Califonia, U.S.A, Aug. 1995, pp. 457-469.

[13] Matthew J. Moyer, Josyula R.Rao, and Pankaj Rohatgi, "A Survey of Security Issues in Multicast Communications", IEEE Network, November/December 1999

[14] W. Fenner , "Internet Group Management Protocol, Version 2", RFC 2236, November 1997